

This item was submitted to Loughborough's Institutional Repository (<https://dspace.lboro.ac.uk/>) by the author and is made available under the following Creative Commons Licence conditions.



CC creative commons
COMMONS DEED

Attribution-NonCommercial-NoDerivs 2.5

You are free:

- to copy, distribute, display, and perform the work

Under the following conditions:

 **Attribution.** You must attribute the work in the manner specified by the author or licensor.

 **Noncommercial.** You may not use this work for commercial purposes.

 **No Derivative Works.** You may not alter, transform, or build upon this work.

- For any reuse or distribution, you must make clear to others the license terms of this work.
- Any of these conditions can be waived if you get permission from the copyright holder.

Your fair use and other rights are in no way affected by the above.

This is a human-readable summary of the [Legal Code \(the full license\)](#).

[Disclaimer](#) 

For the full text of this licence, please go to:
<http://creativecommons.org/licenses/by-nc-nd/2.5/>

**Reducing the Risk of E-mail Phishing in the State of Qatar through an
Effective Awareness Framework**

By

Mariam Khalid AL-Hamar

A Doctoral Thesis

Submitted in partial fulfilments for the award of Doctor of Philosophy of
Loughborough University

2010

© Mariam Khalid AL-Hamar 2010

Abstract

In recent years, cyber crime has focused intensely on people to bypass existing sophisticated security controls; phishing is one of the most common forms of such attack. This research highlights the problem of e-mail phishing. A lot of previous research demonstrated the danger of phishing and its considerable consequences. Since users' behaviour is unpredictable, there is no reliable technological protective solution (e.g. spam filters, anti-viruses) to diminish the risk arising from inappropriate user decisions.

Therefore, this research attempts to reduce the risk of e-mail phishing through awareness and education. It underlines the problem of e-mail phishing in the State of Qatar, one of world's fastest developing countries and seeks to provide a solution to enhance people's awareness of e-mail phishing by developing an effective awareness and educational framework. The framework consists of valuable recommendations for the Qatar government, citizens and organisations responsible for ensuring information security along with an educational agenda to train them how to identify and avoid phishing attempts. The educational agenda supports users in making better trust decisions to avoid phishing that could complement any technical solutions. It comprises a collection of training methods: conceptual, embedded, e-learning and learning programmes which include a television show and a learning session with a variety of teaching components such as a game, quizzes, posters, cartoons and a presentation. The components were tested by trial in two Qatari schools and evaluated by experts and a representative sample of Qatari citizens.

Furthermore, the research proves the existence and extent of the e-mail phishing problem in Qatar in comparison with the UK where people were found to be less vulnerable and more aware. It was discovered that Qatar is an attractive place for phishers and that a lack of awareness and e-law made Qatar more vulnerable to the phishing. The research identifies the factors which make Qatari citizens susceptible to e-mail phishing attacks such as cultural, country-specific factors, interests and beliefs, religion effect and personal characteristics and this identified the need for enhancing Qatari's level of awareness on phishing threat.

Since literature on phishing in Qatar is sparse, empirical and non-empirical studies involved a variety of surveys, interviews and experiments.

The research successfully achieved its aim and objectives and is now being considered by the Qatari Government.

Key words

Information security, Identity theft, E-mail phishing, Social engineering, Vulnerability testing, Security awareness.

Acknowledgements

After sincerely thanking Allah for all blessings and bounties, I would like to thank many people for their contribution, assistance, support and guidance during my PhD research. Special thanks are offered to my parents and family for their continuous encouragement along the joyful journey of knowledge which has brought this research to fruition.

I am also grateful to my home country of Qatar which is committed to education and people development and to my employer, the Ministry of Foreign Affairs, for sponsoring my postgraduate education. I would like to thank my supervisors, Prof. Ray Dawson and Dr. Lin Guan, for their sustained support and valuable advice. I would like to thank as well everyone who has contributed and participated in this research including experts, participants and organisations who the authorisation and copyright clearance. Special thanks go as well to Al-Jazeera Children's Channel for giving me the chance to make an expert contribution to a TV show on phishing.

Contents

Chapter 1 Intorduction	1
1.1 Background.....	1
1.2 Problem Domain.....	4
1.3 Research Scope and Limitation.....	7
1.4 Target Group.....	8
1.5 Research Questions.....	10
1.6 Research Aim and Objectives.....	10
1.7 Research Issues.....	11
1.8 Research Contribution to Knowledge.....	12
1.9 Thesis Structure.....	13
Chapter 2 Literature Review	16
2.1 Social Engineering.....	16
2.2 Phishing.....	19
2.3 Types of Phishing.....	20
2.4 Vulnerability to Phishing.....	23
2.4.1 Clever tricks used by phishers.....	25
2.4.2 Behaviour of users.....	28
2.4.3 Summary of Vulnerabilities.....	33
2.5 Anti-Phishing Solutions.....	34
2.5.1 Technical Solutions.....	34
2.5.2 Non-technical (Awareness) Solutions.....	40
2.5.3 Summary of Non-technological Solutions.....	52
2.6 The Contribution of the Literature Review.....	53
2.7 Summary.....	54
Chapter3 Research Methodology	56
3.1 Research Philosophy.....	56
3.1.1 Positivism.....	56
3.1.2 Interpretivism.....	57
3.1.3 Choice of Philosophy.....	57
3.2 Research Approach.....	58
3.2.1 Qualitative/ Quantitative.....	58
3.2.2 Deductive/ Inductive.....	59
3.2.3 Subjective/ Objective.....	59
3.2.4 Choice of Approach.....	59
3.3 Research Strategy.....	60
3.3.1 Choice of Strategy.....	61
3.4 Data Collection Methods.....	64
3.4.1 Literature Review.....	66
3.4.2 Review of Literature on Qatar and UK.....	66
3.4.3 Survey.....	67
3.4.4 Penetration Tests and Laboratory Experiment.....	71
3.4.5 Findings.....	72
3.4.6 Development and Evaluation of the Framework.....	72
3.5 Data Sampling Method.....	72
3.5.1 Choice of Sampling Method.....	74

3.6 Summary.....	74
Chapter 4 Qatar in the Eyes of Phishers	76
4.1 Overview of Qatar.....	76
4.2 Why Qatar is Attractive to Phishers.....	77
4.2.1 Economic Development.....	77
4.2.2 Growth of Internet Users.....	80
4.2.3 The Lack of Electronic Law.....	89
4.2.4 Effect of Qatar Culture.....	90
4.3 Interviews.....	91
4.3.1 Extent of E-mail Phishing.....	92
4.3.2 Vulnerability to Phishing.....	93
4.3.3 Problems Faced with Phishing Incidents.....	94
4.3.4 Cooperation Between Organisations.....	96
4.3.5 Review of Organisational Strategy of Defence Against Phishing.....	97
4.3.6 Process Deployed for Awareness.....	98
4.4 Summary.....	100
Chapter 5 Surveying Awareness of Phishing	103
5.1 Questionnaire Aim.....	103
5.2 Questionnaire Sampling.....	103
5.3 Questionnaire Planning and Design.....	104
5.3.1 First Review.....	105
5.3.2 Pilot-test.....	106
5.4 Questionnaire Structure.....	107
5.5 Questionnaire Implementation.....	109
5.5.1 Sample Size.....	110
5.5.1 Participant Contribution.....	110
5.6 Survey Analysis.....	112
5.6.1 Questionnaire Analysis.....	112
5.6.1.1 General Analysis of the Qatar Questionnaire.....	113
5.6.1.2 In-depth Analysis of the Qatar Questionnaire.....	126
5.6.2 General Analysis of UK Questionnaire.....	129
5.7 Comparison of Questionnaire Outcomes for the UK and Qatar.....	138
5.8 Summary.....	141
Chapter 6 Penetration Tests and Laboratory Experiment	144
6.1 The Phishing Experiments.....	144
6.2 Penetration Tests.....	146
6.2.1 Test 1.....	146
6.2.2 Authorisation.....	147
6.2.3 Test 1 Process.....	148
6.2.3.1 Planning and Design.....	148
6.2.3.2 Running the test.....	152
6.2.3.3 Analysis of the Results and Discussion of the Findings.....	154
6.2.4 Conclusion.....	156
6.3 Penetration Test 2.....	157
6.3.1 Test 2 Process.....	157
6.3.1.1 Planning and Design.....	158

6.3.1.2	Running the Test.....	160
6.3.1.3	Analysing Results and Discussing Findings.....	160
6.3.2	Conclusion.....	165
6.4	Laboratory Experiment.....	165
6.4.1	Experimental Process.....	166
6.4.1.1	Planning and Design.....	166
6.4.1.2	Running the Experiment.....	170
6.4.1.3	Evaluating the Participants' Responses.....	171
6.4.1.4	Analysis of Results and Discussion of the Findings.....	172
6.5	Collating the Results of All Tests.....	178
6.6	Summary.....	183
Chapter 7 Findings and Recommendations		185
7.1	Findings.....	185
7.2	Recommendations.....	188
7.2.1	Recommendations for Qatar Government.....	188
7.2.2	Recommendations for organisation officials responsible for ensuring information security.....	190
7.2.3	Qatari Citizens.....	192
7.3	Evaluation of Recommendations.....	194
7.3.1	Recommendations for Government.....	196
7.3.2	Organisation recommendations.....	200
7.3.3	Qatari citizens' recommendations.....	202
7.3.3.1	Revised Recommendations for Qatari citizens.....	203
7.4	Summary.....	206
Chapter 8 An Educational Programme for Phishing Awareness		210
8.1	Development of an Educational Programme.....	211
8.1.1	Poster Development.....	212
8.1.2	Cartoons.....	219
8.1.3	Presentation Slides.....	221
8.1.4	Booklet.....	222
8.1.5	Quizzes.....	222
8.1.5.1	Quiz 1.....	222
8.1.5.2	Quiz 2.....	223
8.1.5.3	Quiz 3: Anti-phishing Game.....	224
8.1.6	Development of anti-phishing e-learning.....	239
8.2	Running programme session.....	240
8.3	Running the media programme.....	241
8.4	Summary.....	246
Chapter 9 Evaluation of the Educational Framework		248
9.1	Development of the Educational Framework.....	248
9.2	Evaluation of the anti-phishing educational framework.....	250
9.3	Outcomes for Embedded and Contextual Training.....	251
9.4	Outcomes for Learning Sessions and E-Learning.....	252
9.5	Evaluation of the Television Programme.....	256
9.6	Summary.....	261

Chapter 10 Conclusions and Future work	263
10.1 Research contributions and implications.....	263
10.2 Research Achievements.....	264
10.3 Research Limitations.....	264
10.4 Conclusion.....	265
10.5 Suggestions for Future work.....	268
10.6 The Success of this PhD Research.....	272
Appendices	273
Appendix A.....	273
Appendix B.....	309
Appendix C.....	354
Appendix D.....	384
Appendix E.....	403
Appendix F (CD)	
Appendix G (USB)	
References.....	426

List of Figures

Figure 1.1: Research structure.....	3
Figure 1.2: Thesis outline	14
Figure 2.1: Security indicators in Mozilla Firefox trust bar	37
Figure 2.2: Yahoo sign-in seal	39
Figure 2.3: Loughborough University embedded training	50
Figure 3.1: Research stages.....	65
Figure 3.2: Interview plan.....	71
Figure 3.3: Choice of research methodology	75
Figure 4.1: GDP growth forecast for 2009	79
Figure 4.2: Process of dealing with phishing incidents	96
Figure 4.3: Why Qatar is attractive to phishers	100
Figure 5.1: Decision tree for determining appropriate participants	108
Figure 5.2: Questionnaire structure.....	108
Figure 5. 3: Gender (Qatar).....	114
Figure 5.4: Age group (Qatar)	114
Figure 5.5: Education level (Qatar)	114
Figure 5.6: Occupation (Qatar)	114
Figure 5.7: E-mail phishing knowledge (Qatar)	115
Figure 5.8: Source of knowledge (Qatar)	116
Figure 5.9: Trend of e-mail phishing (Qatar).....	116
Figure 5.10: Participants' worry about e-mail phishing (Qatar).....	117
Figure 5.11: Use of anti-phishing software (Qatar)	117
Figure 5.12: Participants' ability to detect a phishing attack (Qatar)	119
Figure 5.13: Participants' procedure once attacked (Qatar)	120
Figure 5.14: Participants' disclosure of their own e-mail addresses (Qatar)	121
Figure 5.15: Frequency of receiving phishing e-mails (Qatar).....	122
Figure 5.16: Frequency of being tricked by e-mail phishing (Qatar)	123

Figure 5.17: Reason for participants' being tricked by phishing (Qatar)	124
Figure 5.18: Efficiency of existing anti-phishing software (Qatar)	125
Figure 5.19: The best way to defend against phishing (Qatar)	125
Figure 5.20: Participants' preferred method for awareness and education (Qatar)	126
Figure 5.21: Gender (UK).....	130
Figure 5.22: Age group (UK).....	130
Figure 5.23: Education level (UK).....	130
Figure 5.24: Occupation (UK)	131
Figure 5.25: E-mail phishing knowledge (UK)	131
Figure 5.26: Source of knowledge (UK).....	132
Figure 5.27: Trend of e-mail phishing (UK).....	132
Figure 5.28: Participants' worry about e-mail phishing (UK)	133
Figure 5.29: Use of anti-phishing software (UK)	133
Figure 5.30: Participants' ability to detect phishing attack (UK).....	134
Figure 5.31: Participants' procedure once attacked (UK)	134
Figure 5.32: Participants' disclosure of own e-mail addresses (UK)	135
Figure 5.33: Frequency of receiving phishing e-mails (UK).....	135
Figure 5.34: Frequency of being tricked by e-mail phishing (UK)	136
Figure 5.35: Reason for participants' being tricked by phishing (UK)	136
Figure 5.36: Efficiency of existing anti-phishing software (UK)	137
Figure 5.37: Best way to defend against phishing (UK).....	137
Figure 5.38: Participants' preferred method for awareness and education (UK)	138
Figure 6.1: Penetration test 1	148
Figure 6.2: E-mail 1 (Account verification)	150
Figure 6.3: Embedded training alert message.....	151
Figure 6.4: E-mail 2 (Request to download attachment)	151
Figure 6.5: E-mail 3 (Request for private information by e-mail or SMS)	152
Figure 6.6: Penetration test 2	158
Figure 6.7: Laboratory experiment process	166
Figure 6.8: Why are Qataris vulnerable to phishing?	179
Figure 7.1: Grounded theory.....	186
Figure 8.1: Awareness framework.....	210
Figure 8.2: Poster 1- Be aware of phishing.....	214
Figure 8.3: Poster 2- Let's make phishing disappear!.....	216
Figure 8.4: Poster 3- Story board.....	218
Figure 8.5: Cartoon 1.....	220
Figure 8.6: Cartoon 2.....	220
Figure 8.7: Presentation slide.....	221
Figure 8.8: Factors addressed in game.....	226
Figure 8.9: Three educational games.....	226
Figure 8.10: Game characters screen.....	229
Figure 8.11: Log in and register screen.....	230
Figure 8.12: Welcome screen.....	231
Figure 8.13: Introduction movie clip.....	231
Figure 8.14: Game menu.....	232
Figure 8.15: Game instruction screen for the fish maze game.....	232
Figure 8.16: Conceptual knowledge screen.....	233

Figure 8.17: Procedural knowledge screen.....	233
Figure 8.18: Game screen for the fishing game.....	234
Figure 8.19: Game screen for the fish market game.....	234
Figure 8.20: Game screen for the fish maze game.....	235
Figure 8.21: ‘Game over’ screen for the fishing game.....	235
Figure 8.22: Results screen for the fishing game.....	236
Figure 8.23: Game flow chart.....	238
Figure 8.24: Login page of e-learning site.....	240
Figure 9.1: Quiz 2 results.....	252
Figure 9.2: Quiz 3 results.....	253
Figure 9.3: Does it enhance the users’ level of defence?.....	253
Figure 9.4: How it can be best described?	254
Figure 9.5: Is the information provided important to know?.....	254
Figure 9.6: Which educational material was more effective?.....	254

List of Tables

Table 2.1: Learning principles	46
Table 3.1: Additional strategies used for each objective	63
Table 3.2: Data sampling method	73
Table 3.2: Choice of sampling method.	74
Table 4.1: GDP, growth rate, investment and unemployemnt of Qatar and UK.....	78
Table 4.2: Year of Internet access for UK and Gulf States	81
Table 4.3: Growth of Internet use in GCC and UK	81
Table 4.4: Adult (age 15 and older) literacy rates in GCC countries and UK.....	84
Table 4.5: B2C and B2B trade values in Qatar (2005)	88
Table 4.6: Population of Qatar.....	90
Table 5.1: E-mails and possibility of phishing	118
Table 6.1: Results of Reality Study 1	155
Table 6.2: Vulnerabilities identified in Penetration Test 1	156
Table 6.3: Vulnerabilities identified in Penetration Test 2	164
Table 6.4: Six Phishing E-mails Used in Identification Test.....	169
Table 6.5: Score rating for laboratory experiment.....	172
Table 6.6: Results for the Laboratory experiment	173
Table 6.7: Vulnerabilities identified in laboratory experiment.....	175
Table 6.8: Vulnerabilities of Qataris to Phishing Identified in this Research	180
Table 6.9: Vulnerabilities of Qataris to Phishing Identified in this Research	181
Table 6.10: Vulnerabilities of Qataris to Phishing Identified in this Research	182
Table 6.11: Vulnerabilities of Qataris to Phishing Identified in this Research	182
Table 6.12: Vulnerabilities of Qataris to Phishing Identified in this Research	182
Table 7.1: Main outcomes of the research	187
Table 8.1: Scores assessment for Quiz 2	224
Table 8.2: Typical questions for games	228
Table 8.3: Scores assessment for game.....	237
Table 9.1: Research implementation of each training approach.....	248
Table 9.2: Learning principles applied in framework.....	249
Table 9.3: Evaluation process used for each training method	250

Table 9.4: Outcomes for the embedded and contextual training methods..... 251
Table 9.5: Advantages and disadvantages of each method in the framework.....259

List of Publications

Mariam Al-Hamar, Ray Dawson, Lin Guan, "A Culture of Trust Threatens Security and Privacy in Qatar," cit, pp.991-995, 2010 10th IEEE International Conference on Computer and Information Technology, 29 June-1 July 2010, Bradford, UK.

Chapter 1 Introduction

This chapter will guide the reader to the motivation for this research by presenting the research problem domain. In addition, it provides an introduction to the thesis and the research topic along with a general background on phishing. It leads to an identification of the research scope, target group, hypotheses, research questions, aim and objectives, contribution to knowledge and thesis structure.

1.1 Background

Nowadays, since the Internet has become ubiquitous, increasing numbers of people of all ages are getting into this massive, multifaceted electronic medium and users are currently estimated to number 1.8 billion (Internet World Stats, 2009a). The Internet is no longer simply a means of gathering and sharing information, serving economic needs and providing education and entertainment, but is now an indispensable part of the daily life of people in their public and private affairs, assisting them in crucial day-to-day decisions, often with financial links. As a result, thieves have quickly found that the Internet offers them a superior environment in which to carry out their attacks on a still vulnerable society and this has led to the appearance of electronic fraud, the so-called e-fraud. However, with the massive development in security and countermeasures, e-fraud fraudsters have found difficulties in perpetrating their attacks. Therefore, those thieves have thought of ways of bypassing the sophisticated security controls and measures by shifting their focus on people to commit their crimes. Since thieves believe that people are the weakest link in the security chain of any organisation, no matter how sophisticated its security controls, cyber criminals are currently moving to exploit people in committing their offences (Symantec, 2006). Thieves have always known that the best way around any security system is to manipulate a human being into giving them what they want, and this is what people in the IT field refer to as ‘social engineering’ (Gartner, 2002a), to be described later.

Hence, several kinds of attack against people have emerged, of which phishing is a paradigm. It is a type of social engineering attack and takes the form of an online

identity theft which targets people to gather personal and confidential information such as username and password to commit a crime in the name of the true owner which could cause the victim negative consequences (Bielski, 2004; Litan, 2004). However, with the development of new communication channels, phishers have found new means to carry out their attacks. Consequently, different categories of phishing have been discovered such as Vishing, SMishing, Pharming, Google phishing, Wi-phishing, Phishing scam and Spear phishing (described in detail in Section 2.3).

Although 1997 was the first occasion when the media demonstrated phishing and its threat (Ollmann, 2004), phishing attacks have subsequently increased dramatically. The majority of researchers have considered phishing as a formidable attack facing online consumers (Herzberg, 2008; APWG, 2006; Consumer Reports, 2006; Gartner, 2005; Pruitt, 2005). Accordingly, this has provided the motivation to focus on phishing as a research area (for more details, see the research problem domain in Section 1.2).

Since e-mail is one of the most frequently used means for communication through outside networks, it has become the most targeted by attackers using phishing. Consequently, this research focuses on online identity theft through e-mail phishing and the lack of awareness on the part of users of the danger of this attack. The research spotlights the problem of e-mail phishing in the state of Qatar as an example of a developing country, since it was discovered that Qatar presents a fertile ground for phishers to commit their crimes (described in detail in Chapter 4). It seeks to reduce the e-mail phishing hazard in Qatar by developing an e-mail phishing awareness and educational framework consisting of a set of recommendations and an educational agenda. This research will add considerable inputs to knowledge as it sheds light on Qatar society, which is largely ignored in the literature, and identifies the factors affecting people's responses to e-mail phishing, including the cultural and country-specific factors, the awareness of Qatari citizens of the e-mail phishing threat compared to British citizens and the susceptibility of Qatari people to e-mail phishing.

The general research structure is shown in Figure 1.1. The thesis starts with an introduction to the thesis, followed by an in-depth literature review in the areas of

phishing, education and training. This perspective of previous research on e-mail phishing provides the pillars of e-mail knowledge for understanding the nature of e-mail phishing and the previous methods applied as a defence against it, with an emphasis on the methods of education and training which could be adopted. The research methodology is built on these pillars of knowledge, including a review of literature to illustrate the factors which make Qatar an attractive place for phishers, surveys and interviews in Qatar and the UK to illustrate the phishing problem, together with experiments, comprised of penetration tests (Weissman, 1994 and 1995) and experimental studies in Qatar to identify the factors which make Qatari citizens susceptible to phishing. Consequently, the findings are built on the research results, covering all aspects of the research and finally achieving the overall contribution of the research which is to define an e-mail phishing awareness framework to help in reducing the risk of e-mail phishing in Qatar. The framework involves formulating effective recommendations and an e-mail phishing educational framework for target groups (the thesis structure is described in detail in Section 1.9).

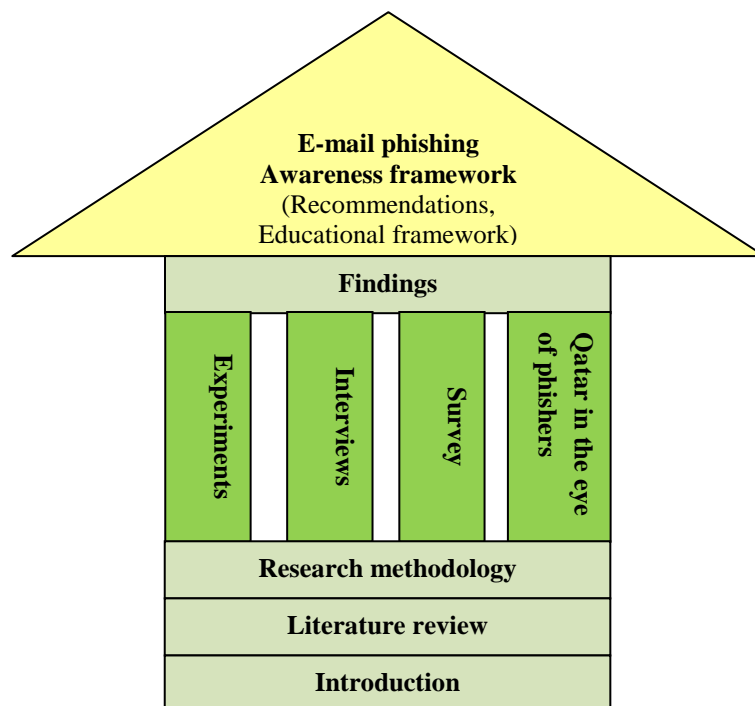


Figure 1.1: Research structure

1.2 Problem Domain

Even with a very secure information system, vulnerability to phishing could be the weakest link for any organisation (APWG, 2006; Ollmann, 2004). It is an attack that is hard to defend against, even with the latest technology in information security. That is because phishing does not attack devices; it attacks the human users who are harder to protect. Since the number of organisations having an online presence has increased, phishers have a greater opportunity to make their attacks on an ever greater number of online consumers (Emigh, 2005).

The susceptibility to phishing is increased since organisations have moved into mobile systems that allow users to access their organisational networks remotely from wherever they choose. With the existence of mobile systems, organisational networks could be breached by an unauthorised party via the users through their Internet-enabled services and electronic communication such as e-mail. The opportunity to send spam e-mails has facilitated the performance of phishers who can thus send a huge number of phishing e-mails at minimal risk. These are usually sent from hacked mail servers and are considered as unwanted e-mail (Honeynet Project and Research Alliance, 2005; Bellovin, 2004).

Much research has demonstrated the danger of phishing and the major consequences of such attack (APWG, 2006; Dhamija et al., 2006; Emigh, 2005; Gartner, 2005; Tsai, 2005; Goldsborough, 2004; Ollmann, 2004). According to Herzberg (2008), phishing has been considered as the most threatening of the attacks faced by online consumers. It has been increasing since it is relatively cheap to launch, whilst the outcome losses could be considerable for victims who were successfully deceived (Consumer Reports, 2006). In late 2003 and the beginning of 2004, phishing intimidation was recognised as it broadened across the Internet (Microsoft, 2006) and it has been considered to be one of the most widespread of Internet threats (Pruitt, 2005).

A survey in May 2004 to May 2005 by Gartner (2005) has found a prevalence of phishing e-mails and around 73 million online USA adults reported that throughout the year they may have received 50 or more phishing e-mails. About 1.2 million online

USA consumers reported that they had been tricked by phishing e-mails; the total impact of their losses to the phishers was about \$929 million (Gartner, 2005). Even more, other research reported that the amount of phishing attacks had reached endemic proportions (APWG, 2006). According to a survey carried out from July 2005 to June 2006 by the CERT Coordination Centre (2006), 31 per cent of organisations stated that they had been attacked by phishing where phishers posed online as employees pretending to be a member of the company and asked for disclosure of the victim's personal data.

Symantec, the world's leading organisation in providing security solutions, detected 1.3 billion phishing e-mails in the first six months of 2006, where 54 per cent of e-mails were considered as spam, an increase over the previous six months when spam records reached 50 per cent. Symantec has commented that some e-mails targeting different users were used several times in different phishing attempts but nevertheless each e-mail was different in content and structure and in the way the phishers tried to deceive the receivers into providing their private information (Symantec, 2006). According to the Phishing Activity Trends Report by the E-mail Phishing Working Group (APWG, 2006), in August 2006 the number of phishing sites had increased and it reported the presence of 10,091 active ones, an increase of 192 per cent on the same month in the preceding year. The fraudulent websites were active for a short time, 4.8 days on average. In addition, the 26,150 unique phishing messages in August 2006 represented a 190 per cent increase compared to the previous August (APWG, 2006).

Today, cyber attacks tend to be carried out by professional attackers with a specific targeted aim, it is no longer a hobby nor a form of cyber destruction (Gartner, 2006b). The study by Gartner demonstrates that replying to e-mail phishing is now more likely to have negative consequences such as stolen money, information or even identity (Bielski, 2004; Litan, 2004). Those who have fallen prey to a phishing attack can suffer considerable losses as a consequence. The victims usually have to spend a huge amount of time and money to recover from identity theft-related damages such as recovering their reputation, good name, credit report and other damage that might occur from the attack (FTC, 2006, 2005; Emigh, 2005). Victims spent around 297 million hours to recover from the damage caused by identity theft attack, according to a study by the

Federal Trade Commission (FTC) in 2005 (FTC, 2006). Research by Kondakci (2009) defines a cost model to estimate the impact caused by Internet malware by identifying the growth and prospective loss caused by the attack. Infection time, it was found, could be reduced by effective recovery techniques through enhancing user awareness or the protection of the system through providing advanced technological solutions and an efficient security policy.

The researcher has classified the impact of phishing as tangible such as financial, loss of information and damage of computer, and intangible such as negative reputation, discomfort and anger, as follows:

1. Tangible impact

Phishers' aspirations have changed from being a mischievous trick requiring technical expertise into a means of gaining financial income by gathering valuable information for committing identity theft or other forms of fraud (Symantec, 2006). However, financial gain is not always the intention of the phisher; sometimes the major consequence of the phishing attack is the loss of confidential information disclosed to the phisher. The attack could cause an indirect financial loss to the victim if the illegally gained information is sold on the black market, for example for identity theft rings, chat channels and online brokering forums (Emigh, 2005; Hubbard, 2005). According to a Gartner (2005) report, during 2005 online information theft attacks on USA online consumers reached \$2.7 billion of losses, of which more than \$2.39 billion were from stolen account information and around \$397 million from attackers' using the stolen information to create new accounts, acquire credit or even create a new fake identity in the victim's name (Litan, 2006).

2. Intangible impact

With the amount of information gained from the victim, the attacker could impersonate that person and such actions could result in a bad reputation and a bad credit report leading perhaps to denial of loan requests or accommodation. The consequences from the attack are not always tangible as there might be a psychological impact: the victim

might experience negative emotions such as feelings of anger, anxiety, annoyance, disgrace and violation (FTC, 2005, 2006). Furthermore, phishing could weaken trust of the online environment (Milletary, 2006; Pandit, 2006; ActivCard, 2004; Litan, 2004) which could result in altered online shopping behaviour and a fear of entering personal data online (Gartner, 2005; ActivCard, 2004). The vice-president of VISA has stated that clients recognise the extreme danger of the online environment and that could limit online expenditure (Radcliff, 2005b).

The phishing threat concerns online consumers, which was proven in various studies. According to a survey by Cyota (2005), cited by Butler (2007), a fraud prevention service provider, because of the phishing threat, more than 50 per cent of Internet consumers are anxious about making e-commerce transactions and 70 per cent have commented that they were uncertain how to react to an e-mail claiming to come from a bank. Another study by Symantec (2006) demonstrates that worries of phishing had led almost one-third of the respondents to avoid online banking (Radcliff, 2005b).

Although phishing is considered a problem, in most research done so far there was a shortage of information about the phishing problem in Qatar. However, the researcher has assumed that the problem does exist in Qatar similar to other countries, especially since there is a massive development in Qatar in all sectors, including the economy and education, in which telecommunications play an ever increasing role, which makes Qatar an attractive place for e-criminals and especially phishers to commit their crimes. An initial objective of this research was to discover the existence and magnitude of the problem in Qatar, the awareness of Qataris of its implications and their vulnerability.

1.3 Research Scope and Limitation

This research focuses on a type of social engineering attack known as 'phishing'. Since e-mail is one of the most frequent communication channels through which users communicate, the research is narrowed to focus on online identity theft through e-mail which is called 'e-mail phishing' and this includes spear phishing e-mails. The time constraint of a PhD means it is not possible to cover all the possible phishing techniques

currently employed, such as Vishing, SMishing, Pharming, Google phishing and Wi-phishing.

Although the technical solutions are essential to defend against e-mail phishing, this research focuses only on awareness and education as a superior solution to reduce the risk of e-mail phishing. The research underlines the problem of e-mail phishing in the State of Qatar, used as an example of a developing country, and seeks to understand the factors which make e-mail phishing successful in such a society and to propose a solution to enhance Qatari citizen's awareness of e-mail phishing through an effective awareness and educational framework. The choice Qatar as a focus was due to the convenience of access. The lack of data on the phishing topic in Qatar makes it original and interesting to investigate, as it is assumed that the problem exists in the region. It would also be interesting to compare results with those similar investigations in the UK.

1.4 Target Group

One of the intended groups to benefit from this research is e-mail research scholars. The research will provide a contribution for scholars' research on e-mail phishing and awareness. It addresses the aspects which make people vulnerable to the phishing threat and offers a valuable e-mail phishing awareness and educational framework to reduce the risk of e-mail phishing. It also provides an empirical study of the e-mail phishing threat in the state of Qatar which has not been covered before in the literature.

E-mail users who may be the potential victims of e-mail phishing would benefit from this research. However, since all types of phishing are a major threat facing all individuals, awareness of e-mail phishing could be valuable for everyone, even those who do not have an e-mail account. The proposed solution will provide sufficient knowledge and awareness required for all individuals to protect themselves against any form of phishing attack.

Moreover, the findings of this research are intended to be of potential significance to a variety of groups such as:

1. Qatar government: The research focuses on identifying the extent of the phishing problem in Qatar and the importance of resolving the problem. A list of recommendations is provided for the government with the main focus on an effective educational framework to provide awareness as a mean of reducing this threat. Moreover, other governments could benefit from the research outcome, the framework proposed and the recommendations made in this research would be applicable elsewhere with certain variations, taking into account the cultural and country-specific factors.
2. Organisation officials responsible for ensuring information security in Qatar: The research meets the needs of this group by defining a list of recommendations for them to facilitate their solving of the phishing problem. It also provides an effective e-mail phishing educational framework through which, if applied appropriately, employees would gain sufficient awareness of e-mail phishing and would consequently reduce the risk of the organisation being attacked by e-mail phishing.
3. Qatari citizens: The research provides a list of valuable recommendations for Qatari citizens to help them to protect themselves against phishing threats. In addition, the proposed solution is designed to reduce the overall e-mail phishing danger in the state of Qatar through an effective educational framework applied for Qatari citizens. The proposed solution would also be beneficial for other nations, allowing for any cultural differences.

In addition, the research identifies the factors which make Qataris vulnerable to phishing threat, including cultural, country-specific factors and others. This is a valuable outcome for all target groups which could be further studied. Although the discovered factors might be alike for other nations with certain variations, this would give clues as to what makes people in general susceptible to phishing and therefore makes phishing successful, and if those factors were eliminated it would help to reduce the phishing threat. Also, discovering those factors would help in developing effective anti-phishing solutions, whether technical or non-technical.

1.5 Research Questions

From the above, the following research questions emerge for this study:

1. Is e-mail phishing common in Qatar?
2. What is the extent of e-mail phishing in Qatar?
3. What are the factors which make Qatari citizens vulnerable to e-mail phishing attacks?
4. Are there any cultural, national or country-specific factors that might assist in the development and diffusion of e-mail phishing in Qatar society?
5. Are there any cultural, national or country-specific aspects that might be associated with people's responses to phishing e-mails in Qatar society?
6. Are Qatari people vulnerable to e-mail phishing in reality?
7. Are they aware of the e-mail phishing threat, how to recognise it and how to avoid it?
8. Are there any differences or similarities between Qatar and other developed countries, such as the UK, in awareness of the e-mail phishing threat?
9. Can the proposed e-mail phishing awareness and educational framework help in reducing the risk of e-mail phishing attack in Qatar?

1.6 Research Aim and Objectives

Experience of e-mail use indicates that e-mail phishing is growing at a massive rate and there appears to be a lack of awareness of its threat. This research focuses on awareness as an effective method to eliminate the threat of e-mail phishing.

The research aim is therefore:

To reduce the e-mail phishing hazard in the State of Qatar through developing an effective e-mail phishing awareness and educational framework.

There are a number of objectives to be met in order to achieve the research aim, as follows:

1. To review literature on previous work in the research area to see what has already been done to identify the extent of the phishing problem in general and in Qatar in particular, and to identify what actions have been taken to defend against phishing internationally and in Qatar in particular.
2. To confirm the existence of an e-mail phishing problem in Qatar.
3. To determine the factors which make Qatar an attractive place for phishers.
4. To compare the awareness of Qatari citizens of the e-mail phishing threat with that of citizens of a developed nation, such as the UK.
5. To investigate the susceptibility of Qatari people to e-mail phishing and the effects of cultural, country-specific, and other factors on the development and diffusion of e-mail phishing in Qatar society.
6. To define, from the results of all above objectives, the need for enhancing awareness and the need to provide an effective e-mail phishing awareness and educational framework.
7. To develop an e-mail phishing awareness framework to reduce the risk of e-mail phishing in Qatar which consists of a set of recommendations and proposed educational framework.
8. To evaluate the effectiveness of the proposed framework in reducing the risk of e-mail phishing in Qatar.

1.7 Research Issues

From the above aim and objectives, a number of research issues have been raised for this research to investigate further:

- An e-mail phishing problem exists in Qatar.
- There are many aspects which make the State of Qatar a fertile ground for phishers to commit their crimes.
- Qatari citizens are less aware of e-mail phishing threat compared to British citizens.

- There are many factors which make Qatari citizens vulnerable to the e-mail phishing threat and lack of awareness is one of the main factors.
- Making people aware of phishing should take account of their background, and cultural and country-specific factors.
- Qatari citizens are vulnerable to e-mail phishing attacks and most are not able to recognise such threat.
- The e-mail phishing threat can be reduced in Qatar by promoting an effective e-mail phishing awareness framework and educating people about e-mail phishing.

1.8 Research Contribution to Knowledge

The research attempts to add considerable inputs to knowledge by shedding light on Qatar society by discovering the extent of the e-mail phishing problem in such a society and defining the culture, country/region-specific and other factors which help in the development and diffusion of the problem. The research is considered original since it tackles a subject largely ignored in the literature: that is, the issue of e-mail phishing in the State of Qatar. It begins by profiling case studies of the State of Qatar, examining the awareness of the Qatari citizens of e-mail phishing and their susceptibility to falling prey to e-mail phishing attacks. It concludes by reporting on the factors which make e-mail phishing successful in Qatar and proposes a solution in an effective educational framework which aims to reduce the threat of e-mail phishing in Qatar society.

The framework involves valuable recommendations and an educational outline that is suitable and attractive for all groups of people, from children to mature adults. It is believed that this will assist not only Qatar, but also any other country with similar characteristics. The research also outlines the cultural and other aspects associated with awareness and people's responses to phishing e-mails, the vulnerability of Qataris to fall prey to phishing attacks, their ability to distinguish such attacks and the eagerness and readiness of Qatari citizens to enhance their awareness on this topic. In addition, the UK was used for comparison in the case study (see Section 3.3.1 for more information about the case study).

1.9 Thesis Structure

This thesis consists of ten chapters and an outline is shown in Figure 1.2. Chapter 1 (Introduction) provides a general introduction for the thesis which is a preface to the research topic ‘e-mail phishing’. Also, it describes the key area of research by illustrating the problem domain, aims and objectives, research scope, contribution to knowledge, along with research questions, hypotheses and thesis structure.

Chapter 2 (the Literature review) starts with demonstrating the history of fraud and its development into e-fraud, online identity theft and social engineering, along with an introduction to phishing in general. Subsequently, the review involves previous research in the field of phishing. It identifies previous research on understanding the threat of e-mail phishing along with the existing technical and non-technical methods developed to defend against this attack. It concentrates on the literature on phishing awareness and education and the literature on education in general to illustrate the need of this research and to define the scope and vision of the research solution.

Chapter 3 (Research methodology) describes the direction of the research path from the justification of research philosophy, approach, and strategy to the decision of the data collection methods used in the research to fulfill the research aim and objectives. Chapter 4 (Qatar in the eyes of phishers) gives an overview of Qatar and the UK. It presents an analysis of the literature and of interviews to highlight the aspects which make the State of Qatar a fertile ground for phishers to commit their crimes compared to other developed countries such as the UK.

Chapter 5 (Surveying awareness of phishing) presents an analysis of the survey questionnaires and interviews with participants to draw a profile of the awareness of Qatari citizens compared to British citizens. It concludes by defining some of the factors which make e-mail phishing successful in Qatar and gives an indication of the ideal awareness scheme to respond to this attack.

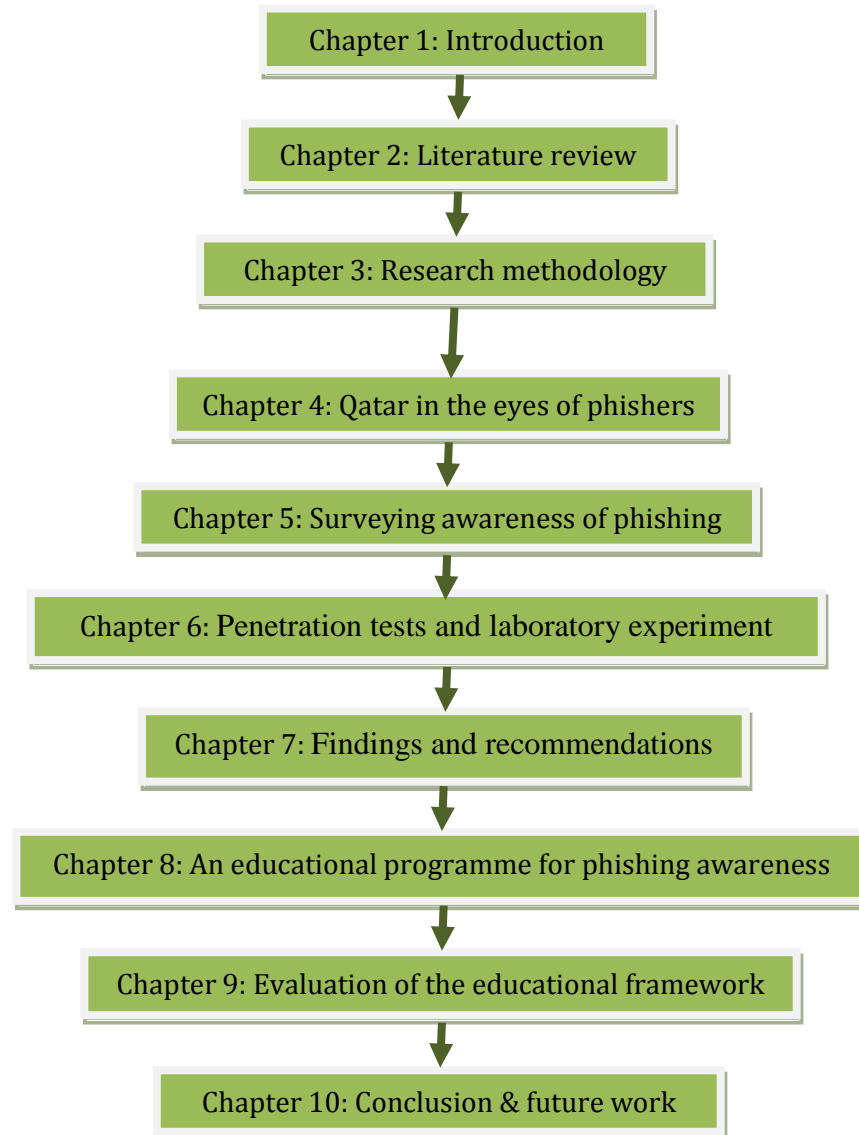


Figure 1.2: Thesis outline

Next, Chapter 6 (Penetration tests and laboratory experiment) describes the e-mail phishing penetration testing and experimental tests made in Qatar to study people's recognition and responses to e-mail phishing both in reality and in an experimental environment. There were two reality studies, one in a Qatari organisation and the other a spear phishing test on a sample of Qatari citizens. The chapter concludes with identifying the factors which make Qatari citizens vulnerable to the phishing threat.

Chapter 7 gathers the outcomes of the previous chapters to define a list of effective recommendations to help in reducing the phishing threat in Qatar. The

recommendations are directed to all target groups: Qatari government, citizens and organisation officials responsible for ensuring information security.

Chapters 8 and 9 demonstrate in detail the development of the proposed e-mail phishing educational framework, starting with the planning and designing of the effective proposed e-mail phishing awareness programme as part of the framework in Chapter 8, and gathering together the whole of the framework in Chapter 9 with an evaluation of its effectiveness in enhancing awareness and reducing the phishing problem in Qatar.

Ultimately, Chapter 10 (Conclusion and future work) presents a summary of the whole research outcome, including its limitations, and proposing recommendations for further studies.

Chapter 2 Literature Review

This chapter reviews previous research in the field of phishing and e-mail phishing in particular. It begins by providing background knowledge for the reader on the topic, starting from the terms ‘social engineering’ and ‘identity theft’ and moving on to phishing and types of attacks. Furthermore, it illustrates the mechanisms of e-mail phishing and how to spot them. Also it reviews anti-phishing solutions and what makes people susceptible to phishing and considers some literature on the culture of the State of Qatar since this is the geographical area of the study in this research.

2.1 Social Engineering

Social engineering is a broad concept which can relate to different fields: social science, politics and computer science, and often has negative connotations. According to the Oxford Dictionary (2005), social engineering is the “attempt to change society and to deal with social problems according to particular political beliefs”. For Mifflin (2000), it is the practical application of sociological principles to particular social problems. Its counterpart in the political arena, political engineering, deals with the designing of political institutions in a society. It also refers to efforts to influence popular attitudes and social behaviour on a large scale, whether by governments or private groups (Popper, 1971). However, social engineering in computer science is going to be the main concern in this thesis where it becomes the technique of manipulating people into performing prejudicial actions or divulging confidential information (Mitnick, 2002).

Social engineering thus applies techniques to deceive users into giving information or access to someone who should not receive it. According to Mitnick (2002), it is usually used against a limited number of targets selected with great care and in most cases the perpetrator never comes face to face with the victim, whereas the majority of technical attacks such as script kiddies, viruses, Trojans and other broad attacks are done without having a clear aim. Social engineering attackers, however, always have a clear aim, which is to acquire information or gain unauthorised access to a computer system. Kajava & Siponen (1997) state that social engineering is a technique in which an unauthorised person manages to pose as an insider or an authority to successfully get

access to information or resources. Hasle et al. (2005) add that a hacker can use social engineering to access other valuable data to benefit the hacker in further attacks. Perhaps the best definition was given by Kevin Mitnick in an interview by Tanneeru (2005):

“Social engineering is using manipulation, influence and deception to get a person, a trusted insider within an organization, to comply with a request, and the request is usually to release information or to perform some sort of action item that benefits that attacker. It could be something as simple as talking over the telephone to something as complex as getting a target to visit a Web site, which exploits a technical flaw and allows the hacker to take over the computer.”

Social engineering was recognised by Mitnick (2002) who managed to gain access to several high security government systems, not by using highly technical attacks, but by using a ‘con man’s’ approach to obtaining information and gain access. He points out that it is much easier to trick someone into giving a password for a system than to spend the effort to hack into the system. He claims it was the single most effective method in his arsenal. He used the telephone and well planned tricks to gather bits of information and then pieced them together to finally reach the intended goal (Mitnick, 2002). Years ago, social engineering was still not considered as a real threat, but recently it has become a concern discussed widely in books, journals, and academic research because it has in fact proved to be a formidable threat as it can penetrate secure information systems.

From the work of Popper (1971), Kajava & Siponen (1997), Mifflin(200), Mitnick(2002) and Hasle et al (2005), it can be concluded that social engineering relies mainly on social skills, which is an art that not everyone has. It does not require huge technical knowledge; it can be done with just a little effort or trickery applied to fool people to attain the attacker’s entire goal. For example, a hacker who spends several hours trying to decrypt a message would save a great deal of time by calling an employee posing as an authoritative person and asking for the information. Encouraged social engineers will be willing to gain information in any way possible by using different techniques to trick people to get what they want. They usually build up

information gathered from one person to another to finally reach their goal. For example, a phone book may lead to a phone call and information thus gathered may lead to another phone call and so on.

There are many techniques that can be used by social engineers to deceive people into giving away access or confidential information. They can be categorised as human-based and computer-based attacks. Computer-based social engineering relies on technology to trick the individual into supplying information which will allow the hacker to gain further access into the network. The simplest and most popular means of social engineering are still human-based. However, social engineers sometimes employ both human and computer-based attacks to achieve their goal. The basic techniques can use established trust, authority, helpfulness, knowledge of internal processes, technology, easily attainable information or any combination of them (Butler, 2007; Hasle et al. 2005; Kajava and Siponen, 1997). Harl (1997) gives some of the basic techniques, including pretending to be an employee, exchanging of favours, convincing the target that the request is normal, assuring the target that he or she will not be held responsible for what he or she is doing and plain old friendliness. In reality, the social engineering attacker might take different avenues to launch his or her attack, which might be a phone call, physical access, e-mail, Trojan programs, instant messages, chat rooms, bulletin boards or even meeting in public places (Hasle et al. 2005).

Social engineering uses several techniques in its application such as pretexting, a Trojan horse, shoulder surfing, dumpster diving, road apples, quid pro quo (i.e. something for something), phishing and some other types. These techniques are explained below (Butler, 2007):

- Pretexting usually uses the telephone to gain access to information; the attacker uses a scenario based on knowledge of some valid information to gather more confidential information such as account details, credit card number and date of birth.
- A Trojan horse uses the victim's interest or greed to deliver malware which appears to be safe (e.g. an attachment, anti-virus software, screen saver, etc.),

but actually it performs malicious actions (e.g. tracks keystrokes, uploads, address book, etc.) to gain the required information.

- In dumpster diving, the attacker searches waste bins to gain the required information from un-shredded and useful sources such as phone lists and bank details.
- For a road apple attack, the attacker relies on physical media (e.g. CD, floppy, USB Flash Drive, etc.) usually labeled to arouse curiosity such as “Salary Survey” or “Confidential Staff Information”, but it actually contains an auto run feature which loads a Trojan or virus when the victims insert it into the PC.
- Quid pro quo means ‘something for something’ (e.g. gift in exchange for information, pretending to be a help desk, etc.).
- In shoulder surfing, attackers use their presence in public places to attain the required information from observing and ‘sniffing’ people in public places such as airports, coffee shops, public Wi-Fi areas in hotels and other public places.
- Finally, phishing is a method of fraudulently obtaining confidential and private information, usually by someone who appears to be a legitimate person, and it comes in different forms: by phone, e-mail, etc. The following section provides a detailed explanation of phishing attack and its categories.

2.2 Phishing

Research has indicated that phishing is a common form of identity theft or stealing a person’s ‘good name’ (Emigh, 2005; Ollmann, 2004). There is a strong relationship between the two as phishing is an attack aiming to gather personal information such as a username and password which is considered as an identity theft, the phisher could then use the information to claim to be the victim and hence could cause the real victim negative consequences by usurping his or her name (Bielski, 2004; Litan, 2004).

Identity theft can be carried out online or offline. It was considered as one of the five increasingly common security risks in the USA in 2006, which are: targeted threats, identity theft, spyware, social engineering and viruses (Gartner, 2006a). The records show an escalation in the number of victims of identity theft in the USA, amounting to 10 million adults linked with huge losses of approximately \$15 billion (Gartner, 2005).

Hence this led to the Executive Order of President George W. Bush which established the Identity Theft Task Force to develop an inclusive approach to combat identity theft (FTC, 2006; White House, 2006).

In August 2005, the term ‘phishing’ was added to the Oxford Advanced Learner’s Dictionary (2005). Nowadays, the definition of phishing has expanded. Different researchers have described phishing differently; some consider it to stand for ‘password harvesting fishing’ (Honeynet Project and Research Alliance, 2005). The Anti-phishing work group (APWG) defines phishing as spoof e-mails designed to commit fraud by attracting receivers and tricking them to enter a phishing website to reveal their personal information and attributes such as usernames, passwords, social security numbers, credit card numbers and other personal details such as dates of birth and maternal maiden names (Emigh, 2005; Ollmann, 2004; APWG, 2006). It is essentially a technique of obtaining private information fraudulently and thereafter obtaining money illegally, which is the main aim of phishers (Vegter, 2005).

It can be concluded from the literature that phishing aims to bypass technology-based security mechanisms by manipulating people and thus tends to be faster and easier than other technical attacks. Accordingly, the majority of researchers have shown that there is an increase in the number of recent successful phishing attacks with considerable consequences for victims (Aburrous et al., 2009; Butler, 2007; Dodge et al., 2007; APWG, 2006; Dhamija et al., 2006; Abad, 2005; Butler 2005; Dhamija and Tygar, 2005; Bielski, 2004). Phishing is a complex phenomenon; there are different types of attack and some are explained below.

2.3 Types of Phishing

With the development of new communication channels, attackers attempt to carry out their attacks using them. Examination of the literature shows phishing can be categorised by the communication channel used and vishing, SMishing, pharming, google phishing, wi-phishing and scams are examples. These are as follows:

- ***Pharming***

Pharmers attempt to redirect the URL to a forged site which looks similar to the legitimate one. Once the user gets into the forged site, pharmers can capture the login information the user has provided.

In essence, pharmers direct the user to another bogus website instead of a requested legitimate website; this is done by inserting ‘wicked’ code into a PC or DNS (Domain Name System) server on the Internet. Pharmers either change the host file on a user’s computer or poison the DNS server by exploiting a weaknesses in the DNS software and getting it to accept incorrect information (APWG, 2006; Fox, 2005; Hubbard, 2005; Pandit, 2006; Radcliff, 2005b).

- ***Google phishing***

Attackers have used the Google search engine to assist their attacks by using it to drive users to their fake website. As phishers do not aim to make any legitimate sales, they will design a fake website which will usually attract online users by claiming to sell a product or provide a service at incredibly low prices. In order to carry out the transaction, users have to enter their private details. Once the information is submitted, an error message will usually be displayed, informing the user of a problem which has occurred which results in an unsuccessful transaction. However, the phisher has already gained the disclosed information (Corrons, 2005; Radcliff, 2005b). With Google phishing, phishers do not have to contact the potential victims; the online users themselves will search for the phishing site by using the search engine which might direct them to a list of websites, some of which are illegitimate (Radcliff, 2005b).

- ***Wi-phishing***

Phishers may use wireless technology and Bluetooth facilities to carry out their crime. This could be done by setting up a wi-fi network in public places that looks like the legitimate networks at designated hotspots in order to trick the user of a wireless broadband connection. Wi-phishing could thus harvest the user’s personal information (Der Hovanesian, 2005; Radcliff, 2005b).

- ***Vishing***

Vishing is a criminal attack over the telephone system to gain access to private information from the users of the system; it abuses user trust in landline telephone

services. Banking clients were targeted by vishing and the first reported incident was in April 2006 (Patterson, 2006; Sausner, 2006). The attackers sent out an e-mail message in bulk, alerting the user to a security risk and asking the potential victim to phone the bank's call centre to resolve the matter. Once the victims called the number given in the e-mail, they were asked to verify bank details, such as bank account numbers and PINs through an automated system set up by the phisher (Patterson, 2006; Sausner, 2006).

- ***SMiShing***

This phishing technique attacks cell phone users; it was identified in September 2006 (Hickey, 2006). The attacker uses the technology of the cellular short message service (SMS) to steal the victim's identity. Phishers capture the required information by sending a misleading SMS to victims asking them to disclose it. The deceptive SMS may refer the victim to visit a fraudulent web site to disclose the information; sometimes the victim is encouraged to download a program that is actually a Trojan horse which allows the hacker to have control of the victim's cellular phone (Hickey, 2006).

- ***Phishing scams***

This is a type of phishing which targets Internet users, where phishers send a deceptive e-mail to the user, posing as a trusted and legitimate entity, but attempting to trick the victim to reveal sensitive information or private information such as username, password and account number. Misleading phishing scams attacks are one of the most successful and common methods of identity theft (Emigh, 2005; Ollmann, 2004).

Popular companies such as PayPal or eBay are frequent targets. For example, e-mails apparently from eBay will claim that the user's account will be cancelled unless the user updates the credit card information in a website which looks identical to the legitimate organisation's site, but which is relatively simple to create by mimicking the HTML code. By using the details, phishers will consequently be able to commit identity theft and possibly carry out a financial fraud (Abad, 2005). However, phishing e-mail messages often include misspellings and poor use of grammar, threats and exaggerations which may help to detect them since phishers are often not native English speakers and lack expertise in the English language (Butler, 2007; Dhamija et al., 2006; Abad, 2005; Butler, 2005; Emigh, 2005; ActivCard, 2004).

- ***Spear phishing***

Usually phishing scams are designed to steal information from individuals in general, whereas, in spear phishing scams, the target is highly specific individuals or groups. Instead of sending a huge volume of e-mails to large numbers of people, a spear phishing attack is usually to gain access to a specific organisation's system (Microsoft, 2006). Spear phishing can be carried out by email or telephone, the phishers appearing as legitimate to the victims. The attack uses authority to commit the crime by impersonating a communication from HR (Human Resources), the manager or any other authoritative figure. It might require the victims to give their user names or passwords or it might contain malicious software such as a Trojan horse or virus (Der Hovanesian, 2005; Pandit, 2006; Radcliff, 2005a, 2005b).

However, this research will not cover all the possible phishing techniques currently employed due to the time and resource constraints of the research. It will focus only on e-mail phishing because it is a relatively more common attack with e-mail being considered as a common communication channel used today. E-mail phishing involves phishing through e-mail (i.e. phishing scams and spear phishing scams).

2.4 Vulnerability to Phishing

Many studies have shown that phishing can be successful in misleading victims (Dhamija et al., 2006; Gartner, 2005; Goldsborough, 2004; Ollmann, 2004; Tsai, 2005), though Gartner (2005) shows only a small percentage of victims (between 3 to 5 per cent) provide phishers with their personal and confidential information. Attackers find phishing a valuable and successful operation because, even though most receivers have no previous transactions with the organisation named in the phishing e-mail, they can still fall prey to the attack. Furthermore, if many e-mails are sent, there will inevitably be a few receivers for whom the named organisation is valid and so they are more likely to become victims of the attack (Sophos, 2005).

There is a shortage of literature on understanding users' vulnerability to phishing from their behaviour (Downs et al., 2007). Jagatic et al. (2006) and Robila and Ragucci

(2006) state that user's susceptibility to phishing attacks would increase when phishing attacks include user perspective information (e.g. name and date of birth). Forte (2009) concludes that people are more vulnerable to phishing e-mails that appear to be from organisations or other sources with which they have a relationship and they are less likely to query their genuineness. Creating a phishing website requires simple IT skills, using simple web design programs to replicate the original one. Phishers can then upload the site either in a web space with a similar name to the original or in the existing site itself by using known vulnerabilities in web applications. However, in the former case, the country's local authority might not allow a domain to be registered with a name similar to that of an institute such as a bank, so phishers usually choose service providers in Eastern Europe or Southeast Asia, where there are few or no controls involved in the opening of a new domain (Forte, 2009). The success of attack relies on slow reaction time by the authorities so that the crime is carried out before the web site is blocked. The second approach requires precise skills in vulnerability testing which can be possible with the availability of the application source code (Forte, 2009).

Downs et al. (2006) investigated why people are vulnerable to phishing based on interviews with 20 non-computer experts. The research concludes that people are susceptible to phishing due to a lack of connection between knowledge of the risk and strategies of phishing prevention or the supposed vulnerabilities. It also concludes that even knowledgeable participants were not well protected against phishing. Tout and Hafner (2009) agree, stating that vulnerability to phishing has two main elements: lack of user knowledge in distinguishing phishing e-mails and the simplicity of conducting phishing and deception as a legitimate entity.

Wardman et al. (2009) identified a technological method for investigating frequent vulnerabilities in websites which could be exploited by phishers to help Webmasters and their hosting companies to protect their servers from possible associated risks. However, details of the method are not available and the method is still being developed, so further evaluation is required to prove the effectiveness of such a method. Forte (2009) shows that there are many factors which affect the success of a phishing attack, including the reliability of the legitimate site being attacked, the content of the

e-mail message and the final user's critical analysis capability and IT skills. Also, he proposes the need to enhance people's protection knowledge after illustrating the susceptibility of people to phishing attacks. He concluded that people are likely to be vulnerable to phishing e-mails which appear to be sent from their banks because they are less likely to question their genuineness. He adds that people are more persuaded by phishers who exploit their social engineering ability. Some phishers use in-session attacks, taking advantage of tabbed browsing where the phisher can trick the user by opening pop-up windows with fraudulent sites while the user is logged in to the online banking site and by informing the user that the session has expired and that they need to log in again (Forte, 2009).

Phishers are continuously improving and developing new phishing techniques to conceal their attacks (Honeynet Project and Research Alliance, 2005; APWG, 2006), leading to a dramatic increase in the complexity of the attacks (APWG, 2006; Jakobsson and Ratkiewicz, 2006). They are improving and inventing new ways and tricks to avoid the anti-phishing measures (i.e. anti-phishing software or anti-spam filters) (Symantec, 2006). For example, one method is to avoid specific words in the e-mail message that the anti-phishing measures will normally search for to identify the phishing e-mails (Symantec, 2006).

2.4.1 Clever tricks used by phishers

E-mail phishing has three aspects: the sender 'phisher', the receiver 'victim' and the e-mail message which may lead to a deceptive web site where the receiver can be lured to reveal private information. Phishers cleverly use these aspects and applies technical and social engineering tricks to persuade and trick victims to disclose their confidential information. The following illustrates how this is done:

2.4.1.1 Sender 'phisher'

Phishers establish a valid e-mail account either by creating an e-mail address from the web or an ad hoc account which is more persuasive, since the phisher may add the name of the defrauded target into the account name (Forte, 2009) where then phishers masquerade as figures of authority in possession of confidential information by getting

them to believe the validity of the e-mail (Honeynet Project and Research Alliance, 2005).

2.4.1.2 Receiver ‘victim’

To deliver the phishing e-mails, phishers need to have a valid e-mail addresses. Creating a mailing list could be easily done by either searching for valid e-mail addresses from the Internet, purchasing valid e-mail addresses on the cyber black market or using programs to extract e-mail addresses from searches within websites known as ‘crawlers’ (Forte, 2009; Bielski, 2004). Therefore Forte (2009) discourages users from providing explicit references to their mailbox in discussion forums. Nagy and Pecho (2009) discuss the risk of exploitation of social network sites by phishers because of irresponsible user behaviour and the openness of such sites, stating the requirement for enhancing users’ security awareness and pointing to people’s willingness to reveal their profiles. Once the e-mail addresses are identified, phishers usually use spam tools to send the e-mail to numerous victims (Bielski, 2004).

2.4.1.3 E-mail message

As mentioned earlier, phishers design the e-mail message carefully so that it appears to be from a legitimate source in order to trick the receiver into divulging confidential information (Bielski, 2004). Phishers usually fool receivers into disclosing their personal data either in the replica of a login page in the e-mail message, the message directs the receiver to a fraudulent web site to reveal the information or even direct the victim to communicate through an online or an offline communication such as e-mail, SMS or phone (Emigh, 2005).

Phishers may play on people’s emotions, exploiting their goodwill to commit their crime such as by calling for donations and help. They can employ intelligent visual tricks to deceive the victim (Dhamija et al., 2006) and make it difficult to identify phishing. Usually the message appears to be innocent, such as a request from Client Support for the user to update their records or to resolve a problem in his or her account and it generally conveys a sense of urgency such as requesting the victim to provide the

private information immediately. For example, the phishers may warn the receiver that a late response would result in a penalty such as closure of the account or loss of an opportunity. In addition, phishers may use the sense of surprise such as informing the receiver about winning a prize and then requesting some private information (Dhamija et al., 2006).

Well known online brands are the main targets of phishers using deceptive websites. Research by APWG (2006) in August 2006 shows that 148 brands were forged by phishing and 92.6 per cent of them were financial services businesses. Phishers attempt to convince the victim that the fake website is a legitimate one by different means, such as hiding the address in an embedded hyperlink, using URL links similar to the URL of the original website and cloaking the URL by showing part of it in the address bar and hiding other parts to conceal the real destination host (APWG, 2006).

In addition, several researchers have stated that phishers also exploit the users' faith in the security indicators to deceive users by applying visual tricks to appear to users as trusted security indicators (Herzberg, 2008; Dhamija et al., 2006; Herzberg and Jbara, 2004). Phishers can fake the security padlock icon by including it as an image in the content of the site. This means, therefore, that the appearance of a lock icon does not necessarily mean that the website is secured (Herzberg, 2008). In addition, phishers can employ visual tricks to deceive the user in some browsers by removing the location bar and replacing it with a fake location bar to prevent users from seeing the URL, one of the main security indicators (Felten et al., 1997; Ye et al., 2002; 2005). Most users will not detect changes in the address bar as it happens rapidly (Herzberg, 2008). Also, there might be a chance that the fake site might hold a high assurance security certificate (Franco, 2005). They are able to establish a fraudulent site with SSL certificate that is faked through the use of the vulnerability in the MD5 hashing algorithm which is a widely used cryptographic function (Sotirov et al., 2008; Stray, 2008). According to US-CERT of the U.S Department of Homeland Security, MD5 is considered as cryptographically broken (US-CERT, 2008) and a move to the more robust Secure Hash Algorithm (the SHA) is therefore suggested (NIST, 2008).

Many phishing sites are hosted at any single IP address for only a short period. In August 2006, APWG (2006) reported that phishing sites were active for an average of 4.5 days and a maximum of 31 days. Since the hosting time is significant for a phisher's profit cycle, phishers aim to increase their hosting life-time by using fast-flux service networks which is a DNS (Domain Name System) technique used to hide phishing and malware delivery sites by allowing their sites to change rapidly (Konte, 2009; ICANN SSAC, 2008).

2.4.2 Behaviour of users

Larkin (2009) concludes that people are not able to protect themselves against hackers from stealing their confidential information. However, he states that identifying the theft earlier can help in recovering the possible damage which could occur to victims, for example by stopping a transaction.

Although phishing e-mails offer little or no meaning of trust, users will still trust them (Downs et al., 2006; Jakobsson and Ratkiewicz, 2006). Kumaraguru et al. (2007) point out the users' susceptibility to phishing in the sensitive trust decisions made during their online interaction. Psychologists claim that stress could cause people to make incorrect decisions (Keinan, 1987) since they depend on patterns (i.e. what the e-mail looks like) instead of related details (Kumaraguru et al., 2007; Robila et al., 2006; Sheng et al., 2007).

Generally, users are more vulnerable to phishing attacks if they do not employ appropriate security practices (Butler, 2007). The Honeynet Project and Research Alliance (2005) concluded that home users or small businesses are more targeted by phishers because they are expected to have less security practice in place. According to the Internet Security Threat Report, home users were subject to 86 per cent of all targeted attacks between January and June 2006 (Symantec, 2006).

Many studies have discussed the gullibility of people and to what extent people will disclose their private information. A study by the UK Treasury Department inspectors shows that one-third of the Internal Revenue Service (IRS) employees gave away their

login and password to auditors who called, pretending to be computer technicians (Dalrymple, 2006). Other studies have provided a certain shock value, such as reported in two highly publicised books. Chocolate for passwords by Wagner (2004) shows more than 70% of the subjects would reveal their password in exchange for a piece of chocolate and 79% would give away information that could be used to steal their identities. The Paris Hilton Hack confirms this, where Krebs (2005) writes about hackers who tricked employees to reveal secret information.

Consumers are unaware of the phishing threat and of the risk of revealing their private information. In the 2005, Infosecurity Europe event, research indicated that nine out of ten individuals are susceptible to identity theft when 180 out of 200 people asked to disclose their personal details responded without question (Clarkson, 2005).

Butler (2007) states that human behaviour is difficult to predict. Therefore it is essential to study user behaviour regarding phishing attacks to assist in the development of an effective solution to combat them. Therefore, laboratory and real experiments were carried out to assess the user's ability to differentiate phishing attempts. Generally, most published experiments to assess the user ability to distinguish phishing websites employing different attack methods show a high rate of user failure (more than 50%) (Herzberg, 2008).

Downs et al. (2007) discuss the need to gain knowledge of user behaviour associated with phishing to provide an effective anti-phishing tool. From a laboratory experiment based on a survey role play with 232 computer users, they investigated the aspects associated with making users susceptible to phishing attacks. Their conclusion was that users who have knowledge and experience in recognising the web environment, including the ability to inspect and differentiate phishing URLs from legitimate ones, are less vulnerable to fall victims to phishing, and will not give false positive responses to legitimate e-mails. Their findings supposed that the severity of the consequences of phishing is likely to increase false positives.

Moreover, some researchers conclude that the ability to distinguish legitimate sites was found to be complicated. Many participants tend to ignore the passive security

indicators and warnings presented by anti-phishing toolbars and depend on the website content to distinguish phishing attempts (Wu et al., 2006; Downs et al., 2007). Users were found to be unfamiliar with phishing attacks and security warnings; some did not detect them or ignored warning signals even though they understood them (Wu et al., 2006). Some research explored user ignorance of toolbar warnings even if they were precise (Wu et al., 2006; Downs et al., 2007).

Research at Harvard University in 2006 showed that lack of awareness of phishing threats and lack of attention to security warnings were the main causes of successful phishing attacks (Dhamija et al., 2006). In the Harvard study, 22 participants were asked to spot the fake phishing websites in the 20 sites given. The result shows that failure to distinguish fake websites happened about 40% of the time and more than 90% of the participants were deceived by effective and devious fake web sites. In addition, the study concluded that 23% of participants ignored all security indications in the web browser (Dhamija et al., 2006).

The majority of web browsers (e.g. Mozilla Firefox and Internet Explorer) provide warnings for known black-listed phishing sites and support the basic security indicators, which are as follows (Herzberg, 2008):

- The URL of the current page and classification of the protocol used to enter the site indicates whether it is an unprotected web page (the URL begins with http) or protected with SSL/TLS (the URL begins with https).
- In SSL/TLS-protected pages, a padlock icon should be shown either on the status area or near the location bar.
- The security certificate of the website is shown by double-clicking on the padlock icon.

Both the SSL (Secure Socket Layer) and the TLS (Transport Layer Security) are sophisticated public-key cryptographic protocols which provide secure connection between the client and server. These protocols provide a flexible encryption method available at the time of the secure transaction. They do not necessitate preconfigured secret keys between the client and server before the connection is initiated, which makes them suitable for Web-based secure services. Therefore, the SSL and TLS are applied in most web pages that contain sensitive traffic such as login web pages (Herzberg, 2008).

The SSL/TLS protocols are supported by most web browsers and servers (Dierks and Rescorla, 2006; Rescorla, 2000). The use of SLL/TLS will protect the transfer of confidential traffic against ‘man-in-the-middle’ attackers who attempt to get access to the traffic between the victim and the legitimate site to make them believe that they are connected and communicating with the legitimate site while they are actually connected to the attacker (Herzberg, 2008).

However, several experiments and studies show that most users do not recognise or understand properly the basic security indicators since they are not very visible in current popular browsers (Herzberg, 2009; Dhamija et al., 2006; Herzberg and Jbara, 2004) and Herzberg (2008) also proves that the basic indicators do not offer adequate security. Moreover, research shows that most users are not familiar with the trust certificate authorities such as VeriSign and GeoTrust (Herzberg and Jbara, 2004).

In addition to the user’s failure to notice the basic security indicators, they are also confused since many sensitive websites do not employ SSL/TLS or they encrypt only the password to reduce the overhead network traffic of SSL/TLS in both the handshake phase and the data transfer phase (Apostolopoulos et al., 1999). Some sites show a padlock even in an unprotected login page, giving an unfounded trust in the padlock image itself (Herzberg, 2008; 2009).

Although many login pages are secured using SSL/TLS, those that use SSL/TLS only to protect the submitted password after submission are vulnerable to a ‘man-in-the-middle’ attack where the submitted information would be held by the attacker instead of transferring it securely to the legitimate server (Herzberg, 2008; 2009). Since the attacker could use visual tricks to deceive the victim by designing a login webpage which looks almost identical to the legitimate one, it would be difficult for users to distinguish these sorts of fake websites. This would require users to examine the HTML code of the web pages as the normal browser interface could not distinguish it (Herzberg, 2008). However, it is not feasible to expect users to examine the HTML code. Some legitimate websites fail by not invoking a genuine secure connection in their webpages, but including an image of a padlock displayed in the page itself. The

Chase.com home page was an example of such a common sensitive login page with a padlock displayed in an unprotected webpage (Herzberg, 2008), however, this has recently been corrected. This leads to confusion for users as there is no difference between the original site and the phishing one especially that phishers could fake the security indicators to trick users (Herzberg, 2008; Dhamija et al., 2006; Herzberg and Jbara, 2004).

There is some confusion over the reliability of experimental results from tests carried out in real life compared with those in the laboratory. Whitten and Tygar (1999) claim that the majority of experiments published are carried out in lab conditions and the result of such experiments might not be reliable since participants will act in a different way during the experiment compared to real life. On the other hand, Downs et al. (2007) disagree and claim that a laboratory experiment based on a survey role play exercise shows a consistent means to assess behavioural response to phishing. They argue that there were no signs of behavioural difference between the lab experiment and real-world test. Herzberg (2008) and Schechter et al. (2007) state that some people may be more cautious in real life as their security preparedness increases when using their real account and because of the possible real consequences faced when falling victim to phishing. Other participants might be more cautious in a lab environment as the exercise is carried out with the awareness of participants who would therefore concentrate more in identifying the indicators than they would in real life. Consequently, Herzberg (2008) suggests carrying out real life experiments or what is called 'penetration tests' rather than lab experiments to have a better understanding of participant behaviour during day-to-day online activity.

However, the reported phishing laboratory studies do not present a large population of e-mail users since the authors found difficulties in motivating a large number of people to participate. Also, a relatively small number of e-mails was inspected in the experiment; for example Downs et al. (2007) applied only 5 e-mails in their laboratory experiment. Large field studies can be more effective but they are less controlled than lab studies with less information available on participants' demographics. Examples of such field studies are given by Jagatic et al. (2006), Ferguson (2005) and New York

State (2005). Some researchers who studied user vulnerability, found that there is no relationship between people's demographics (e.g. age, sex, previous experience, number of hours spent at the computer) and their vulnerability to phishing (Donovan et al., 1999; Dhamija and Tygar, 2005; Dhamija et al., 2006) Conversely, Downs et al. (2007) found that there is a relation between users' susceptibility to phishing and the knowledge and experience they gain on phishing, leading to enhanced awareness. Aston (2009) discovered that, in particular, older males were the common victims; also, education on online scams was found to have a major effect on susceptibility to fall victim to such attacks. Nevertheless, the examination process was based only on "money mule" incidents where scammers steal money from victims and transfer it from one country to another to avoid tracking. It would be valuable to broaden the examination to online attacks and phishing in particular. Aston's paper does not illustrate why older males are common victims, therefore, there is a need for further investigation to see whether this is true.

2.4.3 Summary of Vulnerabilities

This section demonstrates the clever technical and social engineering tricks used by phishers and from this it can be concluded that technical solutions alone cannot be relied on to protect the user and that it would take a high level of user awareness to detect all these tricks. In addition, the behaviour of users shows a high susceptibility to phishing because of lack of awareness on phishing tricks, their consequences, and how to protect against phishing, and people are unable to recognise the security indicators to watch out for and they are gullable even when they do. There is a lot of research which discusses people's vulnerability to phishing based on reality or laboratory experiments which assess people's ability to recognise phishing attempts from legitimate e-mails. Most experiments concluded with a few findings concerning people's ability to recognise phishing sites but they do not identify the possible factors which make people susceptible to phishing. There might be factors such as cultural, country-specific and personal factors which none of the studies has investigated. Therefore, this suggests there is a need for research that focuses on studying user vulnerability to e-mail phishing from a broader angle, covering all of the associated factors affecting users' response to phishing by applying both reality and laboratory tests with a representative

sample of e-mail users. Investigating what makes people susceptible to e-mail phishing will assist in defining a solution to the phishing problem.

Since there is little published material on whether there is relation between susceptibility to phishing and the demography of users, further investigation on this matter is required. There are a number of indications that awareness and education is a key method in reducing people's susceptibility to phishing. However, this also needs further investigation.

2.5 Anti-Phishing Solutions

Phishing is a complex phenomenon, therefore there is no single solution to impede phishing (Emigh, 2005; Ollmann, 2004). The risk of phishing may be reduced in the long-term through applying suitable technology and educating the consumer of the phishing threat (Emigh, 2005). Many solutions have been proposed to reduce the risk of phishing, some are technical solutions and others are non-technical, based on best practices, awareness and education. Since e-mail phishing attacks are no longer a purely technical activity, technical controls alone are no longer enough to defend against them. A holistic view of security is required which integrates technology and people aspects.

2.5.1 Technical Solutions

There are many technical solutions which detect and alert users to an attack such as anti-virus software (e.g. McAfee, Symantec and AVG anti-virus), spam filters and phishing detection tools. Phishing sites are detected by using either URL filtering or by checking the URL with the reported blacklisted phishing URLs. However, it is not easy to manage such a blacklist with an increasing number of incidents, for example phishing reports have increased by 167% from July 2005 to July 2007 (APWG, 2007). Another possibility is to use a heuristics-based approach which uses algorithms to discriminate phishing sites based on users' experience and other heuristics. Although many researchers (Kumar, 2005; Tally et al., 2004; Van der Merwe, 2005) have investigated such a method, heuristics are found to be unreliable for detection in practice, since the

methods are based on defining the likelihood of a site being a phishing site, which Zhang et al. (2007) shows might be underestimated.

Hara et al. (2009) discuss phishing detection, including the blacklist and the heuristics-based approach, based on visual similarity among phishing sites and legitimate ones and keywords used in the Website. This research points out the weakness of such solutions as they can be bypassed when the process is recognised. The approach achieves an 80% detection rate (Hara et al., 2009). Chen et al. (2009) and Xin et al. (2009) provide a novel and more accurate algorithm for phishing web site detection based on the image of the suspicious websites. Other research has defined some algorithms based on a broad investigation of phishing schemes. This shows a detection rate of 80% and an accuracy of 99%, pointing to some risks of phishing being missed by the algorithm and, therefore, there is still a reliance on users taking the right decisions (Yu et al., 2009).

An interesting and ongoing research approach is based on machine-learning which involves advanced detection that enables a computer to learn by itself from the user's behaviour (Pan and Ding, 2006; Fette et al., 2007; Basnet et al., 2008). Miyamoto et al. (2009) provide an assessment of nine machine learning-based methods for phishing site detection for improving accuracy. Liping et al. (2009) identify the intelligence of phishers to bypass the available anti-phishing solutions and propose a reliable categoriser to distinguish phishing e-mails using hybrid features and a machine-learning algorithm. Other research by Awang (2009) introduces Trusted Computing (TC) to improve protection by using the transitive properties of trust. With such a solution the computer will be consistently forced to behave in expected ways (Mitchell, 2005).

However, there are many problems associated with TC, such as privacy, the threat of unwanted surveillance and legal concerns including copyright, anti-trust law and data privacy law (Anderson, 1993). Aburrous et al. (2009) propose a clever, flexible and effective real-time phishing-detecting e-banking based on fuzzy logic and data mining algorithms. However, none of these algorithms are 100% effective.

Several researchers have recognised and examined the use of fast flux in malicious sites and producers have proposed a flux-detection mechanism (Honeynet Project, 2007; Konte et al., 2009; Nazario and Holz, 2008; Holz et al., 2008; Caglayan et al., 2009). McGrath et al. (2009) show the possibility of defending against phishing sites by using fast flux to determine several short-lived IP addresses. Research by Caglayan et al. (2009) studied fast flux service networks (FFSNs) in real time over a short window of minutes using active and passive DNS monitoring and this has provided an effective detection process instead of observing fast flux over a long period as usually done in previous research. Other researchers, such as Zhang et al. (2009), investigated phishing groups by means of data mining techniques to explore the image attachments of spam e-mails by extracting the visual features from spam images and using an unsupervised clustering algorithm to group similar spam images visually into clusters (Chen and Zhang et al., 2009). Furthermore, Liping et al. (2009) provide a novel scheme to cluster phishing e-mails automatically to identify the origin of phishing attacks in order to trace the phishers. However, although the scheme shows effective results, there is still scope for development.

There are many available research projects which work on producing effective solutions to combat the phishing threat. Pal and Atighetchi (2009) introduced the PhishBouncer project with the Symantec Research Lab (SRL) to defend against phishing by investigating the mechanisms to intercept and inspect http and https traffic to distinguish and block phishing sites. The method shows its effectiveness in opening issues for possible server exploitation. However, this research will not help to overcome other types of phishing.

The Honeypot project is another example of a commonly used anti-phishing tool for fast detection and blocking of phishing e-mails based on analysis of collected phishing e-mails and phishers' activities. Shujun and Schmitz (2009) focus on examining users' behaviour while interacting with an e-banking system to help in defending against phishing attacks such as pharming and malware. This research has detected phishing to some extent, however, more evaluation is required to measure its effectiveness in protecting against phishing in other institutions. In addition, Botnet, which involves a

number of computers which have been set up to forward phishing, spam or viruses to other computers on the Internet, has been an attractive research topic related to cyber-crime deterrence including phishing, which applies various detection techniques (Feily et al., 2009).

The majority of research focuses on protecting users from disclosing their passwords to phishing sites by use of various phishing detection tools. However, Knickerbocker et al. (2009) proposed the Humboldt system which aims to interrupt phishers by submitting poisonous fake data into phishing web sites totally different from the actual data. The system has efficiently disrupted the phishing process with practically little overhead.

According to Herzberg (2008; 2009), since basic security indicators are not effective as they depends on users noticing and understanding them, enhanced indicators are needed to assist users to detect phishing sites. Therefore, many researchers have focussed on developing an enhanced toolbar for the Mozilla web browser, called TrustBar, to aid users in better recognition of phishing sites (Ye et al., 2002; Dhamija and Tygar, 2005; Herzberg and Gbara, 2004). The TrustBar is a toolbar providing three enhanced indicators: The *Certificate derived indicator*, *SSL/TLS indicator* and the *User customised indicator*, aiming to improve security and identification for the browser (see Figure 2.1). The Internet Explorer browser (version 7), PassPet and WebWallet (Wu, 2006; Wu et al., 2006; Yee and Sitaker, 2006) are other available similar tools. However, such tools still rely on the user's ability to make the correct trust decision from the presented indicators which are made useable and clear with the enhanced toolbar (Sheng et al., 2007).



Figure 2.1: Security indicators in Mozilla Firefox trust bar (Herzberg, 2008)

The three enhanced indicators are explained below (Herzberg, 2008):

1. SSL/TLS indicator

This provides the user with a clear visual indication of whether the website is secured. For a secured site, the padlock would be displayed in the trustbar while unsecured sites would have a crossed-out padlock.

2. Certificate-derived indicator

This shows the names and/or logos of the organisation and issuer as recognised from the SSL/TLS certificate. Some certificates would display the domain in the organisation field. This is usually because most issued SSL certificates are based on only the validation of the domain name, which is not secure against poison DNS or ‘man-in-the-middle’ attackers since it is carried out by sending packets to IP addresses of the domain listed in the DNS. It is, therefore, important to recognise and inspect the certificate authority carefully.

3. User-customised indicators

User-customised indicators help users to defend against phishing sites which require inputting of private information such as passwords. These indicators are unique to each user and are either randomly selected from the system or chosen by the user. It could be an image, a photograph or just a couple of words. The identifier would be displayed on the web page (Gasparini and Gotlieb, 2003) to avoid phishing attacks, as attackers would not know the unique identifier chosen by the user or even provided by the legitimate website. Even if the attacker tries to impersonate the user, the site would require an authentication before sending the identifiers, e.g. using cookies or the IP address. However, users need to select a unique identifier which is not easily predictable by attackers.

An example of such a user-customised indicator is the Yahoo sign-in seal which assists users to distinguish a genuine Yahoo login page, as shown in Figure 2.2. Even if a phisher knows or guesses the user’s ID or other personal information, they cannot discover the user’s sign-in seal since the sign-in seal is correlated to the user’s computer and not to the user’s ID. When a user finds that there is no sign-in seal or the seal has changed (e.g. change in colour, photo and text), they know it is a phishing site. Nevertheless, many browser-based tools are not fully reliable in detecting phishing sites (O’Brien, 2005; Downs et al., 2007; Zhang et al., 2007).

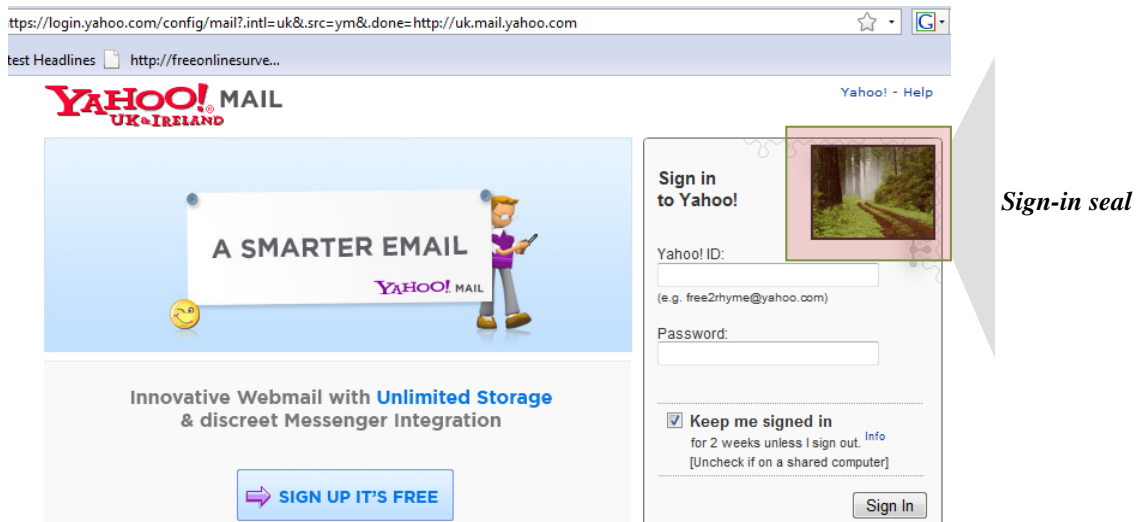


Figure 2.2: Yahoo sign-in seal

2.5.1.1 Summary of Technological Solutions

In conclusion, there are many commercial technological solutions available to fight against phishing. However, it remains an arms' race, with phishers using complicated techniques. Even e-mail-based automated detection tools have limitations (Fette and Tomasic, 2006). A study by Zhang et al. (2007) examined 10 anti-phishing tools: only one identified 90% of detections but it also inaccurately distinguished 42%.

With phishing being complicated and continuously developing, available anti-phishing tools do not have the ability to protect against all types of phishing attacks (Zhang et al., 2007). Although available technological solutions assist in reducing the risk of phishing, they still do not provide an accurate detection of phishing attacks (Dodge, 2006; Dodge et al., 2007). Downs et al. (2007) explore the fact that anti-phishing tools would never give full protection against false detections either for phishing or legitimate e-mails, which are described as false negative and false positive, respectively; therefore users should make their decisions based on their knowledge of phishing and how to protect against it. Since users' behaviour is unpredictable, there is no current technological protective solution that can diminish the risk associated with user behaviour (Dodge et al., 2007). Ultimately, all anti-phishing solutions require knowledge of users' behavioural response to phishing to develop an effective solution, whether through best-practices or anti-phishing tools or education. Therefore, understanding what makes

people fall prey to phishing would have a direct implication for all anti-phishing solutions, particularly awareness and education (Kumaraguru et al., 2007; Sheng et al., 2007). This shows the importance and the need for further research to investigate user vulnerability to the phishing threat since it assists in developing effective anti-phishing solutions and enhancing their performance.

2.5.2 Non-technical (Awareness) Solutions

Although protecting the infrastructure by security controls and technologies will reduce the effect of phishing, protection at the user level needs to be the main defence against phishing since users are the most vulnerable (Ollmann, 2004; Downs et al., 2007). Many researchers, especially those who study vulnerability to phishing, conclude there is a need to enhance user awareness on the phishing threat to improve users' protection level against phishing attacks (Dhamija et al., 2006; Wu et al., 2006; Downs et al., 2007; Kumaraguru et al., 2007; Herzberg, 2009). Forte (2009) concludes that it is hard to implement technological countermeasures to avoid phishing due to the nature of such attacks where they aim to work directly on the users to attain their goal. Therefore, it is crucial to make users aware of the need to verify the legitimacy of e-mails and phone calls received. There is much literature which discusses phishing awareness; some propose recommendations, advice or what is called "best practices" for users to follow and some focus on putting these best practices and advice into useful and effective educational material to train users on how to defend against phishing attacks. These are described in detail in the following sections.

2.5.2.1 Recommendations and Best Practices

Some research provides useful recommendations on best practices and countermeasures to avoid phishing. Winder (2009) mainly advises leaving suspicious sites as soon as possible and reporting the incident to the responsible organisation which should be ready to help in reducing the impact of being phished. Forte (2009) analyses the procedures of a phishing attack, especially in creating the phishing site, and presents some countermeasures to avoid being attacked. Tally et al. (2006) and Tally (2009) focus on developing a real-time phishing data collection, validation, broadcasting and a global archival system to assist in investigating the scope and characteristics of phishing

attacks and the potential victims. This project, called ‘Phisherman’, recommended and showed the value of having a single database of phishing incidents to help organisations, researchers and law enforcement organisations to study phishing techniques and find solutions for avoiding them. However, it is hard to persuade all organisations to be involved in such projects, especially banks, where the records of incidents are confidential. Most organisations keep their records private. Furthermore studying phishing incidents is difficult, requiring extensive in-depth analysis to understand phishers’ tactics. Wu et al. (2006) propose the need for educating users on best practices to avoid phishing.

Butler (2007) aims to educate the Internet consumer on the threat of phishing by proposing a framework of anti-phishing measures. He provides an effective review of phishing techniques and proposes useful proactive measures to prevent phishing and some remedial actions to reduce the possible negative consequences which might be suffered from successful phishing attacks. He also identifies the need for proper anti-phishing education and measures to help to protect online users from the e-mail phishing threat. Overall, however, the proposed pieces of advice in most research has been found to be sparse and obvious to the user, and some publications merely repeat previous literature and articles available on the Internet.

2.5.2.1.1 Recommendations on How to Spot Phishing

Literature which proposes best practices and recommendations defines many clues and offers advice for users to enhance their ability to combat phishing. The following is a summary of best practices gathered from the literature which demonstrates how to avoid e-mail phishing attempts.

1. Users should look out for the following email features:
 - Usually, legitimate institutions will not seek to acquire confidential information by e-mail because it is relatively insecure (ActivCard, 2004; Butler, 2007; Dhamija et al, 2006).
 - An e-mail message addressed to “Dear valued customer” is likely to be a phishing e-mail because the message was sent without addressing the receiver and usually

private e-mails requiring confidential information address the consumer by name (Emigh, 2005; Dhamija et al, 2006).

- Reading the e-mail message carefully is very important; discovery of grammatical or spelling mistakes in the message is usually an indication that the e-mail is not official because it would be checked for language correctness (ActivCard, 2004; Dhamija et al, 2006).
 - Phishing emails often appeal to a user's better nature and moral obligation to launch an attack. For example, in the case of a natural disaster such as an earthquake, phishers will exploit people's kindness by calling for donations. This could be done by setting up a bogus website claiming to be raising funds for disaster relief. Examples of such phishing were noticed after the following disasters: the London terrorist bombings in July 2005 (Technology News Daily, 2005), the tsunami disaster in the Pacific in December 2004 (Vecchiato, 2005) and the hurricane Katrina disaster which hit the south-eastern coast of the USA in August 2005 (American Red Cross, 2005). Research has projected that about 50% of funds raised yearly for donations and disaster relief are actually going to phishing fraudsters (Vecchiato, 2005).
 - Another emotion used by phishers is the sense of surprise, when a too-good-to-be-true offer is made for bargains and the possibility of winning a superior reward. For example, in 2006, for the FIFA World Cup, a phishing e-mail offered cheaper online tickets for this worldwide event (SurfControl, n.d.). Unfortunately, too-good-to-be-true offers are normally precisely what the name implies.
 - Phishing emails can employ urgency and intimidation to get victims to respond faster without thinking. An example of such a phishing scheme are e-mails requesting a tax refund, 105 of which, originating from 27 different countries, have been identified by the Internal Revenue Service (IRS), the US government agency responsible for tax gathering and enforcement. The e-mails claimed to be from the IRS and requested the taxpayers to provide their bank account information in order to pay their taxes urgently or a penalty action would be applied (Dalrymple, 2006; Lank, 2006).
2. Users should look out for the following deceptive website links

- Phishers try to hide the address of the fake website in an embedded hyperlink which makes it difficult for victims to distinguish the actual address (Ollmann, 2004). The true address can be seen in the browser location bar or by a pop up message when hovering over the link.
 - Since many users do not know the actual structure of domain names and will not notice the URL, they are more likely to fall prey to phishing websites. Most phishing web sites use incorrect domain names with a name that does not relate to the organisation that is supposed to be the legitimate site. (Herzberg, 2008).
 - Sometimes the fake URLs contain numeric IP addresses. The Anti-Phishing Working Group (APWG) reported that 36% of phishing attacks contained only the IP address in the URL instead of a host name (APWG, 2006).
 - Other advanced phishers use similar looking URLs to make it difficult for users to distinguish the fake URL at a first glance. This is called a homograph attack (Gabilovich and Gontmakher, 2002). These phishers deliberately attempt to make the illegitimate host name similar to the legitimate host using similar characters in the URL, with only slight changes, thus adding, excluding or swapping letters. The study by APWG (2006) shows that 48% of phishing URLs have similarities with legitimate URLs. Many fake URLs are similar to well known websites such as paypal1.com (with the letter 'L' replaced by the digit '1') created to look like Paypal.com (Bellovin, 2004), likewise the Microsoft web site www.microsoft.com has been faked as www.micosift.com, www.micosoft.com or www.verify-microsoft.com (Microsoft, 2006).
 - Some phishers use 'cloaked' links to hide the genuine destination of a link. As the address bar can display only a finite URL length, phishers use this feature to conceal the true destination host. Phishers use long URLs with the active part placed at the end of the URL to conceal it from the victim (Sophos, 2005).
 - Other tricks would be the use of a 'cloaked' link by inserting the extension of the URL after the @ symbol. When the URL contains the @ symbol, victims have to disregard the characters before the @ symbol and consider only the characters succeeding it (APWG, 2006). For example, the URL www.microsoft.com@phishing.com will not take you to microsoft.com, it will take you to the website phishing.com.
3. Users should look out for the following security indicators for legitimate sites

- If a URL starts with 'https' it means it is protected with SSL/TLS technology (Herzberg and Jbara, 2004)
- A locked padlock icon shown either on the status area or near the location bar shows a secure site. The security certificate of the website is shown by double-clicking on the padlock icon. It is important to ensure that the certificate is trustworthy and assigned for the site and that it is still valid (Herzberg and Jbara, 2004).
- Researchers warn users to pay attention to security alerts such as the ones presented by the browser, operating system and phishing filters (Herzberg and Jbara, 2004).

Generally, the advice is that users should not to respond to suspicious emails or website links and if they have done so, they must react immediately by reporting the incident, cancelling their credit card if their card details has been stolen, changing the information revealed and taking other actions to remedy the possible consequences of falling victim to phishing (Butler, 2007).

Some researchers state that although there is small amount of information available for users on how to spot phishing (Robila and Ragucci, 2006; Emigh, 2005; Merwe et al. 2005) it only involves advice to help identify phishing without embedding education into the approach.

2.5.2.2 Education and Training

Phishing education can be considered to be a promotion of information security awareness. An information security culture has been found to influence behaviour of users (Steyn, 2007). Anti-phishing education has been a main concern of many institutions, including government and private. APWG (2005) and Microsoft (2006) have established phishing awareness sites to help reduce the risk of human incorrect trust decisions on phishing attempts. Most researchers point out the importance and effectiveness of education at the user level to deter phishing (Butler, 2005; Emigh, 2005; Milletary, 2006; Consumer Reports, 2006; Symantec, 2006; Microsoft, 2006; Jagatic et al., 2006; Xin and Qinyu, 2007). Additionally, in May 2006, the Executive Order issued by President Bush stated the US Federal Government's desire to educate the public about the threats of identity theft and on how to protect their personal data (White House, 2006). Online consumers have to be aware of the threats and risks of

identity theft through phishing and should also know how to secure their information from phishers by applying security practices and measures appropriately. They should have the capability to recognise phishing attacks and know how to react to them properly and what to do when they have fallen prey to them. Phishers' capabilities are rising and they are becoming more sophisticated due to the available techniques used to trick online consumers, hence online consumers have to continuously update their security practices and their awareness of phishing threats (Clarkson, 2005; Milletary, 2006).

However, Merwe et al. (2005) claim that education is not discussed in the literature as much as the research into technical prevention and intrusion. Although some security and usability experts state that educating users about security is an inefficient approach to defence (Evers, 2007), other research (Gorling, 2006; Kumaraguru et al., 2007) declares the effectiveness of well designed security education in enhancing knowledge.

Even though there are many available anti-phishing education and training opportunities, they are often ignored by users (Whitten and Tygar, 1999; Kumaraguru et al., 2007). Therefore, there is a need for designing education that will attract users and enhance their knowledge on phishing.

A study by Anton et al.(2004) explores that education on this matter would make users feel more threatened and inhibited from carrying out online activities instead of increasing their protection level (Anandpara et al., 2007). Other researchers (Kumaraguru et al., 2007) claim that teaching users the ability to identify phishing attempts could be done without the need for them to recognise complex security concepts. Downs et al., 2007 propose the need for education that will enhance people's knowledge on phishing rather than warning and intimidating them with the associated risks (Downs et al., 2007). This suggests education should be made simple, understandable and not threatening.

Literature on learning argues that real problem solving activity is required to gain an enhanced learning (Barron et al., 1998; Brown, Collins & Duguid, 1989; Evensen & Hmelo, 2000; Naidu, 2004; Schank & Cleary, 1995; McLellan, 1996). Therefore, more effort should be made in terms of practical training to solve the problem of phishing.

Educational and training material about phishing can be presented in learning sessions, distance learning (e-learning), embedded training, regular learning messages or even through the media. There are several researchers (e.g. Kawakami et al., 2010; Anandpara et al., 2007; Kumaraguru et al., 2007; Sheng et al., 2007) who have studied and implemented phishing awareness through those learning methods by developing different tools such as posters and games, taking account of learning principles. Relevant principles of learning are reviewed in Table 2.1:

Table 2.1: Learning principles

Learning principles	Explanation
Learning-by-doing	This is the fundamental aspect of Adaptive Control of Thought-Rational (ACT-R) theory. It is based on the theory that knowledge is enhanced through practice and experience (Schank et al., 1994; Anderson, 1993).
Immediate feedback	Researchers address the importance and the effectiveness of providing instant feedback throughout the learning process in enhancing users' learning skills (Schmidt and Bjork, 1992).
Contiguity	Mayer (2001) supports the effectiveness of computer aided instruction; words and graphics should be presented alongside the instruction.
Personalisation	This implies using a conversational style rather than a formal style of presenting learning material. Clark and Richard (2002) and Mayer (2001) proved that it enhances learning since people are motivated to understand and learn better in informal conversational learning.
Story-based agents	Agents are characters which assist the user during learning. It was shown by Moreno et al. (2001) that their use enhances learning effectively, especially when offered in a story framework (Mayer, 2001). Learning material that is story-based, using either cartoon or real-life characters to make the learning attractive and interesting, was found to provide more effective learning than a non-story-based condition (Moreno et al., 2001; Maldonado et al., 2005). People learn from stories since managing events in a consequential frame makes them easy to be understood and remembered (Klein, 1999; Mayer, 2001).
Reflection	In applying the reflection principle, it was shown that learning opportunity increases when learners are made to stop and think about the new knowledge gained (Donovan et al., 1999).
Conceptual and procedural	Conceptual and procedural knowledge are knowledge types which both influence learning effectively (Johnson and Koedinger, 2002). Conceptual is the concept knowledge taught to learners to understand the concepts, whereas procedural is knowledge gained from procedures and steps proposed. However, both are important

	to consider when developing educational material.
Motivation	Whitten and Bjor (1977) recommend users to take their time in reading the learning material in order to learn better, this will make it more rewarding. They also suggest actual rewards such as certificates or even money will motivate learners. Motivation was identified as an important factor in the learning phase and Kumaraguru et al. (2007) proved that embedded training users were more inspired than users of regular learning messages.
Knowledge retention	In learning principles, many researchers consider knowledge retention (Rubin and Wenzel, 1996) which reflects the ability of learners to retain the conceptual and procedural knowledge gained from the learning material after a lapse of time. Merrienboer et al. (1997), Kumaraguru et al. (2007) and Sheng et al. (2007) show that those users who were taught how to recognise phishing attempts were better able to remember and distinguish phishing after the training. Few researchers address the retention of knowledge, but Kumaraguru et al. (2007) and Alnajim and Munro (2009) have shown that users involved in embedded training are more able to retain the knowledge they have gained from regular phishing alert messages, seven days after training.

Different anti-phishing training methods and tools, including web-based learning and contextual and embedded training, would assist in enhancing the user's ability to recognise phishing (eBay, 2006; FTC, 2006; Sheng et al., 2007). The methods are as follows:

1. Contextual training

This is an experiment based training which, in the context of phishing, would aim to assess users' susceptibility to phishing according to their ability to distinguish phishing attempts. Some researchers who have carried out such training have shown that, at the end of the test, any educational materials given to participants improves their knowledge on the phishing threat (Jagatic et al., 2006; Ferguson, 2005; New York State, 2005). Kumaraguru et al. (2007) applied contextual training with 30 participants and conclude that, after reading the training messages, participants' protection level and ability to distinguish phishing messages did increased considerably.

2. Learning programmes

In learning programmes a broad range of learning material is used and is either distributed to a small population through session training programmes or widely distributed to the public through the media. Some research is based on learning sessions where there was a direct interaction between the trainer and the learners (Sheng et al., 2007; Kumaraguru et al., 2007).

Many researchers have stressed the role of the media in manipulating people's attitude and behaviour and in increasing public awareness in many subjects, which is likely to lead to citizen action (Hedberg et al., 1995; Goddard and Saunders, 2001; Andrews, McLeese and Currant, 1995: 929-930; Burrows, D., 1988, Krugman, 1996; Levy, 1999). However, some researchers argue that the media could be successful in raising public knowledge and awareness of any topic, but they are unlikely to alter public behaviour (Windahl et al., 1992: 102; Rice and Atkin, 1989; Rogers and Storey, 1987; Media Awareness Network, 2005; Spitzer, 1993; Wilson and Wilson, 2001; Wimmer and Dominick, 1991). Lumsdaine (1963), Mielke (1968) and Clark (1994) claim that the media is not efficient for learning. However, some researchers suggest that learning depend on how the issues are presented in the media rather than the media itself (Clark & Solomon, 1986; Kulik, 1985)

3. Learning through game playing

Sheng et al. (2007) presented the development of an online game to teach users how to spot phishing attacks. The game was very effective in enhancing identification of phishing attacks for 60% of the participants in the learning session. Sheng et al., (2007) claim that in comparison with existing online materials, the game was a better way of raising awareness.

Zhang et al. (2007) presented an impressive game which gives users clues on how to recognise phishing from URLs and uses a search engine to prove the legitimacy of the site because the legitimate one will usually be the top result of the search. However, the game does not train users on all ways to spot phishing messages, relying only on enhancing users' ability to recognise phishing from the URL. The evaluation of the game depends only on the scores of users in playing the game (Sheng et al., 2007). Sheng et al. (2007) used learning principles to design the game which proposes the need

for involving training tactics which are goal-oriented, appropriate, interactive and challenging for providing efficient training (Quinn, 2005).

A lot of literature is available on the effectiveness of games for teaching conceptual and procedural knowledge (Anderson et al., 1993; Johnson and Koedinger, 2002; Gee, 2003). Some research in learning principles has found that an interactive teaching environment, such as in games, is one of the most effective training techniques and is extremely inspiring for users, especially if it follows educational game design principles (Gee, 2003; Quinn, 2005; Reppenning and Lewis, 2005).

4. Laboratory tests

Other research by Robila and Ragucci (2006) shows an increased level of awareness and better recognition of phishing attacks for users who took a laboratory-based survey experiment to assess a user's ability to make correct decisions on whether e-mails in the test were genuine or fraudulent. The experiment was held in a learning session on a computing courses and results from test scores and discussions show 82% of phishing e-mails were recognised correctly but, in contrast, more than 50% of attacks for those phishing e-mails using a social engineering perspective were successful

However, legitimate e-mails are relatively less detectable than phishing attempts (Brandt, 2005) and research by Horgan (2005) shows only 52% correct detections of legitimate e-mails. This might lead users to categorise all the e-mails in the lab test as phishing (Brandt, 2005). According to Anandpara et al. (2007), existing online training materials make people more cautious about phishing such that they wrongly identify legitimate e-mails as phishing. Kumaraguru et al., (2007) state that existing online training on phishing tends to give rules but it does not effectively educate users on means of detecting phishing attempts.

5. Embedded training

Research in education shows that training is effective when it is related to real world testing (Anderson and Simon, 1996). Embedded training is an example of such training which teaches users how to recognise phishing in their daily interaction (Kirkley et al., 2003).

There are numerous researchers who have used embedded training where penetration tests were applied to study users' vulnerability to phishing attacks and to teach users to learn from their mistakes (Jagatic et al., 2006; Ferguson, 2005; New York State, 2005). Those studies have shown the effectiveness of the training in raising the user's defence level against phishing compared to the information booklets or standard security notices usually sent to client organisations (Kumaraguru et al., 2007). Several organisations have applied this embedded training method. For example, Loughborough University is one where a phishing e-mail was sent to students requesting their username and password, but once opened, a message appears to alert students to the threat of phishing and informing them that the University would never request student login details through e-mail (see Figure 2.3).

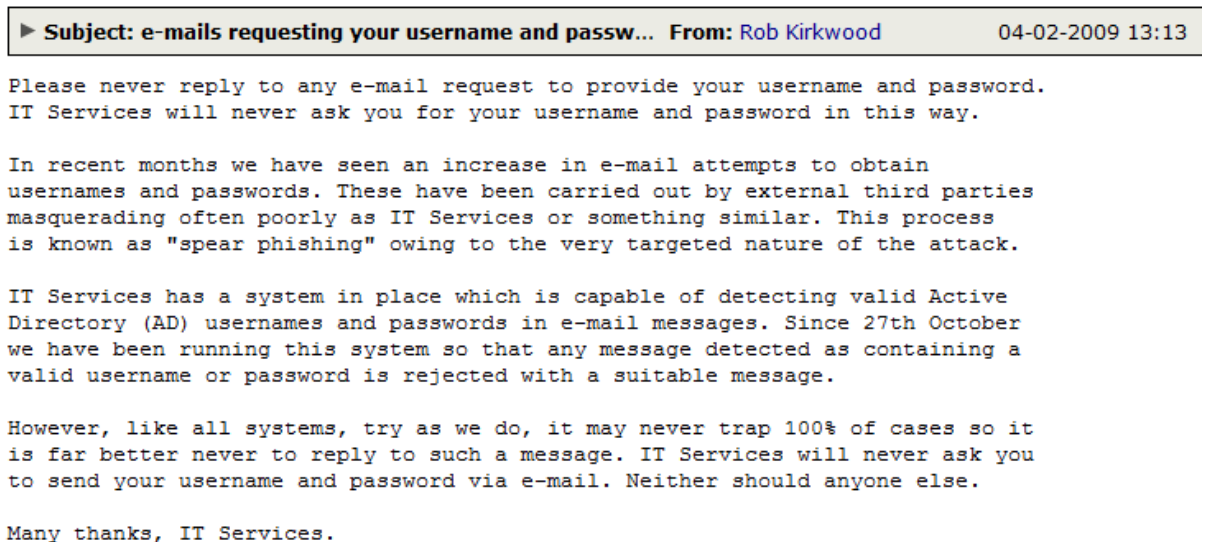


Figure 2.3: Loughborough University embedded training

Kumaraguru et al. (2007) applied embedded training with the main concern to make users motivated to use the training materials to increase their defence against e-mail phishing. The following learning principles were applied in the anti-phishing embedded training: learning-by-doing, immediate feedback, contiguity, personalisation and using a story-based poster shown automatically for users who fail to identify phishing. Results show that users' knowledge of phishing detection was enhanced more by embedded training than regular security notice messages.

Wombat™ Security Technologies (2009) describes the evaluation of PhishGuru™. This embedded training is based on sending simulated phishing e-mails to assess users' abilities to recognise phishing attempts and to provide an educational anti-phishing scenario-based cartoon poster for the ones who fail the test. The research concluded that participants who fell prey to the phishing and received anti-phishing training were 50% less likely to fall prey to phishing in future than those who did not receive the training. People are more likely to remember information when it is understandable and interactive. Their paper claims that embedded training gave users the ability to recognise phishing even 28 days after training. Users provided with a second training were 50% less likely to fall prey to phishing than those trained just once. Wombat™ Security Technologies (2009) claims this shows that repeated training is effective, though there is a need to take into account the motivating of users and avoiding feelings of unexcitement as these may have a negative influence.

6. Distance learning (e-learning)

There is a growing amount of literature on e-learning technologies (Dede, 1996; Kearsley, 2005; Khan, 1997; Edelson, Gordin, & Pea, 1999; Edelson & O'Neill, 1994).

With the continuous development on information security threats and, in particular, phishing, an educational system must as well developed to cope with those changes. This suggests the need for flexible and scalable learning, as it is claimed that e-learning provides. According to some research E-Learning has been found to reduce overall cost and the learning time by 40% to 60% compared to traditional learning methods (Web-based Training Cookbook, 1997, p. 108; Zenger and Uehlein, 2001). Willems (2005) claims that distance education provides flexible access to educational materials and allows learners and teachers to engage in an synchronous and asynchronous interaction in different places, times, and at different speeds (Gomez, Gordin & Carlson, 1995; Gordin, Polman & Pea, 1994; Pea, 1994). More than 30 studies claim that interactive technologies could reduce learning time requirements by a half (Miller, 1990). Research by Horton (2000), shows that virtual classrooms have decreased costs by 80% and also raised student satisfaction by 30% and knowledge retention by 25%. According to Fletcher (1990) Technology Based Training saves 35-45% of time compared to that of the traditional classroom whilst attaining the same or improved learning retention.

Andrew Sadler, vice president of strategy and alliances for IBM's Mindspan Solutions claim that the life of the knowledge is decreasing with the rapid development of technology, especially in the field of information technology where it is measured in months (Schultz, 2002). However, in most learning, the life of the knowledge lasts less than 6 months for Internet-based technologies because of the rapid development in the subject area compared to other subjects where it lasts between 8 and 36 months (Kapp, 2001: 270). Therefore, this should be considered while developing educational material to make it memorable and up to date. Potentially, e-learning could provide a continuable and updateable learning facility with less effort and resources.

Also e-learning shows an increased retention by 25-60% percent compared to traditional learning (J.D. Fletcher, 1991: 33-42). Masatoshi et al. (2010) illustrates the effectiveness of animated e-learning anti-phishing education in enhancing learners' skills in combating the phishing threat. There are many available online tutorials on phishing, such as by Computing & Information Services (CIS, 2009), eBay (eBay, 2006), Microsoft (Microsoft, 2006) and the Federal Trade Commission (FTC, 2006). However, Kumaraguru et al. (2007) state the need for simple and understandable material presented in the e-learning site to provide effective learning, especially if there is an absence of personal interaction.

2.5.3 Summary of Non-technological Solutions

It can be concluded from the literature on non technical solutions that effective education is needed. The advice given in most research publication has been found to be sparse and obvious to the user, and some publications merely repeat previous literature and articles available on the Internet. Many researchers point out the importance and the effectiveness of improving user awareness on phishing threats in reducing the risk of phishing, especially since technological solutions have proved unreliable in providing full protection as phishing has become more and more complex.

Therefore, the research in this thesis concentrates on enhancing the user's trust decision through an effective awareness and educational framework which integrates best practices or recommendations for parties who play a role in dealing with the phishing

problem with education and training on e-mail phishing. The research is built on previous studies with further investigation on users' vulnerability to phishing. The findings are used to understand phishing and to propose an effective awareness framework that is based on the learning principles described in this chapter.

2.6 The Contribution of the Literature Review

Phishing causes immense losses, from \$1.2 billion in the US in the period May 2004 to May 2005 (Kerstein, 2005) and up to £504 million in the UK in the year leading up to March 2005 (Richardson, 2005). Attacks have also been reported in other non-English speaking countries (*Sunday Morning Herald*, 2004) and researchers suggest the development of the phishing trend will continue in the future (APWG, 2006; Korea Internet Security Centre, 2006). According to AVIRA (2010), North America and Europe has the highest phishing incidence, with 45% of all phishing in these regions. In the rest of the world, there is less presence of phishing and under 10% of incidents occurred in Eurasia, Asia and the Middle East regions. However, the number of attacks in those regions were not clearly identified. In particular, Qatar is one of the countries where the incidence of phishing is unknown.

There is a lot of literature available on phishing, as identified earlier, and some studies review its threat in particular parts of the world, for example Spain (Uusitalo et al., 2009), Italy (Leone, 2006) and Malaysia (Gan et al., 2008). However, there is a lack of published literature on the phishing problem in the State of Qatar and in that part of the world.

Qatar has a conservative culture and this may affect on people's vulnerability to phishing, but this is not explicitly covered in the literature. Most literature, guide books magazines, articles, website blogs and forums discuss Qatar culture in terms of customs, traditions, what people wear and eat, arts and hand crafts, Islamic culture and some authors propose 'do or don't' living guides (Bush, 2003.; QatarVisitor, 2000, Explorer Publishing, 2009a and 2009b; Chaddock, 2007; Chaddock, 2008; Ossian, 2005; Usa, 2005; Orr, 2008; Nasr, 2009). They refer to day-to-day activity, tradition and a few

attitudes but they do not describe people's behaviour with IT. There is very little reported research on Qatar culture with regard to Qataris' behaviours, beliefs, interests and characteristics. This makes the research reported in this thesis original since it covers the factors which make Qataris vulnerable to phishing which are not presented in the literature.

One of the reasons Qatar was chosen to be the case study was because of the lack of literature on the phishing problem in Qatar and, in particular, on e-mail phishing. This literature review has thus shown that the aims and objectives are valid because of a lack of literature and confirms that some form of research is needed. Objective 1 in Chapter 1 is therefore fulfilled.

2.7 Summary

The literature reviewed shows that social engineering is a formidable attack that is hard to defend against, even with the highest security solutions since it targets human weaknesses to attain its goal. Phishing is shown to be one of its techniques which is becoming more complex with the development of telecommunications, and many different phishing types are appearing. This suggests a wide range of research projects on social engineering and phishing is possible. However, to keep the research within manageable proportions, this research focuses only on investigating e-mail phishing attacks. This chapter identifies previous research on vulnerability to the phishing threat along with the technical and non-technical methods developed to defend against this attack, with a particular emphasis on awareness and education as a proposed solution.

From the literature, or rather the lack of it, it can be concluded that there is a little knowledge in understanding people's susceptibility to phishing and the mechanisms behind phishing which make it successful and, therefore, further investigation is required through reality and laboratory tests which measure users' ability to distinguish phishing attempts. In addition, the literature suggests that awareness is important to reduce the risk of phishing but there is little to say how this can be implemented. There

is, therefore, a need for further research to increase understanding of how to make people aware of phishing and how to defend against it.

Some literature was found on technological solutions presenting tools to detect and prevent phishing, of which there are many available, using different techniques. However, no technological solution was 100% effective and the increasingly sophisticated phishing methods keep circumventing the technological defences. The non-technological solutions offer recommendations, advice, awareness and education, all of which will assist users in making correct trust decisions. Although tools are effective as one level of defence, users' trust decisions have been shown to be essential as a second line of defence to distinguish phishing attacks that may bypass the tools. It can be concluded that making the technological tools more effective and making users more aware would both be productive areas for further research. However, for this research the scope has been chosen to concentrate on promoting the awareness of phishing as a means of defence against attack, with a particular emphasis on the implementation of an awareness programme in Qatar.

Therefore, this research seeks to provide a solution to the e-mail phishing problem in Qatar based on non-technical solutions by first discovering the extent of the problem and the factors which make people vulnerable to phishing. Then it proposes some effective recommendations for different sectors and provides a complementary e-mail phishing educational awareness framework to enhance their knowledge on phishing and teach them how to distinguish and react to phishing attacks.

The next chapter describes in detail the research methodology. It specifies the research philosophy, approach, strategy and data collection methods used in this research for achieving the overall research contribution and filling the knowledge gap in the literature.

Chapter 3 Research Methodology

This chapter presents an overview of the research philosophy, approach and strategy, and follows this with a detailed description of the data collection methods available to a researcher and the justification of the appropriate one for the testing of the research hypotheses and achievement of the objectives.

3.1 Research Philosophy

It is important to identify the philosophy of the research since it will simplify for the researcher the choice of the appropriate research strategy and data collection methods, and verify how data are gathered and analysed (Crossan, 2003). Information systems (IS) cover all aspects of circulation of information throughout an organisation (Themistocleous 2002; Walsham 1993; Galliers 1992; Orlikowski and Bardoudi 1991). In IS research, the philosophy tends to transfer from epistemology (what is known to be true) (Myers, 1997) into doxology (what is believed to be true) (Galliers, 1992: 29). Positivist and anti-positivist (also called interpretivist) are the two main research philosophies recognised in IS research (Galliers, 1992: 29; Orlikowski and Baroudi,1991).

3.1.1 Positivism

Since the late 1970s, an approach based on positivism has been common in most IS research (Dickson and DeSanctis, 1990, cited in Jackson, 2001). Many researchers have illustrated positivism as the key for IS research (Themistocleous 2002; Walsham 1995; Miles and Huberman 1994; Yin 1994; Galliers 1992). This was supported by Orlikowski and Bardoudi (1991) who stated that about 70% of research in the leading US IS journals uses a positivist approach.

The positivist approach usually aspires to objective authenticity to enhance the perception of phenomena by independent observation, experience or testing of theories by the researchers (Myers, 1997; Galliers, 1992). Although this approach is mainly timeless, many scientists and philosophers have adopted it. It is commonly used in natural science research (e.g. mathematics, physics, etc.). Orlikowski and Baroudi (1991) describe as positivist an approach which involves hypothesis, measurements,

tests, deductions, verifications and suggestions, along with an approved analysis process (Crossan, 2003; Conford and Smithson, 1996; Popper, 1959). However, Hirschheim (1985) and Conford and Smithson (1996) have queried whether a positivist approach is appropriate for social sciences research into matters such as human behaviour.

3.1.2 Interpretivism

Interpretivism is the reverse of positivism in research. Thus Webber (2004) and Stahl (2005) have considered that observers are not independent and interpretivism distinguishes people's comprehension as being associated with their experience and culture (Pather and Remenyi, 2004). Interpretivism used to be the regular philosophy until the late 1970s (Vreede, 1995, cited in Jackson, 2001). It aims to prove or understand a phenomenon and how it is influenced by context (Myers, 1997) through the use of social constructs such as perceptions, human logic and joint meanings and by gathering data from field research in a subjective manner (Pather and Remenyi, 2004; Myers, 1997; Miles and Huberman, 1994; Walsham, 1993; Galliers, 1992), therefore the dependent and independent variables usually can not be predefined (Kaplan and Maxwell, 1994).

3.1.3 Choice of Philosophy

Benbasat et al. (1987) demonstrated the importance of both philosophies without preferring either approach. Others suggest use of a combination approach for IS research to develop research quality (Arnott and Pervan, 2005; Howcroft and Trauth, 2005; Breu and Peppard, 2001; Remenyi and Williams, 1996; Kaplan and Duchon, 1988; Bjørn-Andersen, 1985; Kuhn, 1960).

It is obvious that the interpretivist is the appropriate philosophy for the present research on reducing the risk of e-mail phishing through awareness by an empirical study in the State of Qatar, since this choice allows the researcher to understand the research topic in a subjective manner through empirical studies (Irani *et al.*, 1999). While the researcher aims to understand the phenomenon of e-mail phishing in Qatar with the objective of developing an effective awareness framework, she also attempts to discover if the phenomenon is influenced by complex and interrelated factors that require discovery

(i.e. cultural and country-specific contexts) by entering field data and employing social actions such as interviews and surveys. Positivism supposes that the facts are predefined and independent of the researcher (Themistocleous, 2002), whereas interpretivism usually focuses on balanced considerations emerging from the circumstances (Myers, 1997). Since this research is not a type of natural science research where it seeks to provide proof of theories or mathematical models, interpretivism was the best choice because it studies human behaviour in relation to electronic technology, in particular e-mail phishing attacks, with an intention to reduce this phenomenon through awareness and education. This research can therefore be categorised as computer science research applied in a social context.

3.2 Research Approach

Empirical and non-empirical are the main two research approaches. The non-empirical approach is based on reviewing existing literature in a subject area and then using it as a reference for the research.

Hussey and Hussey (1997) have illustrated the importance of the empirical approach for investigative, expressive, logical or prognostic research. This approach is based on observations in fieldwork (Easterby-Smith, 1991) using different techniques: qualitative/quantitative, deductive/inductive and subjective/objective.

3.2.1 Qualitative/ Quantitative

The choice of the appropriate method of qualitative, quantitative or a mix of both is discussed in various literature (e.g. Leedy and Ormrod, 2001; Darke et al., 1998; Hussey and Hussey, 1997; Myers, 1997; Cavaye, 1996; Miles and Huberman, 1994).

Myers (1997) describes quantitative methods as having originated in scientific research to investigate natural phenomena through gathering and analysing numerical data collected from fieldwork from, for example, surveys, experiments and laboratory tests. In contrast, qualitative methods are usually used in social science research to examine social phenomena through case studies, action research, ethnography, interviews and questionnaires. Furthermore, Hussey and Hussey (1997) have described qualitative

research as a subjective approach involving investigation and observations to study social and human behaviours.

3.2.2 Deductive/ Inductive

Many researchers have described deductive and inductive research (e.g. Perry, 2001; Hussey and Hussey, 1997; Cavaye, 1996). Deductive is defined as ‘top-down’, moving from the general to the particular. It starts from studying a theory and defining hypotheses and examines them through observations, which enables the researcher to confirm or not the original theory (Hussey and Hussey, 1997). In contrast, the inductive approach works the other way round, from the particular to the general (i.e. from precise observations, to defining tentative hypotheses and developing theories or conclusions) (Hussey and Hussey, 1997:13). Cavaye (1996: 236) and Perry (2001: 307) have illustrated the possibility of using both approaches in the same research.

3.2.3 Subjective/ Objective

In subjective research, the researcher has to be involved in the implementation of the fieldwork and has control on the outcome, whereas in objective research, the researcher is independent of the fieldwork. Easterby-Smith *et al.* (1991: 27) state that interpretivism is usually subjective; it requires the researcher to contribute in fieldwork and identify any influences that may have an effect on research findings.

3.2.4 Choice of Approach

In this research, both the non-empirical and empirical approaches are used. The non-empirical approach forms its foundation and involves a review of previous literature on the research and related topics and it defines the empirical research activities.

Creswell (2003) states, “The study may begin with a quantitative method in which theories or concepts are tested, to be followed by a qualitative method involving detailed exploration of a few cases or individuals”. In this research, both qualitative and quantitative research methods are used since the research involves the study of the phenomena of e-mail phishing in Qatar, focusing on investigating people and cultural contexts through numerical data and observations gathered by different data collection methods including experiments, surveys and interviews (Myers, 1997). Research by

Creswell (2003) has illustrated the importance of quantitative and qualitative analysis. Therefore, both kinds of analysis will be the best approach to analysing the data gathered from this research.

Furthermore, a combination of both deductive and inductive approaches is used in this research since the research aim is to develop an e-mail phishing awareness framework and then evaluate it. Perry (2001: 307) states that some research begins from theory construction and then examines the theory.

Since an interpretivist position is adopted in this research, a subjective approach is selected as the appropriate choice to attain the research aim of applying empirical studies in Qatar with personal involvement in the fieldwork.

3.3 Research Strategy

The research strategy presents a general plan for answering the defined research questions (Saunders, 2000) and achieving the objectives of the research. Creswell (2003) suggests the use of multiple methods to develop the conclusion of the research and has referred to “sequential procedures, in which the researcher seeks to elaborate on or expand the findings of one method with another method”.

Many researchers (e.g. Leedy and Ormrod, 2001; Saunders, 2000; Darke *et al.*, 1998; Hussey and Hussey, 1997; Powell, 1997; Cavaye, 1996; Remenyi and Williams, 1996; Alavi, 1994; Miles and Huberman, 1994; Galliers, 1992) have expressed various research strategies that could be deployed, as follows:

Experiment: a traditional form of research usually applied in natural science or social science.

Survey: associated with a deductive approach based on collection of a large amount of data gathered from a sample of population based on questionnaires and interviews carefully defined.

Grounded theory: based on data gathered from a sequence of observations.

Ethnography: based on observing patterns of human activity and societies through the use of different methods (e.g. observation, interview and questionnaire) in which case the researcher makes deductions from participants' visions.

Action research: based on field experiment where the researcher attempts to solve the phenomena by shared partnerships having control over variables.

Modelling: involves the improvement of specific models.

Operational research: recognises activities and their relationships based on operational effectiveness.

Case study: usually used to investigate social phenomena and provides an in-depth understanding of the area of research.

Yin (1989) also demonstrated different strategies for empirical studies that may deploy experiments, surveys, archival analysis, history and case studies.

3.3.1 Choice of Strategy

Referring to the research objectives as outlined in Chapter 1, the appropriate research strategy for this thesis is based on a case study of the phenomena of e-mail phishing in Qatar with some comparison with the UK.

Many authors have clarified case studies as empirical work deployed in reality perspectives to investigate a phenomenon (Jensen and Rodgers, 2001; Perry, 2001; Gillham, 2000; Welman and Kruger, 1999; Darke *et al.*, 1998; Myers, 1997; Tellis, 1997; Cavaye, 1996; Stake, 1995; Yin, 1994). In addition, Yin (1994) states that a case study aims to investigate a phenomenon in a reality context.

Stake (1995) referred to a case study as “the study of the particularity and complexity of a single case, coming to understand its activity within important circumstances”. Many researchers (e.g. Alavi and Carlson 1992; Orlikowski and Baroudi, 1991) describe the case study as the common qualitative method deployed.

According to Yin (1994), there are different types of case studies, each used to answer different research questions, for example exploratory, descriptive and explanatory used to answer what, how and why, respectively. This research begins with exploratory, followed by explanatory and then descriptive case studies, since the research addresses three main questions:

1. What is the extent of e-mail phishing in Qatar?

2. What are the factors which make such threat successful in Qatar?
3. How can an effective awareness framework be developed to enhance Qataris' awareness on e-mail phishing with the aim of reducing the risk of phishing?

Furthermore, Jensen and Rodgers (2001: 237-239) define different categories of case studies:

Snapshot: A comprehensive study of one research area at one point in time.

Longitudinal: Quantitative and/or qualitative investigation of one research study at multiple time points.

Pre-post: The study of one research entity at two time points delineated by some critical event.

Patchwork: Defines a comprehensive vision of the research since several case studies are used for one research project (e.g. snapshot, longitudinal and/or pre-post).

Comparative: Uses various case studies for different research to provide a comparison.

In this research, *patchwork case studies* are used in which both *snapshot* and *pre-post case studies* are used to develop the framework and evaluate its effectiveness, respectively. Since the case studies could employ several data collection methods, including direct or indirect observations, interviews and the study of documentations and records (Yin, 1989), in this research, the case study is comprised of various data collection methods explained in the section below.

Although the case study is the main strategy applied in this research, there are some others used to assist in achieving the research objectives, as shown in Table 3.1.

Table 3.1: Additional strategies used for each objective

Objectives	Strategies used
Objective 1: To review literature on previous work in the research area.	Literature review
<p>Objective 2: To confirm the existence of an e-mail phishing problem in Qatar.</p> <p>Objective 3: To determine the factors which make Qatar an attractive place for phishers.</p> <p>Objective 4: To compare the awareness of Qatari citizens of the e-mail phishing threat with that of citizens of a developed nation such as the UK.</p>	Survey strategy, including interviews and questionnaires
Objective 5: To investigate the susceptibility of Qatari people to e-mail phishing and the effects of cultural and other country-specific factors on the development and diffusion of e-mail phishing in Qatar society.	Experiments were found the appropriate method to achieve this objective, along with ethnography. Although it is beyond the scope of this research to involve in-depth psychology, it is noticeable that there are some elements of ethnography required in this research for investigating people's awareness and responses to phishing.
<p>Objective 6: To define, from the results of all above objectives, the need for enhancing awareness and the need to provide an effective e-mail phishing awareness and educational framework.</p> <p>Objective 7: To develop an e-mail phishing awareness framework to reduce the risk of e-mail phishing in Qatar which consist of a set of recommendations and a proposed educational framework.</p>	Grounded theory is applied to gather and analyse the outcome of all previous methods (surveys and experiments) to identify the need for, and develop an effective e-mail phishing awareness framework and establishing a set of recommendations for Qatar government, citizens and officials responsible for ensuring information security.
Objective 8: To evaluate the effectiveness of the proposed framework in reducing the risk of e-mail phishing in Qatar.	Action research was used to develop and evaluate the e-mail phishing educational framework as it involved cooperation (Rapoport, 1970) with organisations in Qatar to bringing the framework into action in reality.

3.4 Data Collection Methods

Establishing a comprehensible research methodology is an important phase in any research, as stated by several researchers. According to Bouma (1996), the research design and methods should be carefully planned in order to achieve the research aims and objectives. In addition, Yin (1994) has defined the research design as “the logical sequence that connects the empirical data to a study’s initial research questions and, ultimately, to its conclusion”.

However, this research begins with a qualitative method applied through interviews, a quantitative method through questionnaires and, finally, a combination of both in experiments, together with a case study, which define and evaluate the effectiveness of the proposed e-mail phishing awareness framework. The research approach commences by defining theoretical concepts, research aims, objectives and methodology through an in-depth literature review, notwithstanding that the review continues throughout the research process. Afterwards, there is a review of literature on Qatar with some on the UK. The research stages are depicted in Figure 3.1.

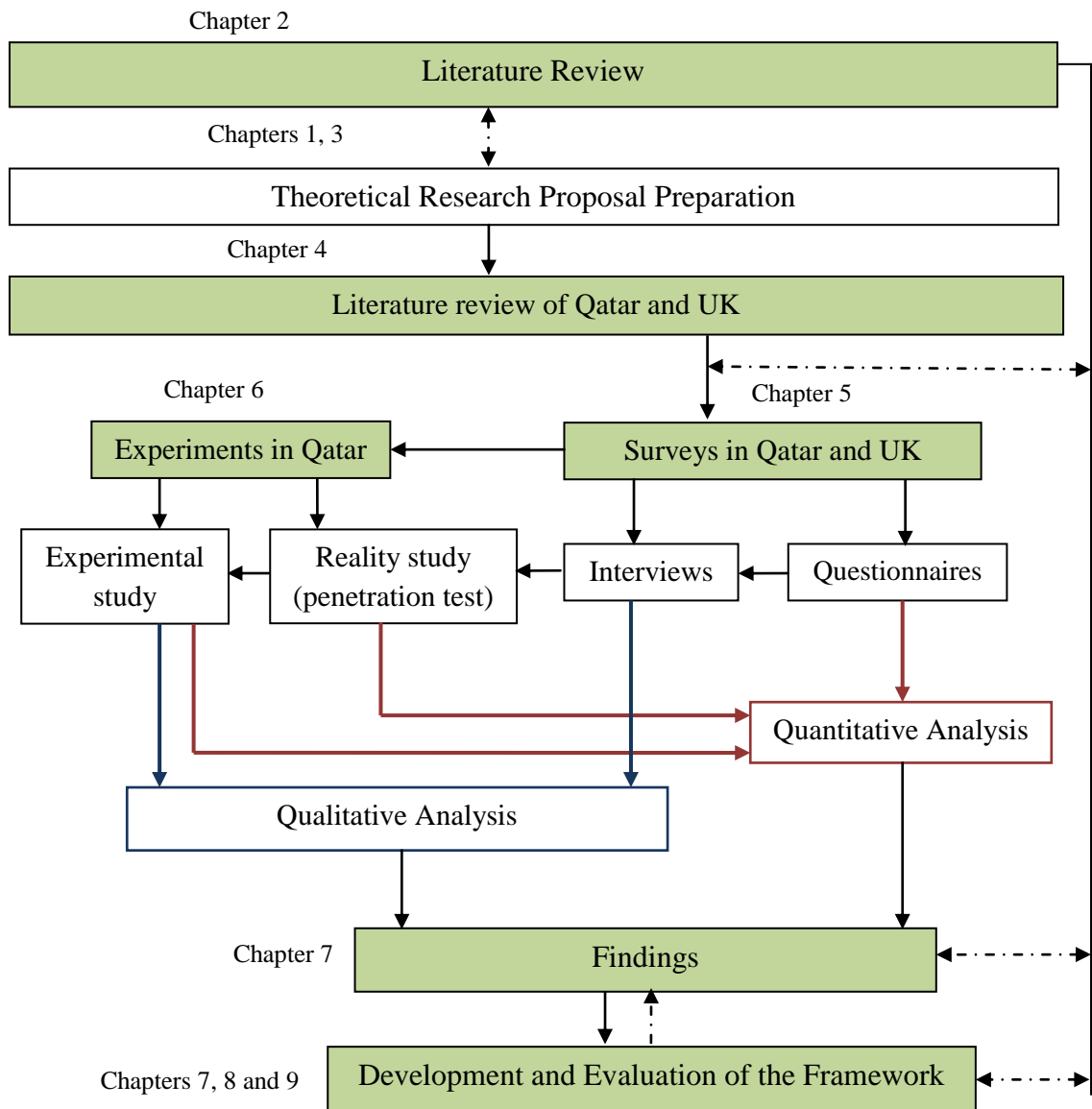


Figure 3.1: Research stages

Subsequently, the research method proceeds with a qualitative interview, a quantitative questionnaire tool to study a defined concept on a focused sample, and a quantitative and qualitative experiment instrument for the reality and experimental study of the ability of a sample of Qatari citizens to recognise phishing e-mails and the factors that might make Qataris vulnerable to the phishing threat. The research contribution is then achieved by applying grounded theory to develop an effective awareness and educational framework (see Figure 3.1).

Following the information gathering phase, data analysis is used to discover the factors which make Qatar citizens susceptible to e-mail phishing, leading to creation of the proposed awareness and educational framework which addresses the discovered factors

with the intention of diminishing the threat of e-mail phishing in Qatar culture (see Figure 3.1).

The research methodology is defined to fulfil the objectives of the research; an explanation of each method used is now given below.

3.4.1 Literature Review

The research process begins with a general literature search focused on key concepts from the following areas: social engineering, phishing, vulnerability to phishing, anti-phishing solutions, education and training (described in Chapter 2).

The initial findings from the general literature help to define and refine the research's aims, scope and the research questions (described in Chapter 1). This drives the research to focus on reducing the e-mail phishing problem in the State of Qatar through awareness and education. Hence, an in-depth literature search is required in the areas of e-mail fraud, e-mail phishing and other related topics on awareness and education to provide an overview of previous research in this field and to discover a proposed solution which will make a contribution to knowledge towards reducing the risk of e-mail phishing in Qatar.

The research methods illustrated in Figure 3.1 show the literature review as a continuous process that assists in reaching major research milestones and contributes through the research phases, starting from the research proposal to develop and evaluate an awareness and educational framework.

3.4.2 Review of Literature on Qatar and UK

Before resolving any situation, it is crucial to prove first that the situation does exist and demonstrate the importance of finding the best solution. Case studies are considered a common data collection method (Myers, 2002). According to Gall *et al.* (1996), "...researchers generally do case studies for one of three purposes: to produce detailed descriptions of the phenomenon, to develop possible explanations of it, or to evaluate the phenomenon". Hence, the research commences with proving that e-mail phishing is a real potential threat facing online consumers in Qatar society, with Qatar being chosen

as a case study as it is a rapidly developing country that has not been researched in this respect.

Therefore, an investigative literature review of Qatar was an important step. The review aimed to discover the extent of the e-mail phishing problem in Qatar society, compared to other developed nations such as the UK, and possible aspects which make the State of Qatar a fertile ground for phishers to commit their crimes (described in detail in Chapter 4). However, there were no sources or literature available which specifically consider the phishing threat in Qatar whereas there was literature covering the issue in other nations such as the UK and USA. Hence, some of the sources used in analysing this topic in Qatar are based on the author's own analysis and interviews in the region.

3.4.3 Survey

In parallel to the review of literature on Qatar and the UK, surveys were carried out. E-mail, face-to-face semi-structured and structured interviews, and household drop-off and pick-up and online questionnaires were the main data collection strategies used throughout the survey phase (Trochim, 2002) (described in Chapter 5). In essence, the literature review has led up to the development of a survey questionnaire and interview instrument.

The questionnaires completed by Qatari e-mail users are used to draw a profile of people's knowledge and awareness of e-mail phishing and their vision of the best method to defend against this attack. Similarly, the questionnaire in the UK allowed comparison of the awareness level of Qatari e-mail users with that of users in a developed nation.

Interviews with the Qatari public, domain experts in online fraud, awareness and education have aimed to provide a better understanding of the e-mail phishing threat and the best method of defence against it, with a focus on effective awareness and education. It also elaborates on the potential threat of e-mail phishing, and the cultural and country-specific factors and other aspects which make phishing successful in Qatar.

Afterwards, a qualitative and quantitative analysis was used to analyse the data gathered from interviews and questionnaires, respectively. Furthermore, a comparison of the outcome of the survey in both countries was provided.

3.4.3.1 Questionnaire

The questionnaire aims to profile Qatari citizens' awareness of e-mail phishing and their vision of defence against such attack compared to that of citizens of other developed nations such as the UK. Questionnaire participants were randomly selected from British and Qatari citizens according to a defined criterion, which is e-mail users aged over 12. Household drop-off and pick-up and online types of questionnaire were used. These were carefully designed and passed through first-review and pilot-test to provide an effective design. English and Arabic versions of the questionnaire were designed with simple language and straightforward questions. A covering letter was attached to each questionnaire to provide an explanation for respondents of the questionnaire aim and target group. The questionnaires were distributed by hand or through e-mail, for household drop-off and pick-up and online questionnaires, respectively. All of the responses gathered in the paper based questionnaire were combined with those from the online questionnaire in order to have a single electronic source with the feature of automated results and filtering. Finally, 2000 responses were gathered, 1000 in Qatar and the rest in the UK. Afterwards, the responses were analysed quantitatively according to statistical analysis of the results and qualitatively according to the participants' interviews (see Chapter 5)

3.4.3.2 Interview

The qualitative research interview aspires to illustrate and understand the meaning of the topic in the life world of the subjects (Kvale, 1996). Interviews are mainly useful for understanding the background behind a participant's experiences where the interviewer searches for in-depth information around the topic (McNamara, 1999).

In this research, structured and semi-structured interviews were chosen. Both are common forms of interviewing technique. In structured interviews the interviewer is tied to a set of questions to ask which makes the evaluation process easier for the interviewer (Campion, 1994; Hollowitz and Wilson, 1993). However, a semi-structured interview is more flexible and aims to turn the interview into a conversation and to assist interviewers to tailor their questions to the interview context and to what the interviewee says (Lindlof and Taylor, 2002; Kumar, 1996). An interview protocol with a set of questions was defined initially to facilitate the interview process. Although a basic group of topics and questions was established for all interviews, questions were

however put differently to some interviewees, depending on their backgrounds (Lindlof and Taylor, 2002: 195; Foddy, 1993).

Most interviews were face-to-face and some were e-mailed, depending on the choice of the interviewees. Most were in English but some were in Arabic, especially with the Qatari citizens who found difficulty with the English language; however, this choice was mainly a decision of the interviewees. Notes were the method of recording interview data. The process of the interviews progressed from planning, preparing and interviewing into transcribing, analysing and discussing findings, as follows (McNamara, 1999):

1. Planning: plan the interviews, e.g. interview type, technique, set major topics to discuss, etc.
2. Preparing interviews, e.g. contact interviewees for interview approval, gather information about the interviewees or their organisation, prepare the interview questions, etc.
3. Interviewing: conduct interviews
4. Transcribing: prepare interview materials for analysis
5. Analysing and discussing findings: apply qualitative analysis and discuss findings

Generally, interviews were held with domain experts and a number of participants who represented a sample of the Qatari public. Some interviews were in parallel with the questionnaire phase with some of the questionnaire respondents, some followed the questionnaire data collection and analysis and some after the implementation of the experiments and the e-mail phishing framework (see Figure 3.1). The questionnaire analysis and literature review of Qatar and the UK suggested questions needing further investigation. Therefore, investigations were made in available literature and because of deficiencies in the literature; interviews were used to support and elaborate the study. Interviews were held with a wide range of Qatar society to gather a full and representative range of views, but interviews also took place with domain experts in the government and private sector organisations from Qatar, UK and Swiss in the field of e-crime, information security, judicial, information security awareness, education, Qatar culture and Islamic studies (see Figure 3.2).

Domain experts were chosen from government and private organisations according to their respective experience in online fraud and, in particular, e-mail phishing and/or awareness and education. Key staff were chosen for interview according to their job titles and responsibilities. Only those who make strategic decisions on e-crime or awareness were interviewed. The ultimate aim of the interviews with domain experts was to review the extent of e-mail phishing, cultural and possible effects associated with people's responses to phishing, organisational strategy, and people's perceptions on protecting themselves and/or their customers from e-mail phishing attacks, in particular the processes deployed for creating awareness among their employees and customers and for educating them about such threats. In addition, some domain experts were involved in the planning and designing of experiments and the e-mail phishing awareness framework proposed by the researcher.

In addition, interviews were held with participants in the questionnaire, experiments, e-mail phishing awareness programme to assist in the evaluation process. Those participants were chosen usually randomly according to predefined criteria assigned by the researcher depending on the needs of each data collection method and according to the convenience and willingness of participants to be interviewed. They were interviewed to have a better understanding of their responses, to discover the ability of Qataris to detect phishing e-mails, to discover the factors which make Qataris susceptible to phishing attempts and to evaluate the effectiveness of the proposed framework. Mostly face-to-face semi-structured interviews were held but where this was not convenient for the participants there were a few structured e-mailed interviews. The interviews were then analysed qualitatively.

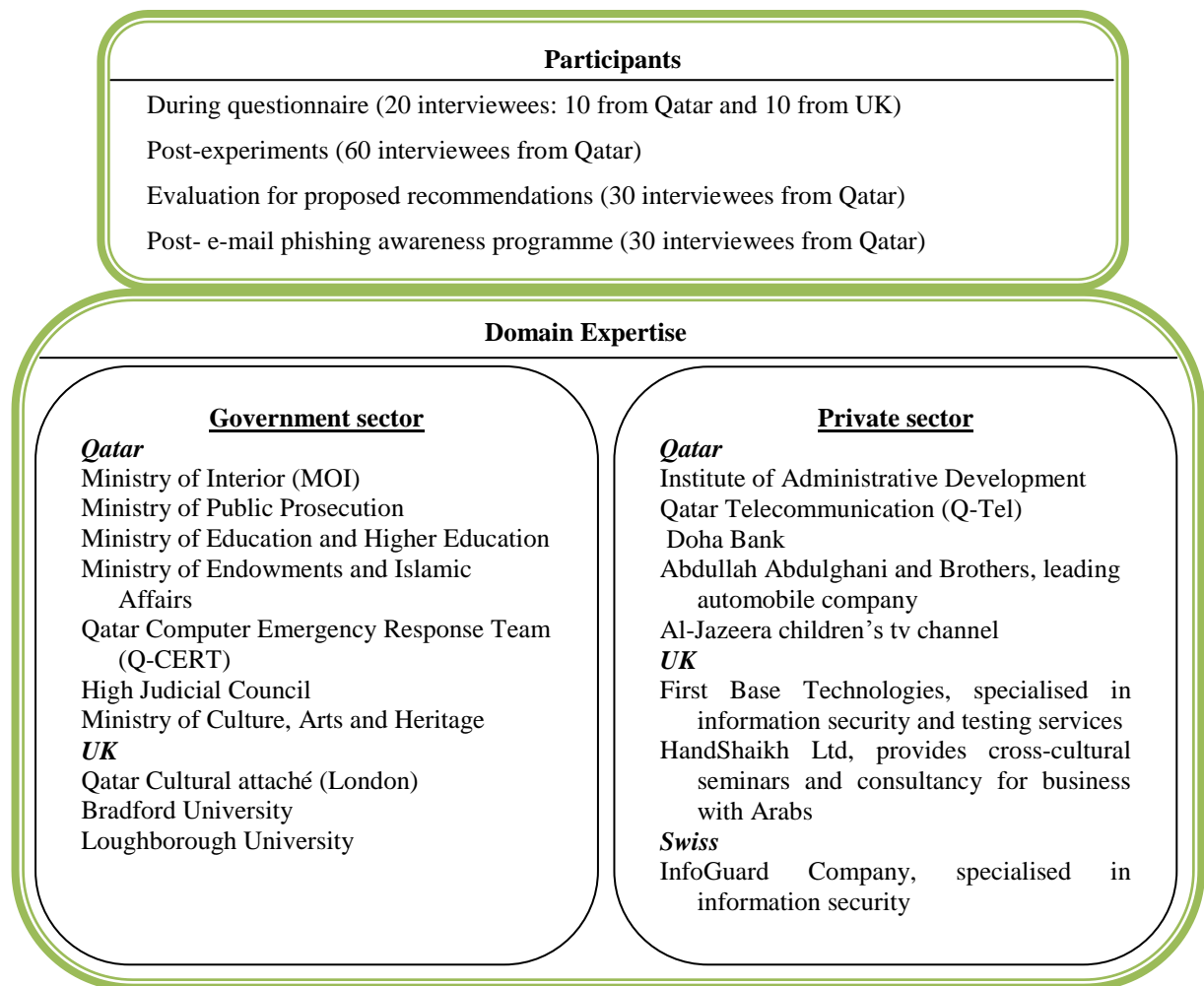


Figure 3.2: Interview plan

3.4.4 Penetration Tests and Laboratory Experiment

A lot of research has used experimental tests to assess user ability to distinguish phishing websites and e-mails (i.e. measuring participants' detection rates against phishing rates) employing different attack methods and different enhanced indicators (Jackson et al., 2007; Dhamija *et al.*, 2006; Herzberg and Jbara, 2004; Gabrilovich and Gontmakher, 2002)

Consequently, in order understand participant behaviour in response to phishing and their ability to recognise phishing e-mails, both lab experiment and real life experiments (penetration testing) were carried out in order to see how Qatari people would behave in reality compared to a lab environment (described in Chapter 6). The evaluation of participants' responses was according to their feedback, their scores and through semi-structured interviews with the participants. The data gathered from experiments in Qatar

were analysed with quantitative and qualitative methodologies to identify the factors which make Qatari citizens susceptible to this kind of attack.

3.4.5 Findings

This phase demonstrates a conclusion of all the above data collection methods (see Figure 3.1). Grounded theory is applied to analyse and observe the outcome of all previous phases which identifies the need for establishing an effective e-mail phishing awareness framework for the state of Qatar as a super solution to reducing such threat (see Chapter 7).

3.4.6 Development and Evaluation of the Framework

From the analysis of the data gathered, a comprehensive awareness framework was developed which involves a set of recommendations for the Qatar government, organisation officials responsible for ensuring information security and Qatari citizens, along with an educational framework aimed at reducing the e-mail phishing threat in Qatar.

The opinion of experts in the field and of a sample of Qatari citizens is used to evaluate the effectiveness of the proposed recommendations in reducing the e-mail phishing threat in Qatar. In addition, the researcher has carried out trials of a phishing awareness programme involving different training methods in Qatar to evaluate the effectiveness of the educational framey (described in Chapter 7, 8 and 9).

3.5 Data Sampling Method

The sampling process involves selecting a sample of the population to further investigate the phenomena. Because of the constraints of time and resources, it is impractical to examine the entire population, so this research uses sampling. Therefore, a sample frame was selected to represent the population. Probability and non-probability sampling are the common types of sampling. Sekaran (1992) has classified sampling methods as shown in Table 3.2.

Table 3.2: Data sampling method

Probability sampling	
Simple random sampling	Sample selected at random, each member of population equally likely to be selected.
Complex probability sampling	<p>Common types:</p> <p><i>Systematic sampling:</i> Begins with selecting random element of population from 1 to n and then every nth element will be chosen to be in the sample.</p> <p><i>Stratified random sampling:</i> The population is divided into groups known as strata e.g. geographical areas, age-groups, genders. Random selection is made within each stratum, the size of each sample being proportional to size of the total population of stratum from which it is taken.</p> <p><i>Cluster sampling:</i> The population is grouped into clusters according to different characteristics of the community, such as interests or jobs. A sample taken from each cluster (e.g. 6 people selected to represent each job type under investigation)</p> <p><i>Area sampling:</i> A sample is randomly selected based on dividing the region of the investigation into geographical units, such as counties and cities. This is a special case of either stratified random sampling or cluster sampling.</p> <p><i>Double sampling:</i> Offers another chance for further investigation where a sub-sample is required to further investigate results defined from main sample</p>
Non-probability sampling	
Convenience sampling	Samples chosen from population based on the elements' convenience to contribute to investigation.
Purposive sampling	<p>Samples selected carefully from the population according to the information, a sample could offer or to defined criteria. Two main types:</p> <p><i>Judgment sampling:</i> The decision on an appropriate sample is made from the population according to judgment on the best sample able to supply the required information.</p> <p><i>Quota sampling:</i> Samples are selected from different groups and backgrounds (e.g. age, gender, education) of population based on convenience. However, samples must be representative of population.</p>

3.5.1 Choice of Sampling Method

This research uses a combination of both probability and non-probability sampling methods to ensure the choice of appropriate samples for the investigation that represent the population and would contribute effectively in the research. Sampling methods used in this research are listed in Table 3.3.

Table 3.3: Choice of sampling method

Sampling method chosen	Where applied
Probability sampling	
Simple random sampling	<i>Questionnaire:</i> Participants selected randomly but according to specific criterion 'Qatari or British e-mail users aged above 12'
Non-probability sampling	
Convenience sampling	<p><i>Reality and experimental studies:</i> Due to sensitivity of such studies, samples were chosen according to the researcher's convenience (i.e. family members).</p> <p><i>Evaluate framework:</i> To ensure the effectiveness of the defined phishing awareness framework in enhancing the level of protection against phishing, samples of populations were chosen according to convenience to participate. For instance, this was used to evaluate of proposed recommendations and awareness programme.</p>
Purposive sampling	<i>Interviews:</i> Both types of purposive sampling, judgement and quota sampling were applied in identifying appropriate interviewees able to provide valuable information to the research. However, some interviewees were selected according to convenience, such as interviews with the questionnaire participants.

3.6 Summary

This chapter describes the research methodology applied in this research, starting from the adoption of the appropriate philosophy, research approach and strategy. Subsequently, a detailed description of the chosen data collection methods is presented, namely literature review, surveys, experiment, grounded theory and development of an effective e-mail phishing awareness framework. A summary of choices is shown in Figure 3.3.

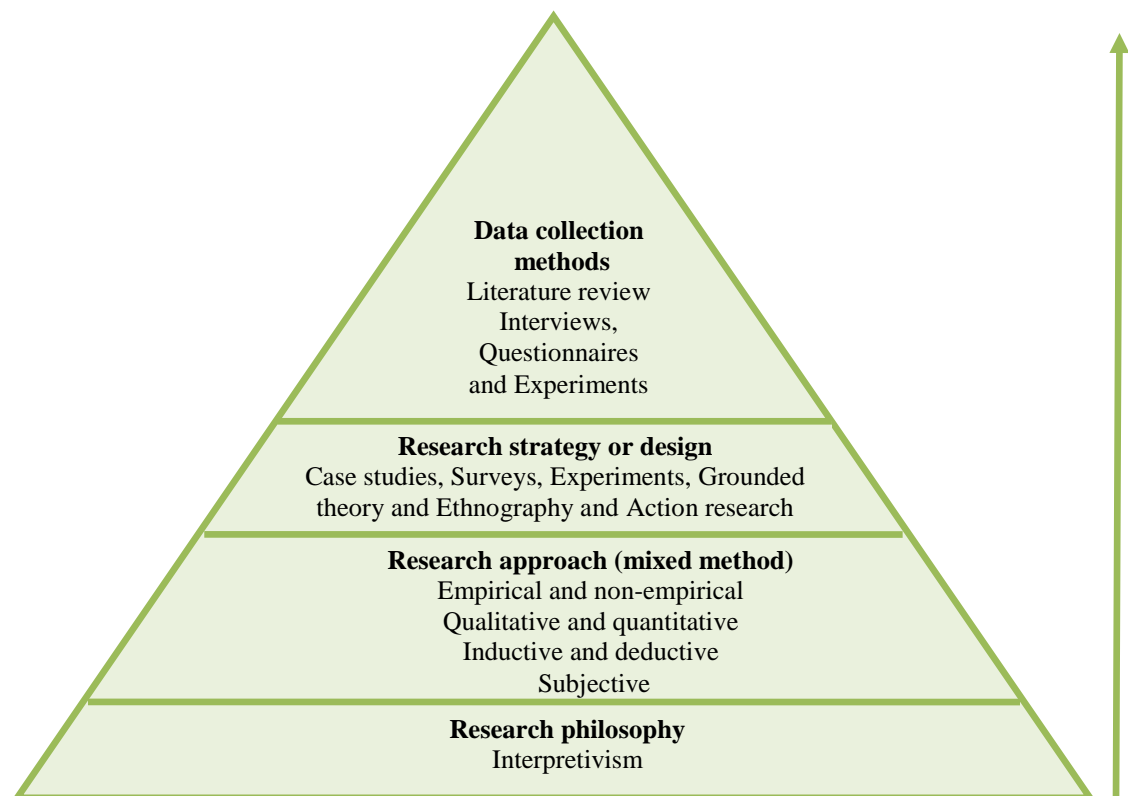


Figure 3.3: Choice of research methodology

In addition, the chapter describes how the research is based on an investigative case study of e-mail phishing in Qatar with a comparison with the UK. In that case study, different strategies are applied to achieve the research objectives (see Table 3.1). Furthermore, the choice of sampling methods was identified for each data collection method applied in this research (see Table 3.3).

In the next chapter (Chapter 4: Qatar in the eyes of phishers), the literature and interviews held are examined to identify the existence of the e-mail phishing problem in Qatar and the factors which make Qatar an attractive place for phishers to commit their crimes.

Chapter 4 Qatar in the Eyes of Phishers

This chapter is based on an investigative literature review of the State of Qatar. Information and publications gathered from literature were reviewed and analysed. In addition, interviews supplemented the review in the State of Qatar which clarifies the aspects which make Qatar a fertile ground for phishers to commit their crimes.

4.1 Overview of Qatar

Qatar is an independent country situated in the middle of the Western coast of the Arabian Gulf. It is on a peninsula with a total area of 11850 sq km, including a number of islands and islets, all together about 5% of the size of the UK. It had a population of about 1.4 million in 2008 (QSA, 2008). The country gained independence from the UK of which it had been a Protectorate since about 1914 on 3 September 1971. Doha is the capital, the official language is Arabic and English is commonly used as a second language. Since the mid-1800s, Qatar has been ruled by the Al-Thani family (Ministry of Foreign Affairs, 2007a).

Qatar is part of the Gulf State formed on 25 May 1981 by the leaders of the State of Qatar, United Arab Emirates, State of Bahrain, Kingdom of Saudi Arabia, Sultanate of Oman and State of Kuwait. This is a cooperative framework joining the six states to effect coordination, integration and inter-connection among the Members in all fields in order to achieve unity through The Cooperation Council for the Arab States of the Gulf, afterwards referred to as the Gulf Cooperation Council (GCC) or simply the Gulf State (GCC-SG, 2005).

According to the GCC (2000), many factors assisted in creating homogeneous characteristics for cooperation such as historical, religious, social, cultural and geographical factors.

Qatar had in the past existed as a poor British protectorate with pearling and fishing as its main source of income and had faced difficulties in the 1920s when its pearling industry tailed off because of the innovation of the Japanese cultured pearl, which had an effect on the Qatar economy. Now, it has been transformed into an independent state with significant deposits of oil and natural gas (CIA, 2008a).

The State of Qatar with its relatively limited population and finance reached two rapid turning points in all fields, including political, economic, educational, media, social, infrastructural and other sectors. The first was after the discovery of oil at the beginning of the 1940s and the second was when His Highness The Amir, Shaikh Hamad Bin Khalifa Al-Thani, assumed power in 1995 (Ministry of Foreign Affairs, 2007a).

According to Amiri Diwan (2009), Shaikh Hamad Bin Khalifa Al-Thani stated that, “We are on the threshold of a new epoch overlooking the 21st century where we aspire to attain the status befitting us.”

4.2 Why Qatar is Attractive to Phishers

There are many factors which makes Qatar an attractive ground for phishers as shown below.

4.2.1 Economic Development

Today, Qatari citizens have a high standard of living equal to that of developed countries, mainly because of the oil and natural gas revenues, with estimated gross domestic product (GDP) growth rate of 11.2% in 2008 compared to the UK’s 0.7%, and which, therefore, led Qatar to have the second-highest GDP per capita income in the world in 2008, reaching \$103,500 compared to the UK which reached \$36,600, and according to the World Factbook of the CIA (Central Intelligence Agency) (2009), Qatar compared to the UK has a lead growth in GDP, investment and industrial produce (see Table 4.1). Qatar, it has the highest GDP in the Arab world, according to the International Monetary Fund (IMF) (2007).

In addition, in 2008 Qatar was ranked as the third country in the growth of industrial production with growth rate of 12.6% compared to the UK with a negative growth rate of -0.1% (see Table 4.1) (CIA, 2008a, b). This is due to a massive increase in Qatar's industrial production which includes manufacturing, mining and construction.

Also in 2008, it was ranked as the third country in the world in investment, with 41.4% of investment compared to the UK's 16.7%. It also had the least percentage of unemployment with 0.60%, compared to the UK's 5.5% (see Table 4.1) (CIA, 2008a, b).

Table 4.1: GDP, growth rate, investment and unemployemnt of Qatar and UK

(2008 est.)	Qatar		United Kingdom	
GDP - per capita (PPP)	\$103,500	Rank 2	\$36,600	Rank 31
GDP - real growth rate	11.2 %	Rank 5	0.7 %	Rank 196
Industrial production growth rate	12.6 %	Rank 3	-0.1 %	Rank 152
Investment (gross fixed)	41.4 %	Rank 3	16.7 %	Rank 136
Unemployment rate	0.6 %	Rank 3	5.5 %	Rank 66

In 2008, the markets were down and most of the world's leading economies, the United States, Great Britain, France, Germany and Japan, faced a decline in their economies. For the first time in decades, the fastest growing economy has been a country almost unheard of by many in the western world, which is the State of Qatar with 13.4% GDP growth, whereas Great Britain was expected to be one of the slowest growing economies in the world as predicted by *The Economist* in 2009 (The Economist, 2008; Roman, 2009) (see Figure 4.1).



Figure 4.1: GDP growth forecast for 2009 (*The Economist*, 2008)

The Saudi American Bank (Samba) Financial Group stated, “Qatar's strong economic performance is being fuelled mainly by growth in the country’s liquefied natural gas (LNG) exports”, and the spokesman commented that in 2009 Qatar expected to be the world’s fastest-growing economy, even in spite of the global financial crisis, because of the increased exports of liquefied natural gas (Sambidge, 2009a). Also, the Bank of America, Merrill Lynch, has said that this inflation may come down in 2010 to 7%, but the country will, however, persist in its growth (Sambidge, 2009b).

Many have commented on the survival of Qatar through the global financial crisis. Addressing the 3rd International Conference on Information and Communication Technologies and Development (ICTD) 2009 in Doha, Braga, the director of economic policy, said that Qatar is one of the few countries which continues to grow despite the global financial crisis. He added that the ICT (Information and Communication Technology) industry in Qatar is well placed, which has assisted in tackling the crisis (Sambidge, 2009c).

However, according to the Urban Planning and Development Authority (2006), the development in Qatar is still in progress; currently the Authority is managing the basis of the Master Plan for the State of Qatar which will guide its physical development to

the year 2025 in all aspects, including transportation, infrastructure, construction and environmental protection.

On the other hand, Britain prepares itself for decades of severity because it faces the sharpest quarterly drop in the British economy since 1979 with a decline of 1.9% in GDP experienced in the first quarter of 2009, which exceeded economists' expectations, and is expected to drop still further by a total of 3.5% by the end of 2009. In 2009, the British economy will decline by 4.1%, followed in 2010 by a further decline of 0.4%. This economic drop has had a major effect in increasing the number of unemployed in the UK, which in February 2009 reached its highest level of 2.1 million since Labour came to power in 1997. However, there might be a forecast of a blooming in the British economy as the Chancellor said that there would be a growth of GDP of 1.25% in 2010 and 3.5% in 2011 (Monaghan, 2009).

In conclusion, the development of the economy in Qatar has leapt considerably in a short time, leading Qatar to become the fastest growing economy in the world ahead of the world's leading economies such as China and the UK. This rapid and considerable growth has attracted phishers to commit their crimes in Qatar since it provides a fertile ground for them to make their attacks where there is an enormous amount of money to steal, which is the ultimate aim for most phishers. Commonly speaking, where there is money, there is also crime.

4.2.2 Growth of Internet Users

The origins of the Internet and the World Wide Web can be found with the development of large communication networks by scientists in the USA in the early 1960s for use by the military. The first international network nodes were set up in England and Norway in 1973 (Pastor-Satorras and Vespignani, 2007). The World Wide Web was launched on the Internet at large in 1991 where countries with established Internet connections, such as the USA and UK could make immediate use of it (W3C, 2010). The arrival of Internet technology in the State of Qatar was significantly later, in 1996, and it was the last country in the Gulf to establish the Internet (Table 4.2).

Table 4.2: Year of Internet access for UK and Gulf States (Kalathil and Boas, 2003)

Country	Internet First Access
UK	1973
Kuwait	1992
UAE	1993
Saudi Arabia	1994
Bahrain	1995
Qatar	1996

In 2008, approximately 0.4 million people in Qatar logged on to the Internet for various reasons, some for gaining information, others for online shopping or electronic services and so on (CIA, 2008a). The UK growth rate in Internet users in the period 2000 - 2009 was about 203%, which is not extremely large, whereas a very rapid rate of development in Qatar has led to a huge boost in its users and a growth of 1,353% was estimated from 2000 to 2009. Compared to its neighbouring countries in the GCC, Qatar comes next to Saudi Arabia in the growth of Internet usage; according to Internet World Stats (2009b), Qatar has a significant rate of Internet usage even though it was the last country in the GCC to access the Internet (see Table 4.3).

Table 4.3: Growth of Internet use in GCC and UK (Internet World Stats, 2009b)

GCC and UK	Growth of Internet Use (2000-2009)
Bahrain	907%
Kuwait	567%
Oman	417%
Saudi Arabia	3,750%
UAE	298%
Qatar	1,353%
UK	203%

This rapid growth in number of Internet users was due to many factors, as discussed in the next section.

4.2.2.1 Telecommunications' Development

Since Qatar is an important connecting link in the world telecommunications network, there have been huge developments in the telecommunications' field, postal services and transportation (Ministry of Foreign Affairs, 2007b; INTELSAT, 2010). This has led this sector to being independent and effective and therefore the Ministry of Communications and Transport was dissolved and three Emiri decrees were issued to set up the Civil Aviation Authority, Customs and Ports Authority and Postal Services Authority (Ministry of Foreign Affairs, 2007b).

Later, the Supreme Council for Information and Communication Technology (SCICT, ictQATAR) was established in August 2004 under the chairmanship of His Highness Sheikh Tamim bin Hamad Al-Thani, the Heir Apparent (Ministry of Foreign Affairs, 2007b). IctQATAR aspires to create an advanced knowledge-based society, developing and leading the national strategic vision relating to ICT initiatives in government, business, education, health, cyber security, market development and knowledge management (ICT Qatar, 2009a).

Also, Qatar Telecom (Q-Tel), since its establishment in 1987, has played a major role in the improvement of telecommunications in Qatar. Examples of main services supplied by Q-Tel were the establishment of the GSM network, Internet access, e-commerce and the launch of the fibre optics cable between Qatar and Saudi Arabia (Ministry of Foreign Affairs, 2007b).

Consequently, the telecommunications sector improved dramatically and the number of subscribers in telecommunication channels has increased noticeably. According to the CIA (2009), in 2007 the number of mobile telephone subscribers reached 1.264 million and fixed line reached 237,400.

According to the *Global Information Technology Report 2008-2009* (ICT Qatar, 2009f) Qatar has reached the top 30 in ICT with an enormous development experienced in governmental readiness and usage of ICT.

4.2.2.2 Education Development

An issue that has prompted the diffusion of the Internet in Qatar is the massive development in the education sector. According to H.H. Sheikha Mozah Bint Nasser Al Missned (2009), the Government of Qatar's declared policy is to consider education as the main foundation for development and that the quality of the individual as an asset is the most important element in the development process.

Education has been transformed dramatically since the establishment of official education in 1952. A comprehensive educational policy has improved it, based on the solid principles of the development of curricula and educational systems, continually seeking to benefit from the modern achievements, techniques and new educational experience, along with adherence to the heritage of the Islamic nation.

The Government launched an initiative to develop public education in the State of Qatar under the slogan "Education for a New Era", aiming to prepare Qatari citizens to keep pace with the requirements of economic and social development in Qatar and global changes through development of educational curricula (Ministry of Foreign Affairs, 2007c).

The government has focused on educational development and numerous educational projects were applied to make Qatar a centre of excellence in higher education and research (H.H. Sheikha Mozah Bint Nasser Al Missned, 2009). A huge investment was made in education and it was estimated in 2005 that 3.3% of GDP had been spent in the education sector (CIA,2009a).

H.H. Sheikha Mozah Bint Nasser Al Missned, the consort of H.H. the Emir of Qatar, has many roles within Qatar in regard to education. Her Highness considers human beings as one of the most important elements for the development of the State of Qatar (H.H. Sheikha Mozah Bint Nasser Al Missned, 2009). As a result, Qatar has achieved a noticeable increase in the number of students at all educational levels. This was accompanied by an increase in education inputs, such as schools, teachers and curricula. (QSA, 2008).

As a consequence of the educational development, the literacy rate in Qatar has improved. Among the GCC countries, as estimated in 2008, Qatar has the highest literacy rate at 93% (UNDP, 2009) (Table 4.4). In contrast, in 2003, it was estimated that the UK had a very high literacy rate of 99% (CIA, 2008b). There is a huge educational development and the literacy rate in Qatar has become relatively high, but it is still below the minimum average of 95% in the developed nations (AME info, 2004).

Table 4.4: Adult (age 15 and older) literacy rates in GCC countries and UK (UNDP, 2009)

Country	Literacy Rate %
Bahrain	89%
Kuwait	95%
Oman	84%
Saudi Arabia	85%
UAE	90%
Qatar	93%
UK	99%

In conclusion, the educational development has not only enhanced people's literacy but also their computer literacy, since ICT is one of the major subjects taught in schools and this, therefore, has led to an increased amount of Internet usage among students of young ages. While it is heartening to see that there is a huge evolution in education to build knowledgeable pupils in all sectors including ICT, this has raised the question of whether those young people are aware of Internet threats and, in particular, phishing.

4.2.2.3 Growth of Computer Literacy

Most of the organisations in Qatar are connected to the Internet since it is essential to their work. Therefore, computer skill has become a crucial requirement for most jobs.

Research by ictQatar has indicated that the Internet has become an essential element of daily operation for most (over 90%) businesses in Qatar. Khalid Al Mansouri, Executive Director of Qtel's Business Solutions, said, "Broadband technology provides the communications backbone for many of Qatar's key companies, enabling them to access international markets, and helping to increase the level of contact with customers, suppliers and stakeholders" (Qtel, 2009d). Therefore, the government has

attempted to enhance the computer literacy of Qatari citizens as it has become a crucial need for people to cope with the country's global and national development.

To enhance the computer literacy level for Qataris, computer skills and ICDL (International Computer Driving Licence) programmes were adopted for students and employees in Qatar (ICDL GCC Foundation, 2009). Since there was a huge demand for the ICDL programmes in the Gulf region, the ECDL (European Computer Driving Licence) Foundation has set up the ICDL GCC Foundation to execute the programmes in the Gulf Region with the help of certified bodies and the chief educational organisations in the region (ICDL GCC Foundation, 2009).

In conclusion, this growth has led in enhancing the usage of computers and Internet both at work and at home. However, this fast growth of computer literacy may have the consequence that a high percentage of the population have insufficient experience and knowledge of computing, and especially the threat of e-crimes.

4.2.2.4 Low Price of Internet Connection

In 2004, the Qatar government granted the Qatari Telecommunications Company 'Qtel' a 15-year monopoly on wire line and mobile telephone and cable television services and Internet service provision (Arabic Network for Human Rights Information, 2004). However, in June 2008, Vodafone Group Plc, won Qatar's second mobile networks' and services' licence. This has brought another company into the Qatar telecommunication market (AME Info, 2008; ICT Qatar, 2009b).

Vodafone in Qatar currently provides only a mobile network. Fixed lines and Internet are not yet offered but delivery is expected in the near future (Vodafone, 2009). Therefore, in this research, only Internet services offered by Q-Tel were evaluated to identify whether there is any difficulty in Internet access. The broadband and dial-up services were inspected in respect of Internet price, speed and features and the prices are converted into GBP sterling.

While Q-tel's vision is to reach the top 20 telecommunications companies in the world by 2020 (Qtel, 2009a), it has paid attention to improving its services and satisfying its

customers by providing superior and relatively low-cost services, especially after the entry of a big competitor to the market. The adoption of fostered competition in the telecommunications sector in Qatar has assisted in raising the products and services offered by telecommunication companies. Such an example was in April 2009, when Q-Tel Business users benefited from Free Internet Broadband Business ADSL Speed Upgrade (Qtel, 2009d).

The evaluation concluded that Qtel ADSL has high-speed Internet access, which provides downloads and streaming up to 2 Mbps. It offers a broadband speed of up to 8 Mbps with relatively cheap monthly subscription ranging from 200 to 600QR (about 33 to 99 GBP) with superior features and free installation fees for a one-year contract (Qtel, 2009b). In conclusion, the reduction of Internet access prices in Qatar has facilitated public access to the Internet.

4.2.2.5 Availability of Free Internet Access

To encourage Internet access in Qatar, ictQATAR and the Ministry of Municipal Affairs and Agriculture initiated in March 2007 Qatar's free wireless Internet access at public parks, known as 'ipark'. The launch of the ipark was a continuation of the efforts that the government is exerting for building up a modern society. The Minister of Municipal Affairs and Agriculture commented that the launch of the ipark project was required for the establishment of a modern society where all citizens are of concerned (ICT Qatar, 2009c).

Thus, the availability of free Internet access for the public has assisted in increasing the number of Internet users in Qatar.

4.2.2.6 Transformation to E-businesses

The GCC countries have considered e-commerce as a major concern that must be enhanced and paid attention to, as it has a huge impact on GCC commerce (GCC Secretariat General, 2001). The Ministerial Council of the Commercial Cooperation

Committee held in November 2005 discussed topics related to e-commerce such as the establishment of the GCC E-commerce Organisation and to issues like consumer protection against commercial limitation and cheating (GCC Secretariat-General, 2006).

As a result, today, Qatari citizens can accomplish their transactions and services through the Internet as e-services and e-commerce have been developed in the region. According to the newsletter of the Qatar Science and Technology Park, on-line services are leading to on-line shopping in Qatar. Shadi Eideh, senior manager of e-channels at the Qatar National Bank (QNB), oversees the development of electronic services in Qatar, especially in the banking sectors, where e-services have become essential due to the development of Qatar's economy and customers' demand. Currently, the banks provide e-services such as Internet banking and e-payment to utilities (QSTP, 2007).

Other organisations also provide e-services such as the Qatar share market, Qatar Airlines and hotels. Also, government institutes have devoted significant effort to provide e-services, for example e-education, e-health and e-government (ICT Qatar, 2009d). Use of e-services has increased and a good example is the Qatar e-government service called Hukoomi, where a considerable increase in the number of transactions was noticed throughout 2008 when it reached QR 428 million compared to QR 237 million, QR 79 million, QR 9 million for 2007, 2006 and 2005, respectively. Moreover, since its establishment in September 2000, the total revenues of e-government reached QR 930 million in 2005 (ICT Qatar, 2009e).

However, e-commerce in Qatar is still in a very initial stage. Khaled Tawfik, Enterprise Development Manager at the Supreme Council of Information and Communication Technology (ictQatar), has stated that e-commerce in Qatar is 'starting to scratch the surface' (QSTP, 2007) and added that e-commerce uptake will involve all organisations in raising the level of computer literacy and access in Qatar. This is being carried out by many institutes, such as QNB and iHorizons, which have initiated programmes to enhance computer literacy for their clients, as well as ictQatar which is committed to IT literacy and the ipark project to promote Internet access.

M. Takriti, Chief Executive Officer of iHorizons, explained the small size of the e-commerce sector in the region by the core dependence on outside vendors. He added that recent improvement in Qatar's education system, along with the enhancement of

computer literacy, will assist in boosting e-commerce in Qatar. Nevertheless, experts who expected a boost of interest in e-commerce with the persisting development of the economy in Qatar, have pointed out the need to raise public awareness of the benefits of e-commerce (Ashrafi et al., 2007; QSTP, 2007).

The level of B2C (business to customer) and B2B (business to business) e-commerce activity in Qatar was determined by a statistical study carried out as part of a GCC e-commerce study. The results show that the total B2C trade has improved and reached US \$54 million in 2005 compared to US \$27 million in 2002.

On the other hand, the study has estimated that the current total of B2B e-commerce, in which the automotive industry, the oil industry and the IT industry accounted for the bulk of the online transactions, reached US \$342 millions in 2005 (Ministry of Industry & Commerce, Kingdom of Bahrain, 2002). The level of B2B trade values in the GCC countries are shown in Table 4.5.

Thus this rapid transformation led to the growth in the number of Internet users shopping, using services and communicating online with organisations and institutes. However, this raises the same question again as to whether customers have the experience to be aware and ready for this rapid transformation and how they should protect themselves from phishing attempts.

Table 4.5: B2C and B2B trade values in Qatar (2005)

Estimated B2C value (USD millions)	Qatar
2002	\$27m
2005	\$54m
Estimated B2B value(USD millions)	Qatar
GDP 2001	\$34150m
B2B E-Commerce %	1%
B2B EC Value	\$342m

4.2.3 The Lack of Electronic Law

The legal framework in Qatar has passed through development phases in which the judiciary is an independent body. Previously, the judicial system was divided into two court systems: the civil, commercial and criminal courts and the Sharia courts which manage Islamic laws. Then, in October 2004, the new judiciary law was established where the previous two court systems merged into one and the Court of Cassation was established (Qatar Law Forum, 2009; Embassy of Qatar in Washington DC, 2005). Although the law in Qatar has been developed accordingly over several years, there is still no specific e-commerce law or e-law in Qatar.

Experts have indicated that continuous development of Qatar's economy will assist in enhancing e-commerce use and therefore there will inevitably be the establishment of an effective e-law. According to M. Takriti, Chief Executive Officer of iHorizons, some issues related to electronic law are: "How courts enforce contracts signed online via e-mail; whether e-mails are legally binding in online transactions; stealing e-commerce sites (also known as "phishing"); what kinds of e-commerce are allowed and what are not; and how taxation is determined among countries that have different taxation codes, particularly in the Arab world." (QSTP, 2007). Currently, ictQatar is concerned in establishing a law relating to e-commerce (e-law) which addresses all the challenges raised by e-commerce, including electronic transactions, digital signatures, electronic payments, data encryption, privacy and data protection, software protection, piracy and e-government (QSTP, 2007).

Furthermore, the GCC countries are planning for development of a western-based e-commerce law to protect the rights of online consumers. The governments of Bahrain and Kuwait are currently considering developing e-commerce law (Ministry of Industry & Commerce, Kingdom of Bahrain, 2002). However, in January 2006, UAE was the first Arab country to issue an e-law to legalise e-commerce and protect online consumers (Elsidafy, 2009).

The lack of e-law has assisted in motivating phishers to commit their crimes without fear of punishment, as there is no protection for Internet users. In this research interviews were held with legal experts in this field to discover how e-crimes are currently processed and the difficulties they face in the absence of any e-law.

4.2.4 Effect of Qatar Culture

One result of the rapid development and transformation in the State of Qatar in all sectors has been an imbalance in the population composition as Qatar has become an attractive place for a large numbers of foreign workers. They are attracted by the massive investment and jobs are available with no income tax and free services to the population. This has led to a growth in population from 369,000 in 1986 to 1.4 million in 2008 (QSA, 2008) (see Table 4.6), of whom, however, approximately 350,000 were believed to be Qatari citizens (United States Department of State, 2005). As a result, Qatar has become a multi-ethnic country with people of Arab, Indian, Pakistani, Iranian and other nationalities (CIA, 2008a).

Table 4.6: Population of Qatar (QSA, 2008)

Year	Population
1986	369079
1997	522023
2004	744029
2008	1448446

However, Qatar was able to maintain its heritage despite the enormous development in all areas and the influx of a large number of different communities. Because of the interest of the State of Qatar to preserve the heritage of its civilisation, the Ministry of Culture and the Arts was established on October 1998 to preserve the national legacy of heritage and archaeology (Ministry of Culture, Art and Heritage, 2008).

Qatar is a relatively conservative country where Islam is the main religion and 77.5% of the population are Muslims (CIA, 2008a; QSA, 2008; U.S. Department of State Diploma in Action, 2007). Customs, traditions and the Islamic religion are thus part of

the Qatari culture where Islam has a major influence on people's behaviour and responses in their daily life.

Despite all these changes in the Qatari society, the State of Qatar continues to maintain its culture, customs and characteristics. The author has experienced that Qataris, in general, are trustful, helpful and generous. This suggests there may be cultural factors which might affect the responses of Qatari citizens to e-mail phishing. Further investigations on this subject were carried out which showed that there are cultural factors that affect victims' responses to phishing which make them an easy prey for phishers.

4.3 Interviews

To further investigate the problems of e-mail phishing in Qatar, as there is a lack of literature on e-mail phishing in Qatar, interviews were held with thirteen domain experts in online fraud, awareness and education from both governmental and private sectors. The experts were drawn from various ministries and organisations as follows:

1. Head of Computer Crime at the Ministry of Interior in Qatar
2. Head of Public Relations in the Ministry of Interior in Qatar
3. A senior employee of an international bank based in Qatar.
- 4 and 5. Senior employees of Qatar Telecommunications (Q-Tel)
- 6, 7 & 8. Members of the Qatar Computer Emergency Response Team (Q-CERT)
9. A representative of the Ministry of Public Prosecution in Qatar
10. A member of the Ministry of Endowments and Islamic Affairs in Qatar.
11. A representative from the Ministry of Education and Higher Education in Qatar
12. A computer lecturer with the Institute of Administrative Development

13. The Chief of Operations, First Base Technologies, an e-crime consultancy company in the UK

The interviews aimed to identify the extent of e-mail phishing in Qatar, the problems of dealing with phishing in Qatar, the vulnerability of Qataris to phishing, including the effects of the national culture, and the legal situation regarding phishing in Qatar. Semi structured interviews were held with each of the thirteen interviewees. Questions on the above topics were asked depending on the interviewee's area of expertise but in each case they were given the freedom to expand on their answers and give further comments. The interviews were held in December 2009 with each interview being of twenty minutes to two hours in duration, except for the interview with the Chief of Operations of First Base Technologies which was conducted via e-mail. Full details of the interviews are given in Appendix B. The findings of the interviews are given in the following sections.

4.3.1 Extent of E-mail Phishing

According to the interviews with experts in the fields of e-crimes, education, awareness and Islamic studies, all of them had found that e-mail phishing has spiked recently and become of more concern. Although none had a definite statistical record of phishing attacks, they did think they were less successful since their organisations applied a strategy to defend against phishing involving a multi-layer defence of technological solutions, policies and awareness.

Nevertheless, the Head of Prosecution, Ministry of Public Prosecution, had noted that since this phenomenon began to appear from 2004, it has risen and criminals' intentions have extended from stealing victims' money and personal/confidential information to exploiting and blackmailing victims for political and terrorist ends. Interviews with the Officer of the Computer Crimes Unit, a Manager of the PR Department in the Ministry of Interior (MOI) and Q-cert employees have pointed out that most attacks were targeting financial sectors such as banks.

For the Manager of an ISP and the network engineer in Qtel, the attacks were fewer, about 4 cases per month, and phishing by phone, websites, e-mails and SMS were the most common attacks they had encountered. They stated that they had met a couple of incidents in Qatar where an attacker had mimicked banks, hacked into a website server and hosted his/her own phishing site.

Furthermore, the Manager of Operation Risk at the Doha Bank pointed out that the first phishing attack they suffered was on March 2008 and since then they had experienced an average of two per month. However, he added, that had stopped in November 2008 due to implementation of some security measures.

Almost all of the interviewees believe that the rapid development which Qatar has experienced in the last few years in all fields - economic, politics, telecommunication and others - makes Qatar vulnerable to cyber crimes. In particular, development in the economy and ICT has encouraged the existence and the development of the phishing problem in Qatar. They believe Qatar is attractive for phishers with the availability of a lot of money and with online users who are novices to the Internet and most likely do not know the risks associated with it. However, some commented that this does not mean the country has to stop developing.

4.3.2 Vulnerability to Phishing

The majority of interviewees believed that people are still not sufficiently aware of phishing, they still get fooled by the simple attacks and therefore more effort has to be made to enhance awareness on how to protect themselves against such attack, how to recognise it and how to react. The interviewees at Q-CERT stressed that it is hard to measure security awareness.

Also, the Head of Prosecution noted that the modernisation of Qatar is new for people and most are not well practised in this new development, especially in technology, which then leads to huge vulnerabilities. The experts believe that the society needs time

to absorb such huge developments in the country and by the time people get used to such changes they will be more aware, since the government and institutions in Qatar are trying to defend against such attacks by making people aware and enhancing the security measures.

All of the interviewees noted that Qatari culture has an effect on people's responses to phishing attacks, since Qataris are living in a conservative society with a collection of traditions, customs and religious beliefs which have become part of their culture. Furthermore, most Qataris are religious and follow Islamic beliefs in being moral, doing good, treating people nicely, trusting them and helping them when required. Therefore when phishers use factors which play upon their kindness, goodness, trust, morals, emotions and religion then Qataris tend to believe them. Also, Qataris in general are generous, trustful and helpful, so this would be used by phishers to fool them. In addition, the interviewees said that phishers will usually study the culture of Qatar before committing their attacks and because Qatar is a trusted environment, people feel they are safe.

Some of the interviewees mentioned that there are no specific criteria for victims of phishing, nearly all categories can fall prey and can be vulnerable, regardless of their backgrounds, and even experts in security could fail victims, especially if the phishing convinces them by engaging their interests. Also, they added that phishers try to trick victims by using clever techniques to bypass the spam filters.

4.3.3 Problems Faced with Phishing Incidents

The officer in the Computer Crime Unit in the MOI and the Head of Prosecution stated that there is no clearly assigned e-law in Qatar. However, in Penalties Law No.11 of 2004, there is a small section about computer crimes on pages 142-147 (Ministry of Public Prosecution, 2004). However, it does not cover all types of fraud existing today, only general topics such as viruses, misuse of data or computers and unauthorised access. It does not even criminalise e-mail phishing attacks, it only criminalises viruses

which are distributed through floppy disk and CDs. Therefore, when phishing cases go to the court, there is not actually an explicit law to make phishing punishable because the law is quite old and was not planned very well. Furthermore, the experts stated that phishers are taking advantage of the lack of e-law in Qatar and, therefore, the establishment of a special law on cyber crime would be essential to reduce e-crimes in Qatar and, in particular, phishing, while noting the need to modify it frequently to cope with the fast development in technology. Currently, Q-CERT is in the process of developing a new specialist law on e-crimes in collaboration with all relevant bodies seeking access to a comprehensive law to cover all aspects to suit current and future developments. The law covers almost all issues associated with Internet usage including topics such as misuse of devices, cyber crime, computer-related fraud and others. The Q-CERT experts noted that, although Qatar has delayed in the establishing of its e-law, it has learned from others' mistakes and experience in e-law. The majority of interviewees believed that the new law will protect victims and help to support decision, noting the common Qatari saying, "When there's no punishment, people get awful ill-mannered".

The officer in the MOI noted that some banks do not report phishing incidents since they think it might affect their reputations even though they were asked to report any incident to the Qatar Central Bank (QCB) to take further action. Also, they face difficulties in the investigation of phishing crimes, especially in proving the good faith of the accusers, since phishers usually try to take advantage of victims in Qatar without their knowledge (e.g. by getting their PCs infected, stealing their identity or impersonating them for committing their crime).

Also, the Head of Prosecution had mentioned that many victims do not report phishing incidents to avoid embarrassment and being ridiculed but also most were unaware of the right actions to take at the crisis time. Moreover, they face a problem in tracing phishers, since usually the stolen money is integrally transferred abroad in a mesh, which makes it difficult to catch the phisher, especially when the investigation leads to countries such as China, Nigeria and Russia, where cooperation is ineffective in tracking those attacks. The interviews at the Doha Bank and Q-CERT have shown that there are some phishing attacks committed inside Qatar, especially in iparks since there is no control over the users.

Qtel has experienced some difficulties in blocking websites outside Qatar from the web host as some refuse since it affects their business and reputation, therefore Q-CERT will be required to communicate with the equivalent computer emergency response team in the country concerned to request the blocking of the phishing site. However, in some countries such as Nigeria, there is no equivalent institute, so it would be hard to block and, in that case, Qtel can only block their clients from viewing the site in Qatar. Q-CERT noted that even if sites are blocked, phishers will launch again with a new site.

4.3.4 Cooperation Between Organisations

Victims usually report phishing incidents to their organisations, banks, telecommunication service provider or Q-CERT, which then report them to the Computer Crime Unit in the MOI for investigation and action, then the case is referred to the Ministry of Public Prosecution to proceed with the case (see Figure 4.2). The ministry will refer to Qtel in some cases where there is a need to block a certain website or IP. Similarly, there is cooperation between Q-CERT and Qtel in this matter since Q-CERT is registered with the APWG (AntiPhishing Working Group) and computer emergency response institutes around the world. Q-CERT has also directed the ‘Honey Pot project’ in Qatar (Spitzner, 2002).

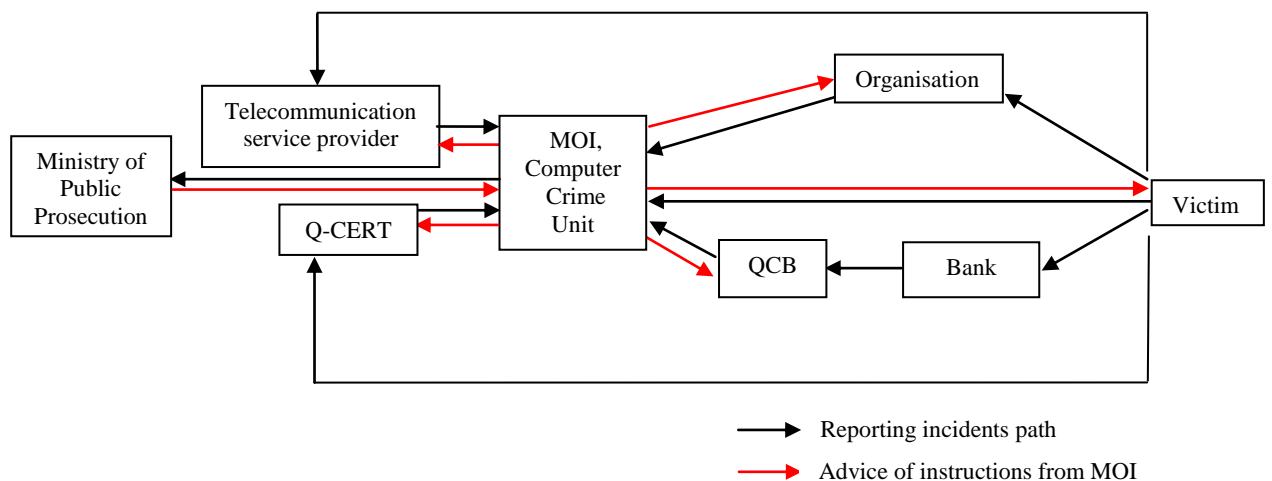


Figure 4.2: Process of dealing with phishing incidents

4.3.5 Review of Organisational Strategy of Defence Against Phishing

All organisations interviewed have a planned strategy to defend against e-crimes in general by providing layers of protection from the technological solutions (either hardware or software) policies and awareness. Most of the experts stated that spam filters are not reliable and some phishing attacks might bypass them, and therefore it is important to educate their employees and clients on how to recognise phishing attempts and to react effectively. The Head of Prosecution reported he is working to limit phishing by awareness, enhancement of laws that criminalise this phenomenon, participation in related conferences and cooperation with other countries and all competent authorities to limit this phenomenon.

The Doha bank has taken some actions to prevent phishing attacks, such as creating the need for 24 hours to activate accounts added as a third-party account on the client side, reducing the limit of daily transactions from 50,000 to 40,000 QR, by default not allowing transactions over the phone, providing SMS services for clients for any transactions in their account and increasing the level of security in online banking by involving randomised security questions and virtual keyboards which protect the user from Trojan programs intended to capture user key strokes.

In addition, the interview with the voluntary administrator of the Ministry of Endowments and Islamic Affairs revealed that the ministry has closed a lot of suspicious charity centres. The ministry has established a licence system which allows some charities and Red Crescent Societies to collect charity and ‘Zakat’ (see Appendix C, p.365) from individuals and institutions once they have passed rigorous checks to ensure they are not associated with criminal or terrorist organisations. As a further check, delegates have been assigned in many countries to verify the arrival of donated funds for eligible applicants. The ministry stresses to people they should donate only to accredited institutes and individuals. However, the interviewee pointed out that enhancing awareness on the topic could have a negative impact on those in need since it

could create a kind of lack of confidence in any message received, even if it was correct and genuine.

None of the interviewed organisations in Qatar would hold a phishing penetration test to assess their employees' or clients' level of awareness of phishing, some were, perhaps, overconfident in the awareness level of their employees, but others said it would be hard to implement as it would require high level authorisation. Most were concerned about the ethical and legal issues that might be associated with such an audit and some pointed out that this might affect employees' trust in their organisation, and that there is also a possibility that phishers might utilise this by sending the same e-mail which instead will direct victims to a malicious website. The Head of Prosecution noted that penetration tests could be legal if it was mentioned in their employment contract but there are ethical issues that should be taken into consideration regarding employees'.

The Chief of Operations at First Base Technologies stated that it is hard to protect against phishing since people are vulnerable because phishers are using clever tricks which are difficult to identify, and there is a lack of awareness and training about phishing. The company carries out penetration tests, explains guidelines and policies for employees and provides awareness and education on best practice through seminars, videos and publications, which will usually take up to one hour. Their best practice includes never clicking on a link in an e-mail but instead browsing to the site manually, and if in doubt, checking the e-mail message headers and turning on the anti-phishing function in the Internet browser with the NoScript plug in.

4.3.6 Process Deployed for Awareness

All the interviewed organisations emphasised the importance of awareness of phishing since people are the weakest link. Q-CERT is responsible to develop an aware community with regard to ICT, and the PR department in the MOI is responsible for enhancing awareness of the public on various topics, one of which is phishing (Nagy, 2009). The PR department stated that they have to deal with the matter cautiously to

avoid intimidating society, as the people are conservative and have ethical and religious beliefs.

Most of the interviewed organisations showed that they have diffused awareness on e-crimes, including phishing, by using various techniques: e-learning, seminars, exhibitions, publications, posters, leaflets, newsletters, SMS, e-mail and media (TV programmes, newspapers). Although all were found an effective way of education against phishing, the majority of experts emphasised the media since it reaches a high proportion of people. In addition, most interviewees agreed that an anti-phishing game is an interesting idea for achieving an effective and motivating awareness, especially for children.

Q-CERT added that ictQATAR, a cooperative member in the development of the Child Online Protection initiative, had conducted an awareness workshop to protect Qatar's children from cyber crime in cooperation with the International Telecommunications Union (ITU) as an initiative for the Telecommunications and Information Society Day (Al Jaber, 2009). In addition, ictQATAR cooperates with the Supreme Education Council (SEC) and private schools in Qatar in conducting workshops in Arabic and English. Currently, QCERT is developing an awareness campaign called K2-12 Cyber Safety Curriculum for schools in cooperation with SEC, the Council of Family Affairs and ITU. It aims to address the gap between the heavy use of technology in schools and the knowledge of how to use it safely. It covers the topics of Cyber Community Citizenship, Online Personal Safety, Cyber Predator Identification, Cyber Security and Intellectual property.

However, the Director of one of the high schools in Qatar in the Ministry of Education and Higher Education opposed the inclusion of awareness of phishing in the curriculum, since it is contrary to the values and principles that the Ministry tries to instil in the students, such as trust and kindness. She added that the Ministry is trying to make students aware away from the curriculum by bringing in with other organisations in this field such as the Ministry of Interior and ICT to hold seminars and workshops in schools. Furthermore, she noted the awareness should be planned with a clear aim and objectives, taking account of participants' background, by providing interactive and interesting awareness tools to keep people engrossed and by awarding a certificate of approval. She also suggested that personal observations, simple tests, questionnaires and

interviews held with participants might in evaluating the effectiveness of the awareness programme. She added that the difficulty in assessing the effectiveness of an awareness programme and in getting people to remember what they learned depends on the participants' personalities. and therefore research has been done in this area.

One of the Computer lecturers at the Institute of Administrative Development, an institute responsible for staff development in Qatar, stated that employers are responsible for providing security awareness training programmes for their employees, especially on phishing and e-crimes.

4.4 Summary

This chapter shows the existence of the e-mail phishing problem in Qatar. Due to the massive development in the Qatar economy, the availability of huge numbers of online users, the absence of electronic law and the effect of culture, Qatar was found to be an attractive place for phishers to commit their attacks (see Figure 4.3).

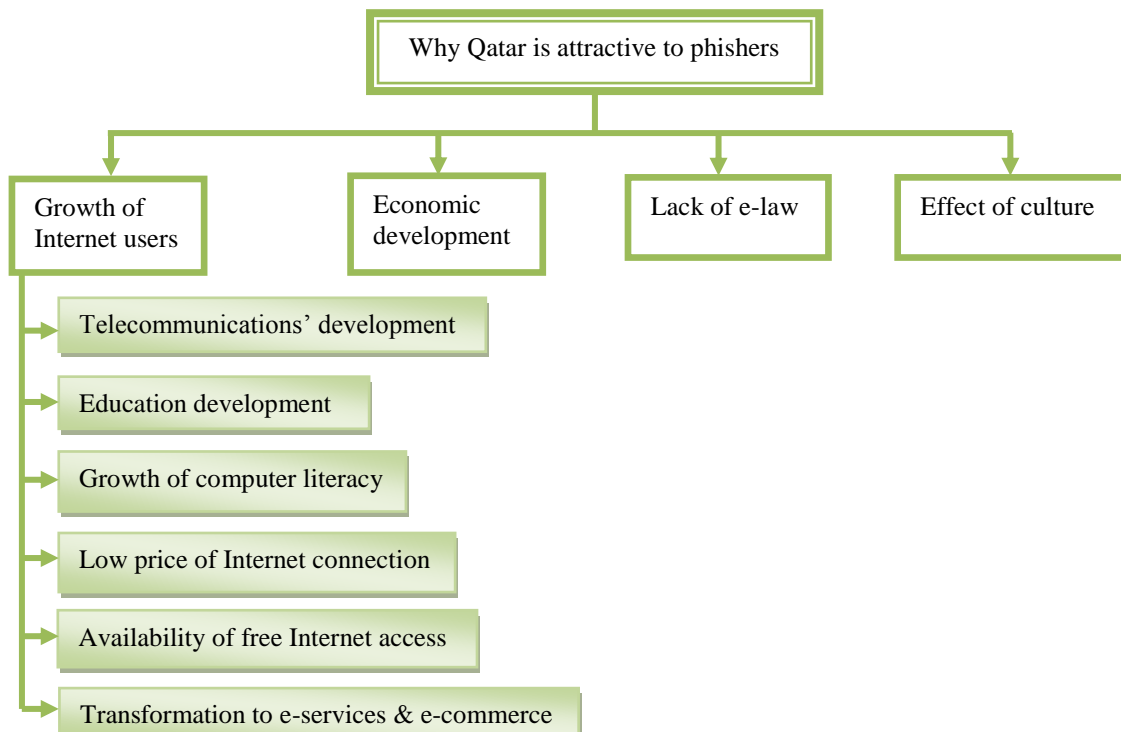


Figure 4.3: Why Qatar is attractive to phishers

This was supported by interviews with experts. However, they believed that although there is a high frequency of e-mail phishing in Qatar, incidents have been reduced recently where some organisations have adopted a strategy of defence against phishing by applying technological solutions and policies and focusing on awareness and education. It was agreed that awareness would be a more effective means of defence since technological solutions have been found to be unreliable against the clever tricks phishers use to bypass technological solutions. Although there is a clear cooperation between organisations in Qatar to deal with phishing incidents, there are still some problems encountered, for example in blocking phishing sites, getting hold of phishers and proving the innocence of the victims of identity theft. However, the main concern of this research is to focus on awareness so it does not cover these problems, although it is worthwhile to point them out.

Interviews have given a clue to various techniques organisations use in developing awareness, including e-learning, seminars, exhibitions, publications, posters, leaflets, SMS, e-mail and media, with an emphasis on the latter and on the idea of developing an anti-phishing game. Also, experts in education have pointed to the importance of developing an effective awareness programme that is well planned and interesting, and this will be considered in the development of the e-mail phishing awareness framework.

The majority of interviewees believed that Qataris are vulnerable to phishing because they are not sufficiently aware of it. Interviews with experts have concluded with identifying some of the aspects which make Qatari citizens susceptible to phishing, as follows:

- The nature of Qataris is to feel embarrassed and stupid to mention or report phishing and that they have fallen prey to it.
- There is a lack of clear e-law in Qatar to protect people from electronic crimes.
- The majority of people are still not sufficiently aware of phishing. Most do not know how to protect themselves against phishing attacks and how to detect and react to phishing. With the rapid development experienced in Qatar many Qataris

become susceptible to phishing because they have not absorbed sufficiently the technology revolution

- Qatar culture has an effect on people's falling prey to e-mail phishing attacks (Further investigated in Chapter 6).
- Qataris are trustful, religious, helpful, generous, emotional and good-willed therefore they could be vulnerable to phishing which exploit these characteristics.

In addition, interviews with experts revealed that there are no specific criteria for victims of phishing, especially if the phishing convinces them by engaging their interests. This will be examined more in the following chapter (penetration tests and laboratory experiment). The interviewees stated that culture has an effect on people's falling prey to e-mail phishing attacks, especially when phishers exploit their virtuous qualities and this is going to be examined in depth in the next chapters on the survey and the reality and experimental studies.

The next chapter presents the survey data collection method by means of a questionnaire used in Qatar and the UK and interviews with Qatari e-mail users. The survey outcome outlines the level of the e-mail phishing problem in Qatar society, the level of awareness of Qataris, along with possible methods to defend against attacks. The next chapter also examines the significance of the results of the survey made in Qatar and the UK.

Chapter 5 Surveying Awareness of Phishing

This chapter describes the survey data collection. It begins by defining the survey aim and sampling criteria. Next, it describes the survey planning, design and execution. Finally, it concludes with a quantitative and qualitative data analysis of the survey to discover the extent of the e-mail phishing problem in Qatar society, how to defend against it and the possible cultural and country-specific factors which make this problem arise.

5.1 Questionnaire Aim

The ultimate aim of the questionnaire is to draw a profile of Qatari people's awareness of e-mail phishing and their views on the best method of defence against this attack compared to the views of people in other developed nations such as the UK. The survey will gauge people's knowledge about e-mail phishing, give a good indication of their vulnerability to this threat and define the extent of the problem by presenting a profile of the number of people who have been attacked by e-mail phishing. In addition, it reveals their views on the best way they propose to defend against phishing attacks and, in particular, what they believe is the most effective tool to deploy and to embed awareness and education about e-mail phishing attacks.

5.2 Questionnaire Sampling

Leedy (1997: 219) argues, "...the two elements that are more important than any others in survey research are randomization and bias", and "...the descriptive survey method demands that the researcher select from the general population a sample population that will be both logically and statistically defensible". According to Bryman and Cramer (1990: 99), "...researchers should strive to create, as accurate as possible, a representative sample of the general population or case of study, and that such sample, if planned precisely, will highly increase the external validity of the research". In addition, according to Bryman and Cramer (1990), "...the researcher should divide the population into strata. The strata must be categories of a criterion."

This research has taken into consideration the above points in defining an accurate sample for study. The sample was first narrowed down from the general public of the UK and Qatar to a more focused sector of the society. The aim was to define criteria for users most likely to fall prey to e-mail phishing attacks. Participants were chosen randomly from the focused sector of British and Qatari society and the criteria were used to refine the sample. The criteria set for inclusion in the questionnaire were only those people who use the Internet and have an e-mail address because they are the potential e-mail phishing victims. To further narrow inclusion, people aged 12 and above were defined to fulfil the criteria. Other segments of UK and Qatari society (e.g. children) were not involved because they are not potential victims and can not provide clear decisions about the phenomenon investigated. In conclusion, participants were randomly selected from UK and Qatari citizens using the adopted criteria (e-mail users aged over 12).

5.3 Questionnaire Planning and Design

Punch (2003) states that “Developing the questionnaire operationalises the research questions”; therefore the questionnaire template (see Appendix A) was developed with the consideration of the research questions. There is extensive literature on surveys which discusses the design of questionnaires (e.g. Jeffrey, 1986; Fischer and Rohs, 1985; Sudman, 1982; Babbie, 1973). In addition, Leedy (1997) has defined four practical guidelines in developing a questionnaire, as follows:

1. Using clear language
2. Meeting research aims
3. Planning development, sample, distribution and collection
4. Creating a solid cover letter

Although designing a perfect questionnaire is impossible, the study does, however, follow the above guidelines in the case of this questionnaire. It was designed and developed to provide answers to the research questions and concerns and used simple

language. Since the survey was targeted at Qatari and British e-mail users over 12, two versions of the survey were designed, in English and Arabic, as they are the official languages in the UK and Qatar, respectively. However, respondents had a choice of version. Before achieving the ultimate design, this questionnaire passed through first review and pilot-test towards providing an effective questionnaire. Each stage is explained below:

5.3.1 First Review

Reviewing the questionnaire first, before field application, helps in creating an enhanced questionnaire, fit for purpose. Therefore, it was reviewed by researchers and domain experts to assist in determining its strengths and weaknesses. The researchers were Dawson, Professor of Knowledge Management at Loughborough University, and Benkhalil, Post-Doctoral Research Assistant and Teaching Fellow at Bradford University. The experts in the domain of information security also involved were Lethold, Head of Middle East Operations at InfoGuard, a Swiss company specialised in information security. Other experts were employees of Q-CERT (Qatar Computer Emergency Response Team) which is Qatar's coordination centre for dealing with internet security problems. These were Lewis, Deputy Director of Q-CERT, Mundie, Q-CERT's manager for Outreach and Training, and Phelps, an information scientist working with Outreach and Training. The review took a couple of weeks as it involved discussions with the researchers and domain experts to plan an effective questionnaire.

Following the review, the questionnaire was refined accordingly. The major outcome was some corrections in the language, suggestions for a cover letter and some changes in the questionnaire format (see Appendix A). A short, simple cover letter was created to notify the participants of the aims, significance of the research and the targeted group and to verify the privacy and the confidentiality of the questionnaire. The cover letter was written both in simple English and Arabic language and attached to the questionnaire to encourage recipients to respond honestly. Since it was difficult to inspect each participant to determine whether he/she fitted the defined questionnaire criteria (i.e. e-mail users above 12 years, who are either Qatari or British citizens), the cover letter clarified the questionnaire criteria.

5.3.2 Pilot-test

Although the questionnaire had been refined by experts, to achieve an efficient questionnaire it was crucial for the draft questionnaire to be completed by a sample of Qatari and British people fitting the criteria similar to the final respondents. Later, in a semi-structured interview, participants were asked to provide their feedback on the questionnaire regarding simplicity, structure, length and design, along with some questions from the Salant and Dillman (1994) method of pilot testing. Finally, the questionnaire was evaluated according to the answers to the following questions:

- Were all questions clear and simple? If not, then please specify which ones were unclear or hard to understand?
- Did you find the questionnaire is well structured (i.e. has a clear and attractive layout)? If not, what is your criticism?
- Was the questionnaire too long or was it reasonable?
- Did you have the chance to answer all of the questions?
- Have you any other comments?

Salant and Dillman (1994) used:

- Does the question measure what it needs to measure?
- Do respondents understand all the words?
- Are questions interpreted similarly by all respondents?
- Does each closed-ended question have an answer that applies to each respondent?
- Does the questionnaire create a positive impression, one that motivates people to answer it?

Both the Arabic and English versions of the questionnaire were pilot-tested with 20 people of different ages and levels of education with a view to creating an effective and understandable final questionnaire. The conclusion of the pilot-test was that the majority of participants found the questionnaire somewhat long and contained too many questions. Therefore, the author removed some of the unnecessary questions and merged some into another related question. Finally, the questionnaire was shortened to two pages instead of four, which the pilot test indicated would be more realistic (see Appendix A). Also, the author observed that during the pilot phase, most participants

went immediately to the questionnaire questions without reading the cover letter, therefore it was decided to include the questionnaire criteria as questions within the questionnaire in order to include only appropriate participants and to exclude those not meeting the criteria.

5.4 Questionnaire Structure

The questionnaire was divided into different sections according to the required information to assist both the participants in reading and completion of the questionnaire and the author in analysing the questionnaire and drawing associated conclusions. The questionnaire consisted of 20 simple questions relating to e-mail phishing, some of which were closed-ended, such as yes/no multiple choices, and others were open-ended. Also, there were some contingency questions. The questionnaire had a structured response format with graphical user interface (GUI) of radio buttons, check boxes and text fields. The ultimate aim of the questionnaire was to draw a profile of people's awareness of e-mail phishing and their views on the best method of defence against this attack, therefore the questionnaire consisted of six sections, each contributing to the aim of the whole questionnaire.

The first section requested background information from the respondent, which although useful for questionnaire analysis, was also used to determine participant inclusion in or exclusion from the questionnaire results, according to the criteria explained above, to provide a fair analysis. The decision tree for determining appropriate inclusion is explained in Figure 5.1 below. In addition, this section contained an e-mail request, where participants would be asked to disclose their e-mail address if they would like to receive more information about phishing, the research topic. This actually had a hidden purpose designed to survey participants' willingness to disclose their private information (e-mail address) in a kind of penetration test to measure people's vulnerability to e-mail phishing in reality.

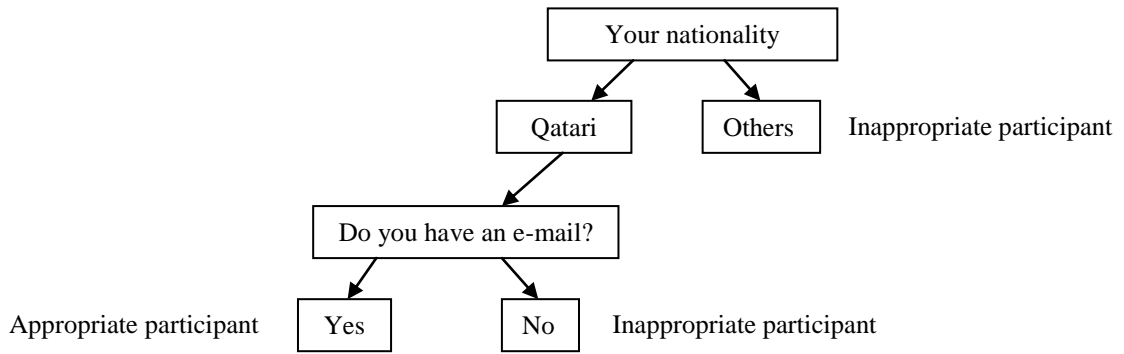


Figure 5.1: Decision tree for determining appropriate participants

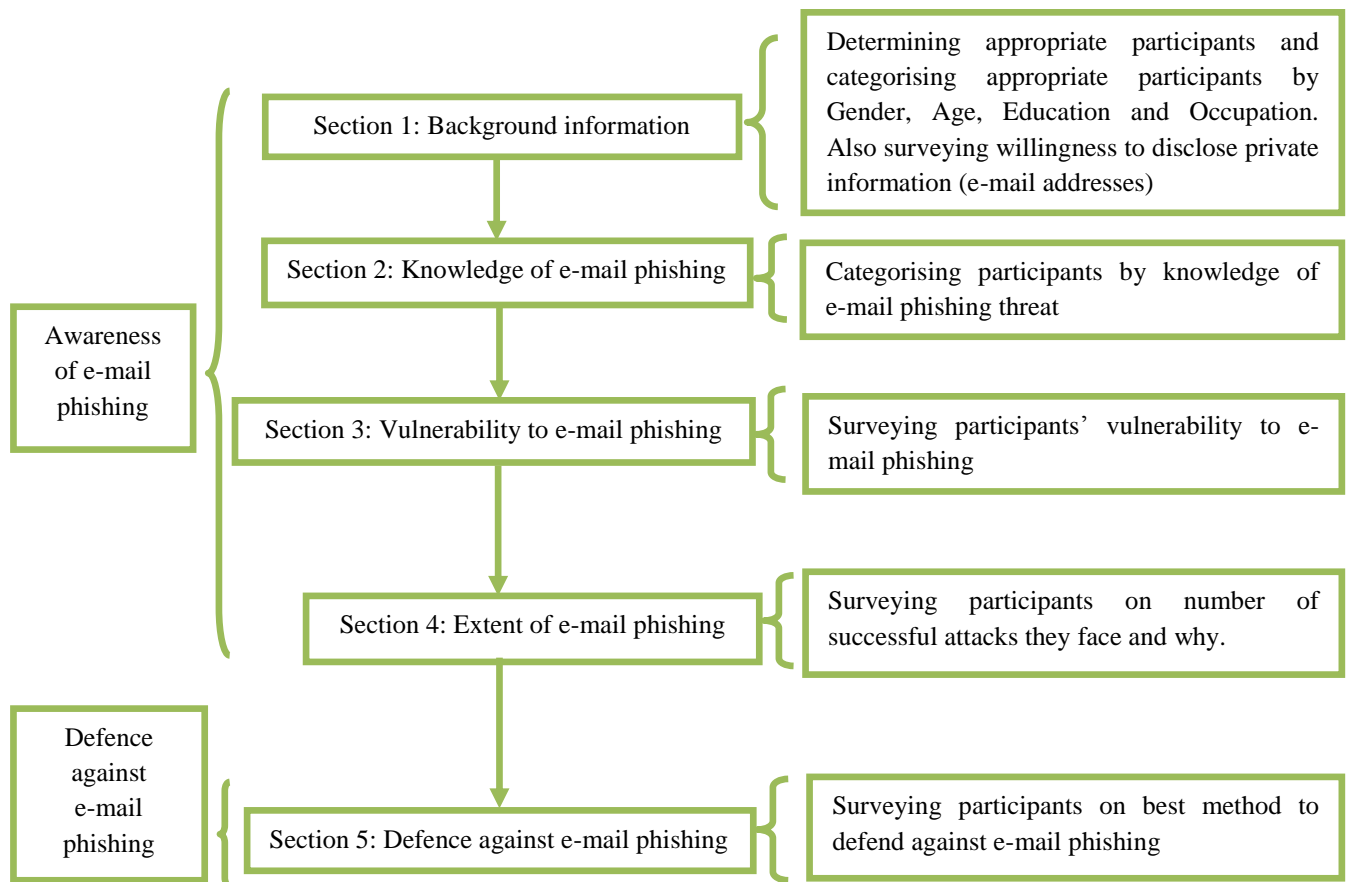


Figure 5.2: Questionnaire structure

Sections 1, 2, and 4 contribute towards drawing a profile of people’s awareness of e-mail phishing, whereas section 5 draws a profile of their views on the best method of defence against e-mail phishing. Figure 5.2 represents the outline of the questionnaire along with the aim and the sequence of each section within the questionnaire (see Appendix A for fuller details about the questionnaire design).

5.5 Questionnaire Implementation

Participants were randomly selected using the above-mentioned criteria (e-mail users over 12, either Qatari or British citizens). There is a wide range of questionnaire formats, e.g. written, oral and electronic questionnaires, and these can be distributed using a variety of media. In this research, the questionnaire uses the household drop-off and pick-up and online types of questionnaire. In the household drop-off, the author went to the respondent's home or organisation and handed over the questionnaire and then picked it up once completed. With this approach, the respondent could work on the questionnaire in private, when it is convenient and the author could make personal contact, answer questions and give clarification about the study. On the other hand, online questionnaires provide another option where the author would e-mail the organisation or respondents a description of the survey along with a link to the survey (Trochim, 2006)

The online questionnaire was created from a free online survey software tool available from (<http://freeonlinesurveys.com>). This website allows users to create their own online website survey easily without the need to install any software. Also, it offers live results collected automatically from the website with the features of customisation and filtering the results. The filter feature provided an in-depth quantitative analysis of the questionnaire results. The author used this feature in the questionnaire analysis phase to provide a comprehensive quantitative analysis as it can be used to filter, for example, an age group to see their response in the questionnaire.

In general, the online questionnaire provides more flexibility in processing the questionnaire results and also flexibility for some organisations which prefer to complete an electronic form of survey rather than to do it manually since it is faster and needs less effort. It is reasonable to assume that this would increase the response to the survey.

The questionnaires were distributed in Qatar and the UK to organisations in the private and public sectors. They were contacted before distributing the questionnaires to confirm their support for the research. The organisations which offered to distribute and collect the questionnaires were chosen.

5.5.1 Sample Size

The following equation (Bock et al., 2007: 442- 443) was applied to find the sample size:

$$ME = z \times \sqrt{\frac{\hat{p}\hat{q}}{n}}$$

where z = z value, n = sample size, \hat{p} = population proportion and ME = margin of error, which identifies the chance of error. To ensure an accurate result, the researcher used 3.1% as a smaller chance of error. Confidence level defines certainty level; levels of 95% or 99% are more common. The 95% certainty level was used in this analysis with a 95% confidence $\frac{z\alpha}{2}$ level and $\alpha = 5\%$ (level of significance). Therefore, $\alpha/2 = 0.025$ and to the right of $z = 0$, $=0.5 - 0.025 = 0.475$. Looking at the standard z distribution table, $z = 1.96$. Values of \hat{p} and \hat{q} were estimated, for the worst case, the value of $\hat{p} = 0.5$ (maximum variability) will define the largest sample necessary regardless of the true proportion. Similarly, $\hat{q} = 0.5$ since $\hat{q} = 1 - \hat{p}$.

$$0.031 = 1.96 \times \sqrt{\frac{0.5 \times 0.5}{n}}$$

$$n = 999.4$$

This shows at least 1000 respondents are required both in Qatar and the UK to keep the margin of error 3.1% with confidence level of 95% and $\pm 5\%$ precision.

5.5.2 Participant Contribution

In both the UK and Qatar, about 2,000 paper-based questionnaires were distributed manually to those organisations which confirmed their support, along with the online questionnaires distributed through e-mail. Within the collection phase, 20 respondents with different backgrounds were interviewed using a semi-structured interview based on

their point of view on the subject area and on their responses to the survey in order to have a better understanding of participants' responses.

The questionnaires were managed and tracked by the author to enhance the response rate. Good support was obtained from the participating organisations and the response rate was about 50%, much higher than usual in a survey investigation. In the results' gathering phase, all the hard copy questionnaires were collected and entered by the author into the online survey to gather the entire questionnaire results into a single database source. Finally, 1,200 participants contributed to the questionnaire both in UK and Qatar. Afterwards, the filtering feature in the online survey was used to exclude participants not meeting the questionnaire criteria explained above (see Figure 5.1). As a result, only 1,000 UK citizens and similarly 1,000 Qatari citizens of E-mail users participated in the questionnaire. This implies that the researcher had reached the minimum sample size defined for margin of 3.1% with confidence level of 95%.

This high response was due to the support giving by the organisations to the research, the use of different survey types, online and hard copy and to the offer of chocolate for participants which promoted people's contribution to the survey. This idea was taken from Wagner's (2004) 'Will Trade Passwords for Chocolate', which shows that more than 70% of the subjects would reveal their password in exchange for a piece of chocolate. However, this technique was not applied for the online survey.

Generally, these were government officials, private sector employees, businessmen/women, university lecturers and students, and secondary and primary school students (see Appendix A for fuller details about participants). The questionnaire in Qatar has taken advantage of the researcher's large family, friends, personal contact with the organisations and ICT Qatar support with communication with other Qatari organisations. The questionnaire in the UK has taken advantage of friends, neighbours, people in public areas such as restaurants and towns and personal contacts with organisations and the support of the Qatar Embassy in distributing the online survey to all Qatari students in the UK.

5.6 Survey Analysis

The analysis of the investigative survey allows the combination of findings from both quantitative and qualitative data in order to create an initiative for developing an anti-phishing awareness and an educational framework regarding e-mail phishing.

The analysis began by identifying the general responses of the questionnaire along with analysis of some of the participants interviewed. Later, in-depth analysis applied correlation to discover possible relationships between key variables. Also, the results of interviews with Qatari participants and domain experts were used to elaborate on the findings from the questionnaires.

5.6.1 Questionnaire Analysis

The research followed Punch's (2003) three main principles for quantitative data analysis of creating variables, distributing variables across the sample and creating relationships.

In the questionnaire structure in Figure 5.2, each section generates a number of variables drawn from its aims as follows:

1. Background information: nationality, e-mail user, e-mail address, gender, age, education and occupation. However, nationality and e-mail user are variables used only to determine suitable respondents for this questionnaire. Although the request for e-mail address is in the background information, it is really used to detect people's vulnerability to e-mail phishing. The request is there to lead participants into revealing their e-mail addresses as if part of the survey data collection, but in fact it reveals willingness to disclose their private information (e-mail address) and is therefore a kind of penetration test to measure people's vulnerability to e-mail phishing, in reality without obligation. Therefore, the e-mail request is considered a crucial variable of vulnerability to e-mail phishing.
2. Knowledge of e-mail phishing: Forecast of e-mail phishing trend, e-mail phishing level of knowledge and its source.

3. Vulnerability to e-mail phishing: Participants' worries about e-mail phishing, usage of anti-phishing software, ability to detect a phishing attack, their procedure once attacked and their own divulging of their e-mail addresses.
4. Extent of e-mail phishing: Number of phishing e-mails received by participants, number of times participants have been tricked and the reason for being tricked.
5. Defence against e-mail phishing: Efficiency of existing anti-phishing software, the best way for participants to defend themselves against e-mail phishing and their preferred method of being made aware of and educated about this attack. Each method of awareness creation listed constitutes a variable to be addressed in the analysis stage.

The general analysis used basic frequency distribution to illustrate the characteristics of the survey participants according to the defined questionnaire variables. Further, the in-depth analysis identified the possible relationships between the above variables. Moreover, the findings from interviews with 20 of the Qatari survey participants extended and gave further details about the survey outcome.

5.6.1.1 General Analysis of the Qatar Questionnaire

General quantitative analysis of the questionnaire was made in relation to the variables defined in Section 5.6.1. Details of the analysis are explained below.

1. Background information

The questionnaire survey involved 1,000 Qatari e-mail users; most were female, with the highest number of participants in the age group 18-29. In addition, the majority were employees and students of higher or further education level (see Figures 5.3 to 5.6).

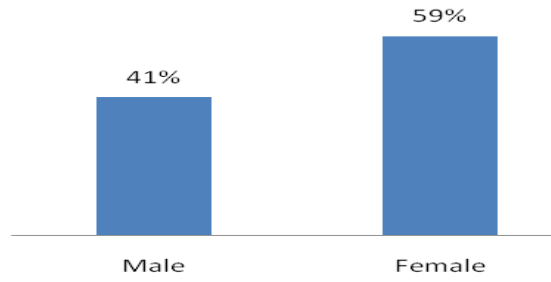


Figure 5.3: Gender (Qatar)

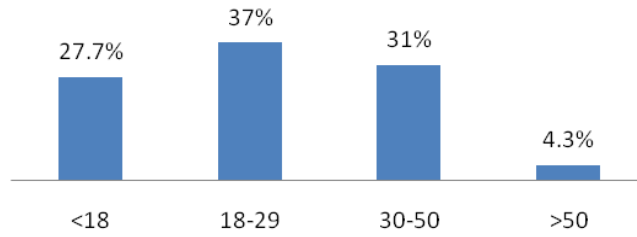


Figure 5.4: Age group (Qatar)

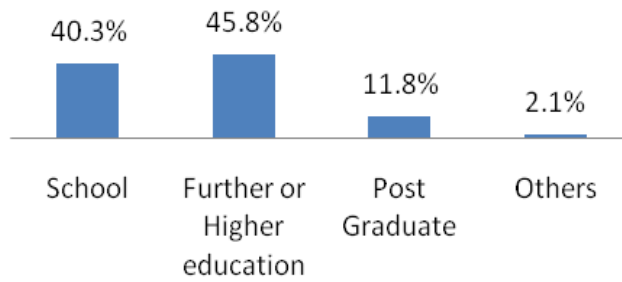


Figure 5.5: Education level (Qatar)

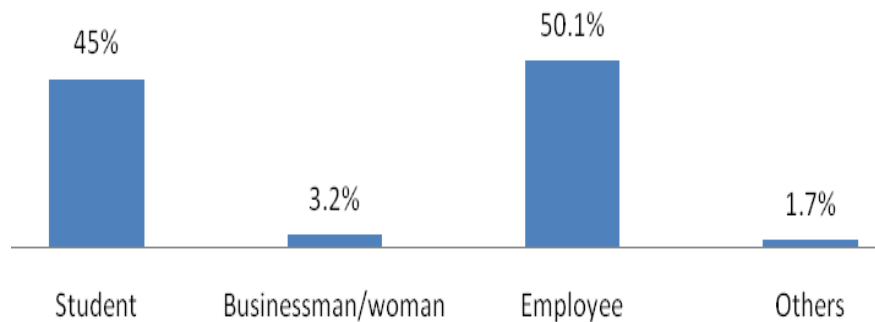


Figure 5.6: Occupation (Qatar)

2. Knowledge of e-mail phishing

Knowledge of e-mail phishing needs to be 'good' or 'expert'. 'Poor' and 'average' are not at all enough to protect respondents in the mysterious world of phishing. Participants were asked to assess their level of knowledge of e-mail phishing according to the following criteria:

None: Do not know anything about e-mail phishing

Poor: Have heard of e-mail phishing

Average: Know the term e-mail phishing and understand its simple techniques

Good: Know the term e-mail phishing, understand more about its techniques and how to protect against it.

Expert: Know the term e-mail phishing; understand more about its complex techniques, how to protect against it, how to detect it and how to react to it

The result of the questionnaire shows that few Qatari citizens, about one third, have the required knowledge (good to expert) about e-mail phishing (see Figure 5.7). Most participants gained this knowledge from the Internet and media, then schools and universities, very few from employers and from others such as friends, relatives and their own experience (see Figure 5.8). Most participants forecast that the e-mail phishing trend is increasing (Figure 5.9).

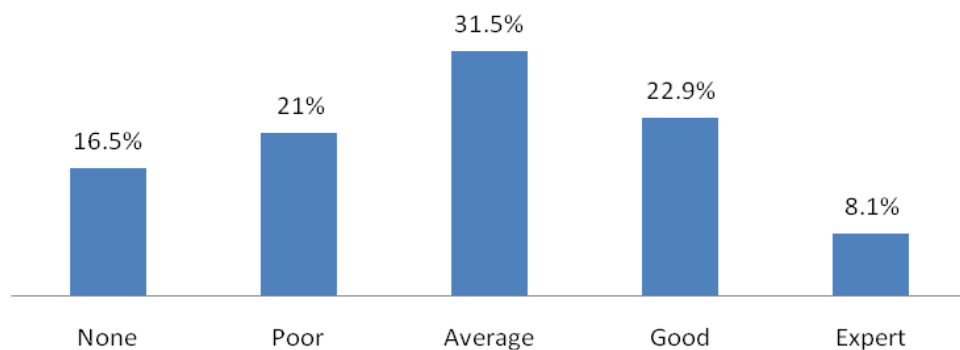


Figure 5.7: E-mail phishing knowledge (Qatar)

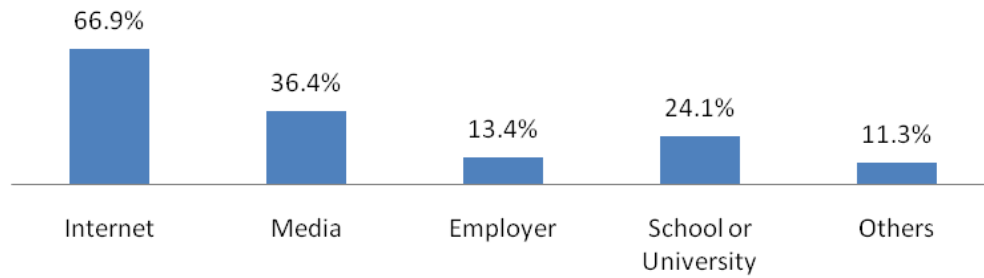


Figure 5.8: Source of knowledge (Qatar)

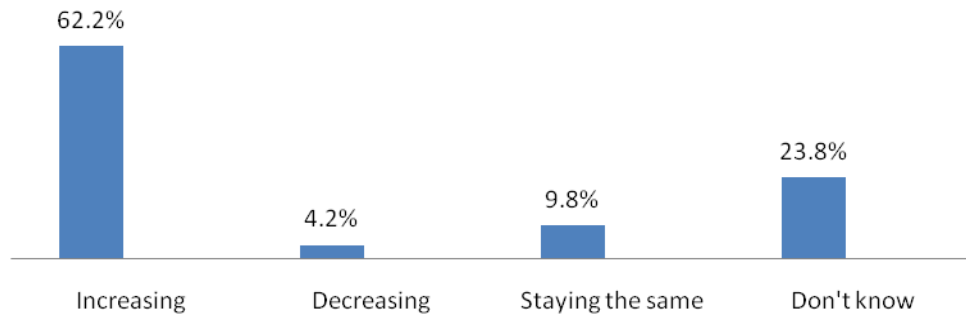


Figure 5.9: Trend of e-mail phishing (Qatar)

In conclusion, most Qatari participants did not have enough knowledge of e-mail phishing and only 31% of them did. The academic sector and employers do not play a huge role in enhancing awareness of phishing and the majority of participants consider it to be an increasing threat. It is good that Qatari citizens have the latter perception regarding their region; however, there is a need to enhance the knowledge of Qatari citizens about the phishing threat and to get involvement of academics and employers in achieving it.

3. Vulnerability to E-mail phishing

The survey shows that there is a large percentage (more than 70%) worried about the e-mail phishing threat (Figure 5.10). This has been reflected in the high use of anti-phishing software by respondents (about 69%) as most protect themselves from such attack by installing anti-phishing software such as spam filters and anti-viruses (Figure 5.11).

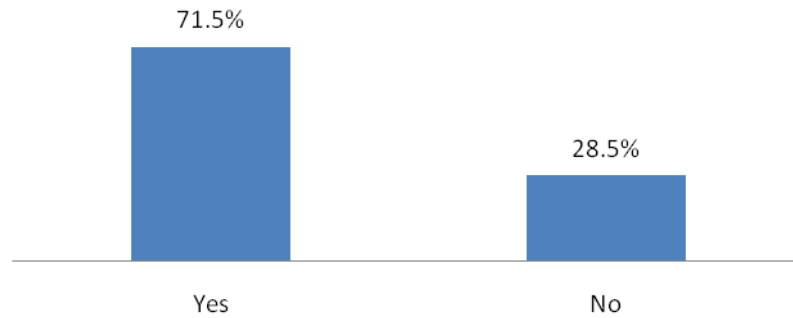


Figure 5.10: Participants' worry about e-mail phishing (Qatar)

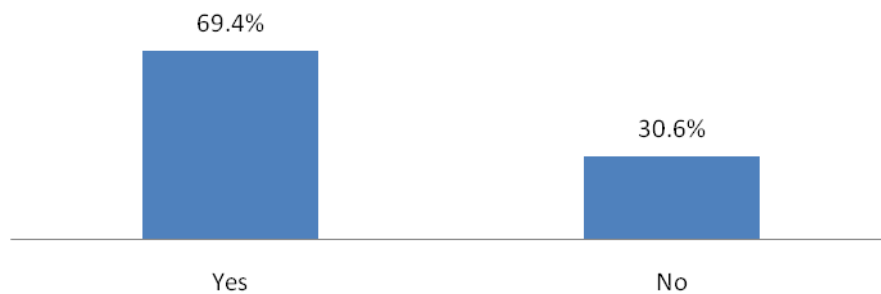


Figure 5.11: Use of anti-phishing software (Qatar)

Participants were also asked to identify cases of e-mail phishing in a list of e-mails in order to determine their ability to detect phishing or fraudulent e-mail. Table 5.1 shows the examples of e-mails presented in the questionnaire, the possibility of phishing for each and the percentage of responses for each type of e-mail. Participants who fail to detect a phishing e-mail might be vulnerable to being 'hooked' by such an attack.

About half of the participants, 44%, failed in detecting legitimate e-mails such as those which address users by their first and last name and those which direct users to a website with a URL starting with https and to a website containing a legitimate security certificate. Most of the participants interviewed after completing the questionnaire said that they are not familiar with the security indicators such as the terms 'https' and 'security certificate' and most of their decisions were just guesses. A few participants, just 11%, chose to skip this question (see Figure 5.12).

In contrast, about 57% failed to distinguish phishing e-mails. Those which ask users to enter information about their account and which convey a sense of urgency and surprise were detected by more than half of the participants. However, e-mails which had been classified as junk or spam mails, contained an attachment with viruses or asked users to phone a number, were detected by only about one third of the participants (see Figure 5.12). That is because the majority of interviewed participants stated that not all e-mails classified as junk or spam mails or which contain viruses are fraudulent and some do check their junk mails and sometimes download attachments with viruses, even if the sender is unknown. Also, some participants think that communicating off-line by telephone or post is more trustworthy and safer than online communication since most thought that online methods are more commonly used in a fraudulent attack. However, this is not true since hackers nowadays use different communication channels to commit their attacks.

Table 5.1: E-mails and possibility of phishing

Which of the following generally indicates that an e-mail may be phishing or fraudulent?	Possibility of phishing	% indicating they believe the email is phishing
Asks you to enter information about your account	Phishing	53.2
Addresses you by your first and last names	Legitimate	8.1
Directs you to a website containing a security certificate matching the name of the website.	Legitimate	17.7
Conveys sense of urgency and surprise	Phishing	57.9
Classified as junk or spam mail by your e-mail system.	Phishing	31.5
Contains attachment, notifying you that it might contain viruses that could harm your computer.	Phishing	38.2
Directs you to website with URL starting with https.	Legitimate	17.8
Asks you to phone number supplied in the e-mail.	Phishing	35.7

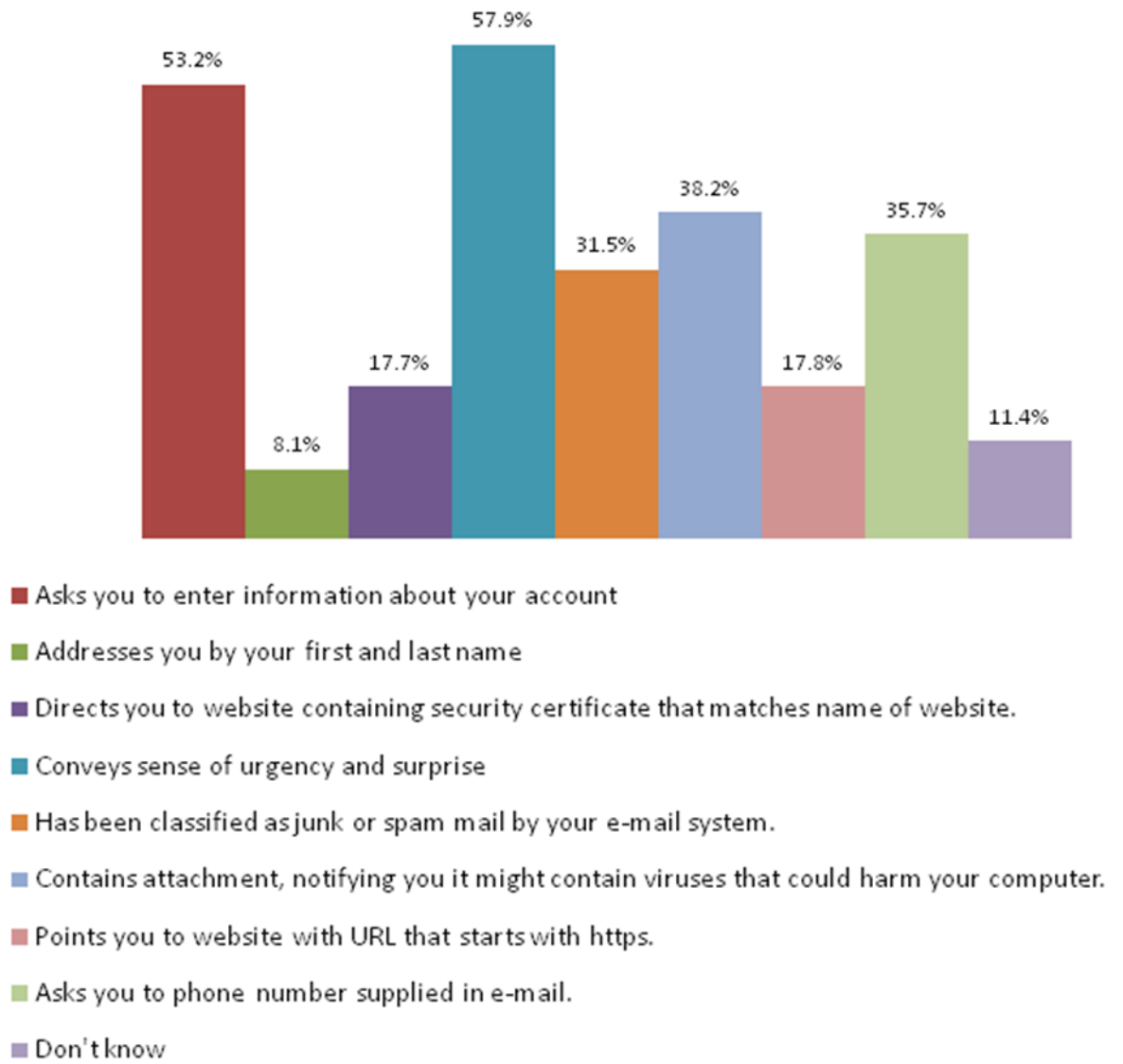


Figure 5.12: Participants' ability to detect a phishing attack (Qatar)

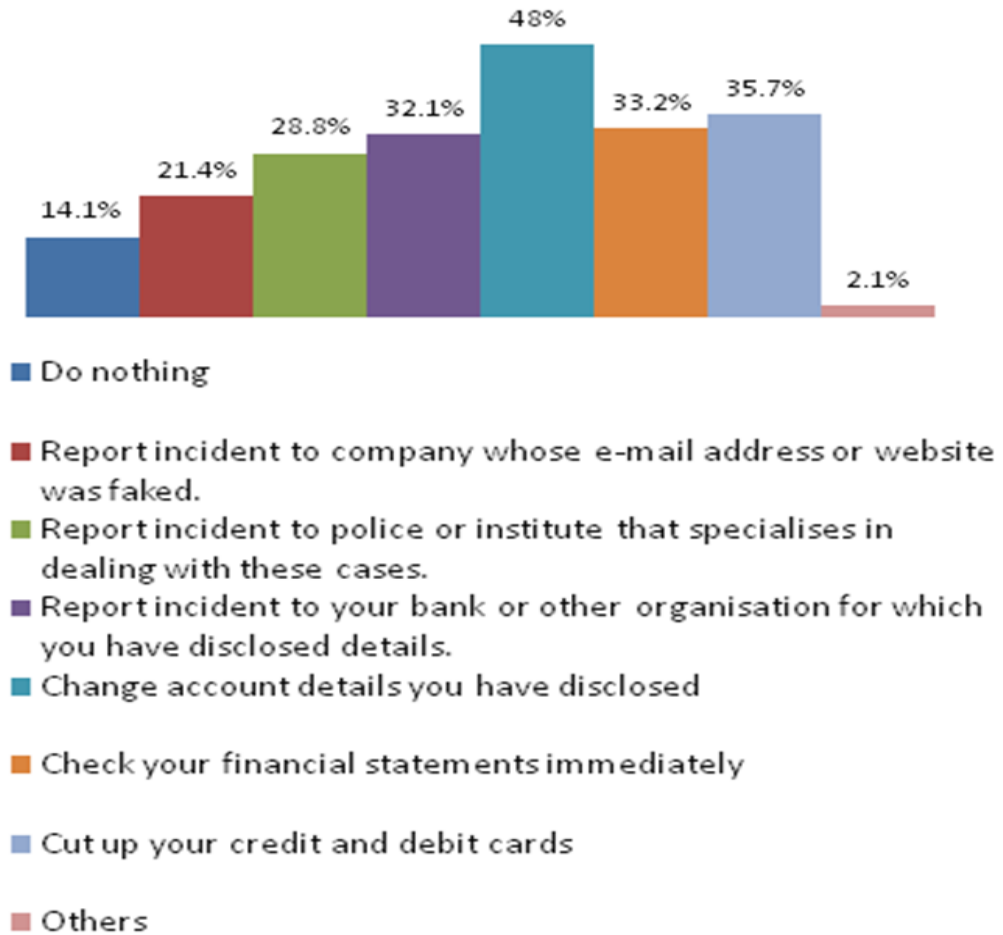


Figure 5.13: Participants' procedure once attacked (Qatar)

Regarding the actions which would be taken by victims on being tricked, fewer than half of the participants change their account details, check their financial statement immediately, cancel their credit cards or report the incident to their banks or other organisations whose details they have disclosed. Few report the incident to the police or any specialised body dealing with such cases or to the company whose e-mail address or website was faked (see Figure 5.13). Some of the interviewed participants commented that reporting to the police would create more problems and some people said “*The law does not protect the dupe*” (a common saying in Qatar). Also, it was believed that reporting the case to the company whose e-mail address or website was faked will not make any difference to what happens, as most think that it will not take the matter seriously. Furthermore, some stated they did not know that there is a specialised body to deal with such cases, the Q-CERT (Qatar Computer Emergency Response Team), which handles Internet crimes in Qatar. In general, the nature of the

surrounding culture leads Qatari citizens to be ashamed to report that they have been caught by phishing since the community is small and people would laugh at them. On the other hand, other participants proposed other valuable actions such as sharing their experience in one of the well-known blogs and forums to alert other people to such threat and contacting the service provider to take further action.

However, for an ideal situation, victims of such attack should apply all of the above actions in order to protect themselves from its further consequences. Fewer than 10% of the participants would take all of the above steps and about a seventh of them would do nothing once they have been tricked by phishing, which means most are vulnerable to huge consequences as a result (see Figure 5.13). Regarding the e-mail request, about 38% of the respondents disclosed their e-mail addresses, which shows a lack of awareness of some participants (see Figure 5.14).

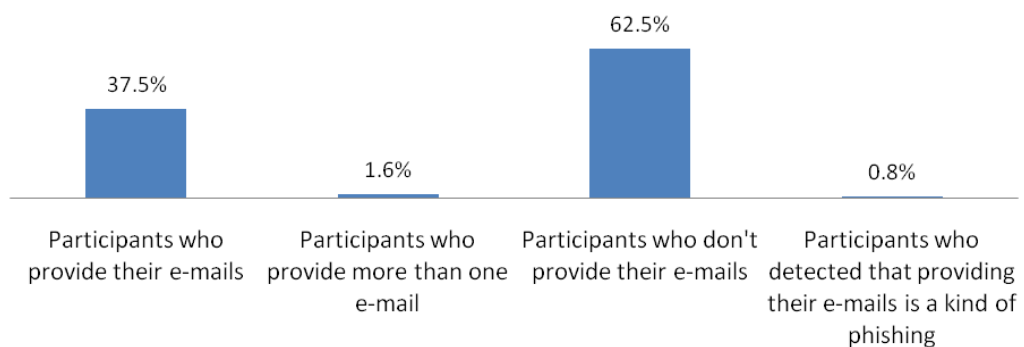


Figure 5.14: Participants' disclosure of their own e-mail addresses (Qatar)

In conclusion, even though the majority of participants do worry about the e-mail phishing threat and use specific software to protect themselves from it, most Qatari citizens are not able to detect phishing e-mails from legitimate ones. Even the most straightforward phishing attacks which ask users to disclose their confidential information and usually convey a sense of urgency and surprise were not distinguished by a large percentage of Qatari participants, which makes them vulnerable even to such basic phishing attacks. In addition, the majority do not take enough or even any action to diminish the possible consequences of successful phishing. The responses to e-mail requests indicate that some Qatari citizens are willing to disclose their private

information to anyone. Even though they noticed that the survey was on phishing, very few detected that this trick request was seeking to phish their e-mail addresses. In brief, this means that Qatari citizens are generally vulnerable to e-mail phishing threats.

4. *Extent of E-mail phishing*

Responses showed that the majority of participants, about 80%, receive phishing e-mails on a regular basis and that about 50% had fallen prey to phishing, with 11% having been tricked more than three times, which clearly shows these participants were not able to detect phishing (see Figures 5.15 and 5.16).

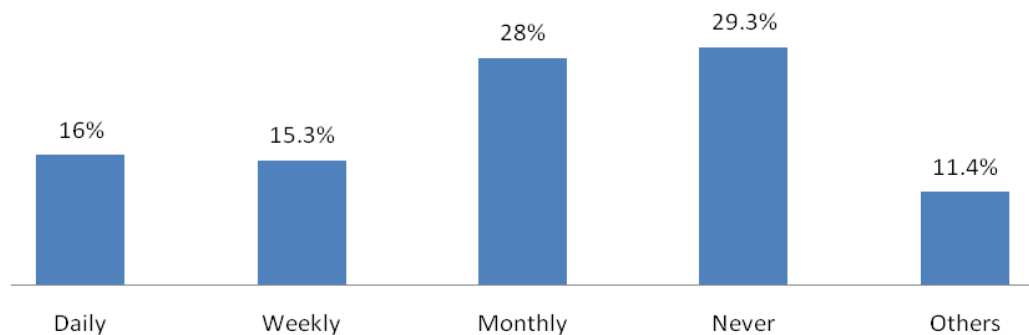


Figure 5.15: Frequency of receiving phishing e-mails (Qatar)

Although phishing e-mails were received very often, 40% of respondents indicated they had never fallen prey to them. The rest of the responses vary, the highest, 19%, being that respondents do not know whether they have been tricked, about 15% have been tricked once and 11% have even been tricked more than three times (see Figure 5.16). The interviews indicated that most of those who have been tricked more than once have become more aware of phishing. Most now have more ability to detect phishing attacks than those who have not been tricked at all. Also, the procedures they carry out after being tricked are more planned. As expected, this implies that the more participants have been tricked, the more their awareness will increase. In the interview, participants revealed that because they did not believe they were being tricked, because they lacked awareness of the phishing threat and because of the smart and varied techniques used by phishers against their victims, these participants frequently fall prey to such attacks.

The participants refer to the reason for their being tricked as being the following, arranged in descending order by percentage of responses:

- Phishers come up with smarter tricks which make it difficult to identify phishing
- They did not install software to protect against phishing e-mails and websites
- They did not believe they would be tricked
- The fake website looked almost identical to a legitimate one
- They lacked awareness and training about phishing
- The e-mail came up with sense of urgency and surprise
- They trusted the e-mail because they did not know about phishing (this confirms the response in the previous question)
- They were not aware of the importance of the information they had divulged.

The above responses indicate all of the above reasons were significant causes of Qatari participants' falling prey to e-mail phishing attacks (see Figure 5.17).

In conclusion, the extent of the e-mail phishing threat in the State of Qatar is high in view of the regular quantity of phishing e-mails received in participants' e-mail inboxes and the rate of successful phishing attacks.

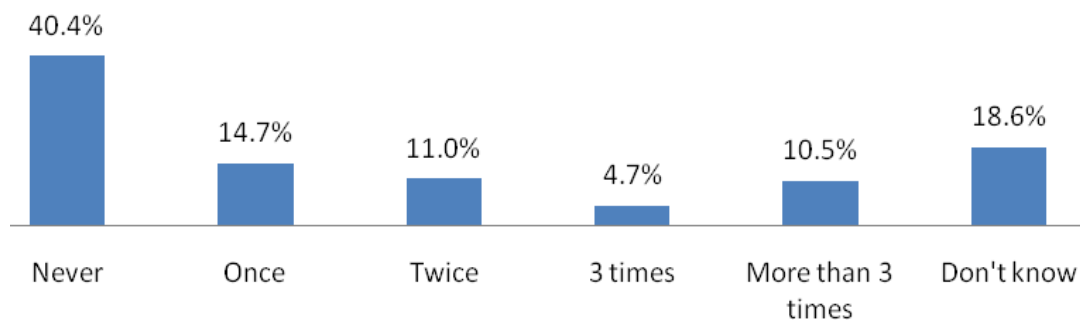


Figure 5.16: Frequency of being tricked by e-mail phishing (Qatar)

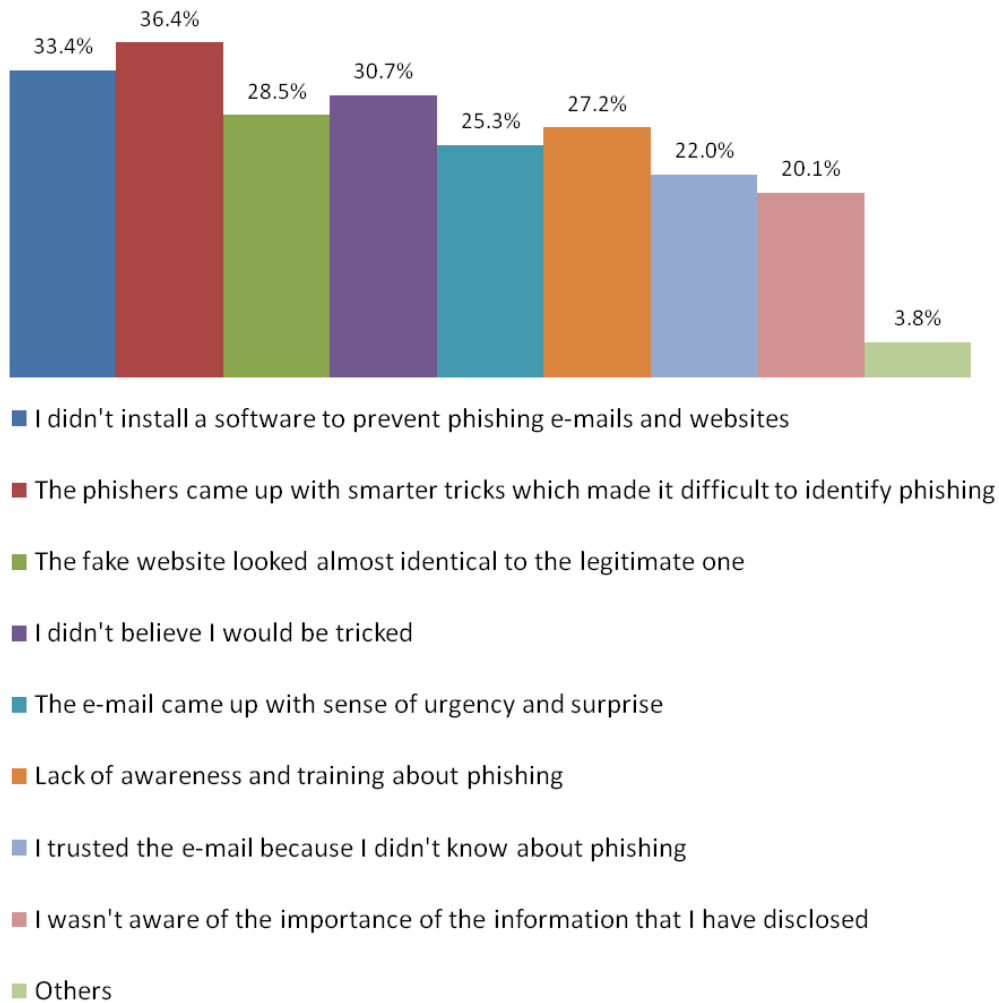


Figure 5.17: Reason for participants' being tricked by phishing (Qatar)

5. Defence against e-mail phishing

Although the use of technological protective solutions such as anti-phishing tools and software will assist in identifying and protecting against the phishing threat, phishers are still improving and trying to bypass those technological solutions and phishing is also related directly to human decision making and behaviour. Therefore, technological protective solutions are not able to diminish the risk of incorrect user behaviour. This was understood by about one third of participants who believe that anti-phishing software is not effective enough to protect online users from the professional and talented phishers today, since most who use it commented that they still receive phishing e-mails and viruses even though they use such software. In contrast, about the same percentage said that such software was very effective (see Figure 5.18).

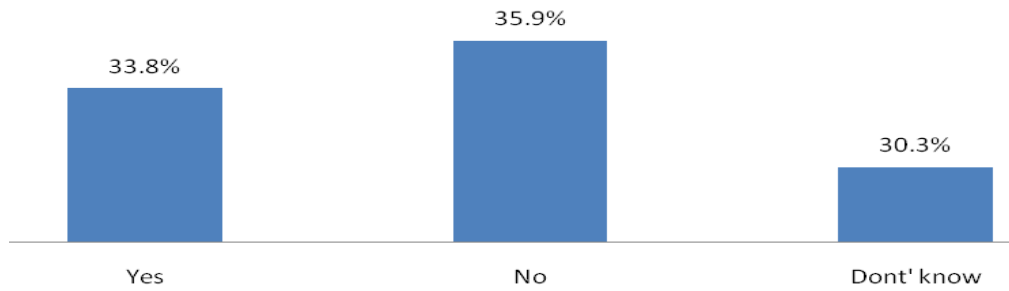


Figure 5.18: Efficiency of existing anti-phishing software (Qatar)

Although there are lots of ways to protect against e-mail phishing attacks, it was of interest to discover Qatari participants' outlook on the best way to defend themselves. The responses were positive, since most (66%) considered awareness to be the best defence, then came use of technological solutions, guidelines and, finally, fewer than 10% think that the experience of getting infected by phishing would be the best method of defence. In addition, others suggested that they follow employer policies, continuously upgrading protective software (see Figure 5.19).

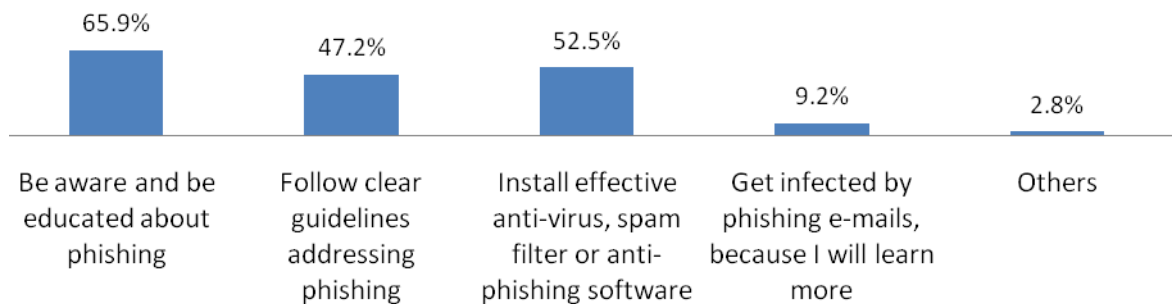


Figure 5.19: The best way to defend against phishing (Qatar)

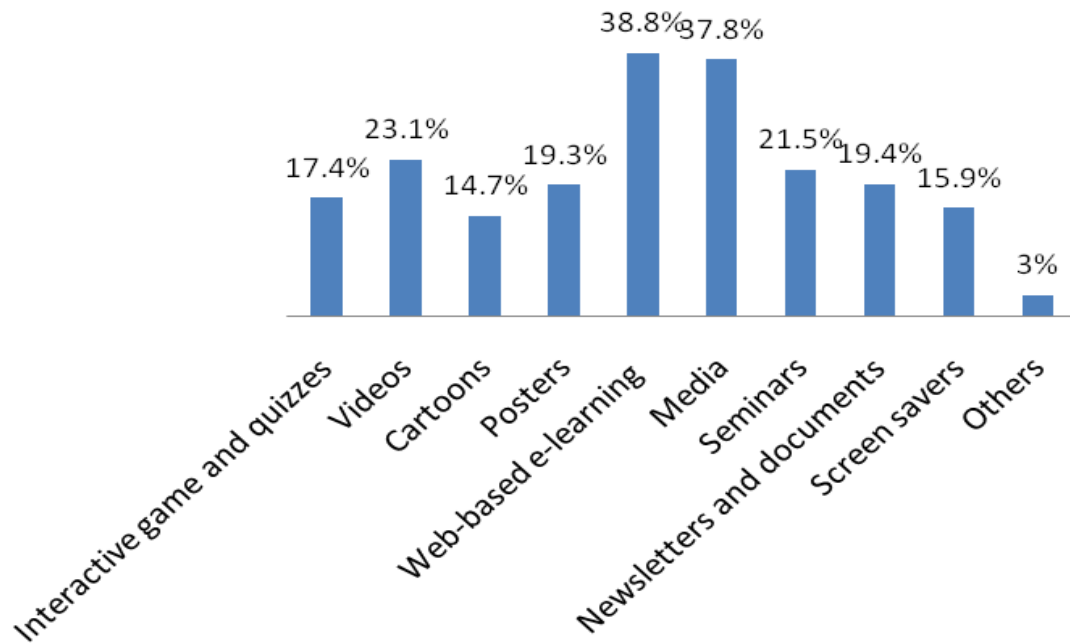


Figure 5.20: Participants' preferred method for awareness and education (Qatar)

Most participants, about 77%, preferred to be educated about e-mail phishing through web-based e-learning and media. The rest prefer other tools ranging from videos, seminars, newsletters, posters, interactive games, screen savers to cartoons (see Figure 5.20). Furthermore, interviews have revealed the importance of considering the background of people before applying an awareness programme, since participants' background has a major influence on their responses.

5.6.1.2 In-depth Analysis of the Qatar Questionnaire

Creating relationships between variables was significant in the analysis of the questionnaire results. Since the main target is Qatari people, an in-depth analysis was carried out only for the questionnaire used in Qatar. This was undertaken to define possible relationships between the questionnaire variables for better understanding of the outcome.

The chi-squared test (χ^2) is used to test hypotheses. In this research, the test was applied to show the relationships between the responses gathered in Qatar using a null hypothesis which states that there is no relation between the responses:

H0= The two responses are not related

with

H1= The two responses are related

χ^2 was calculated using the following formula: (Bluman, 2008: 578-584; Bock et al., 2007: 608-615)

$$\chi^2 = \sum 2 n_i \ln \frac{n_i}{e_i}$$

where n_i is the observed number of individuals in category i and e_i is the expected number of individuals in category i .

In this research, the value of P (level of significance) is usually 1%, 5% and 10%. For small P value, χ^2 is larger and this leads to the rejection of H0, therefore 5% was chosen as the target level. An online chi-squared calculator was used (Kirkman, 1996)

There were some relationships between the following variables according to the chi-squared test:

1. Worries about e-mail phishing with age, education and occupation.
2. E-mail phishing level of knowledge with age and education.
3. Divulgence of e-mail addresses with gender, worries of e-mail phishing and e-mail phishing level of knowledge.
4. Use of anti-phishing software with divulgence of e-mail addresses and efficiency of anti-phishing software

In brief, the major findings of the analysis are as follows (see Appendix A for the full results):

1. E-mail phishing level of knowledge.

The chi-squared test shows clearly a relation between level of knowledge with age and education. Responses show that about one third of participants with different ages have the required knowledge of e-mail phishing and this was less (about 28%) for

participants aged 18-29. The majority of those with postgraduate and school education levels have a required level of knowledge, more than those with further or higher education and others.

2. Participants' worries about phishing.

It was discovered that most Qatari participants of middle age, 30-50, were slightly less worried about e-mail phishing than other age groups. Business men and participants with school education were less worried about e-mail phishing than those with other educational levels and occupations.

3. Participants' disclosure of their e-mail addresses.

Males were more likely to disclose their e-mail information than females since about 65% of them did so in the survey. This is likely to be because the culture of Qatar is such that females would not normally disclose their private information such as phone numbers and e-mail addresses.

One shocking result is that 100% of participants with 'expert' knowledge failed the penetration test by giving their e-mail addresses, in contrast to participants with other levels of knowledge. This means most participants who thought that they had expert knowledge actually did not notice the possible tricks that phishers would use to trick their victims, so their knowledge was not as good as they believed. Therefore, Qatari citizens should understand that phishing is becoming more sophisticated and that achieving a 'good' or 'expert' level is not easy and requires continuous updating of their knowledge of e-mail phishing. Those who failed in this test stated in the interview that this question was trusted because it was within a survey for a research purpose and some said they did not think their e-mail addresses were confidential information that should not be disclosed.

Most of the participants (70%) who were worried about e-mail phishing succeeded in passing the penetration test, since most of them did not disclose their own e-mail

addresses. This implies worries of e-mail phishing have a significant influence on the awareness of people since this makes them more cautious and therefore less vulnerable to falling prey to phishing. In addition, more than 50% of participants who use anti-phishing software did not disclose their e-mail addresses. This implies that they are aware of phishing. However, the interviews show that most users of such software may rely too much on their software to detect phishing which makes them more vulnerable than others in the case where e-mail bypasses the software, as they tend to trust such e-mail. Although there is no need to be over concerned about phishing, there should be a balance of concerns about e-mail phishing so that users will not take the wrong decisions and this aspect is considered in the awareness programme research in this thesis.

4. Use of anti-phishing software

The majority of participants who use anti-phishing software were confused about the efficiency of what exists and about one third were not sure or found it efficient. However, about 38% found the software was not enough to rely on for detecting all possible types of phishing, even though the anti-phishing software will also designate some legitimate e-mails as phishing. They agreed that although the software helps to detect a lot of the phishing e-mails, it will not detect them all.

5.6.2 General Analysis of UK Questionnaire

The ultimate aim of this data collection is to measure Qatari citizen's awareness of e-mail phishing and their vision of defence against this attack compared to citizens of developed nations. Hence a similar questionnaire was used in the UK, an example of a developed country, in order to provide such a comparison. Quantitative analysis of the outcomes in the UK was made according to the defined questionnaire variables (see section 5.6.1). 1000 British citizens who met the sampling criteria were surveyed, with demographic details as follows:

1. Background information

Male participants were slightly more than females. Nearly half the participants were in the age group 18-29 (50%), with the next biggest group being aged 30-50 (35%). About half of the participants had further or higher education, then come postgraduate students (29%). With regard to occupation, most were employees (52%) and there were many students (50%) (see Figures 5.21-5.24).

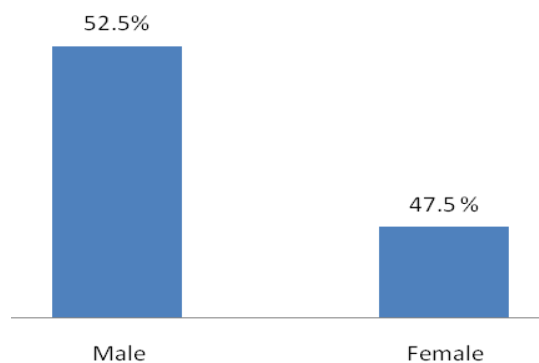


Figure 5.21: Gender (UK)

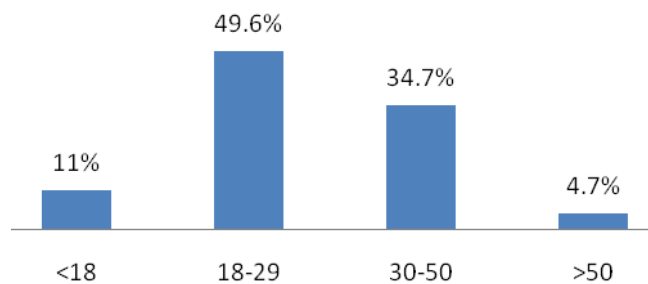


Figure 5.22: Age group (UK)

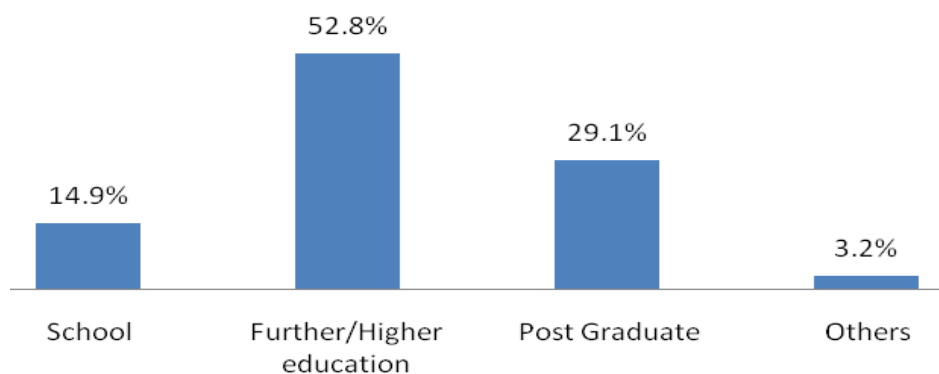


Figure 5.23: Education level (UK)

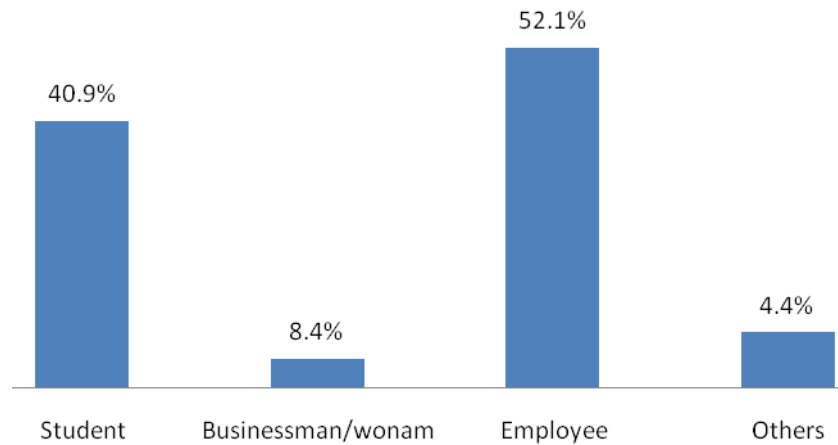


Figure 5.24: Occupation (UK)

2. *Knowledge of e-mail phishing*

The majority of participants claim to have an ‘average’ or ‘good’ knowledge of e-mail phishing and about one third of UK participants have the required knowledge (see Figure 5.25). The majority (about 68%) indicated the Internet as the main source of their knowledge, then came the academic sector (34%) and media (26%), with only a few indicating employers (11%) (see Figure 5.26). Most participants forecasted phishing would be an increasing threat in the UK, the majority (about 68%) forecast the trend of phishing is increasing and only a few (about 12%) thought it is staying the same or decreasing. The rest (about 21%) didn’t know (see Figure 5.27).

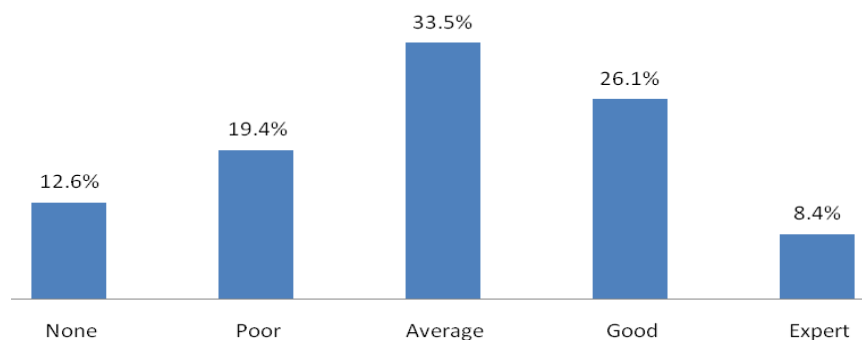


Figure 5.25: E-mail phishing knowledge (UK)

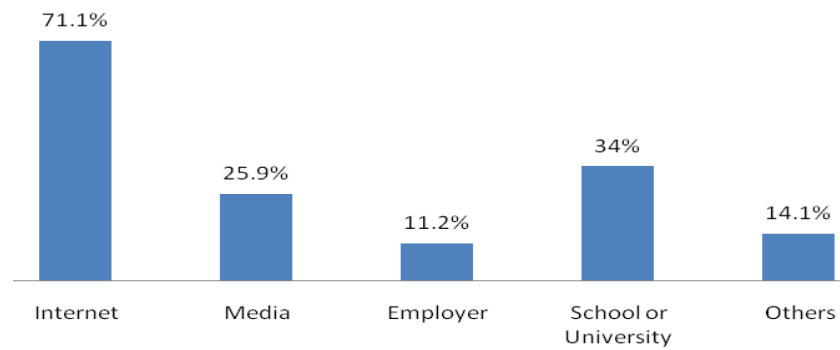


Figure 5.26: Source of knowledge (UK)

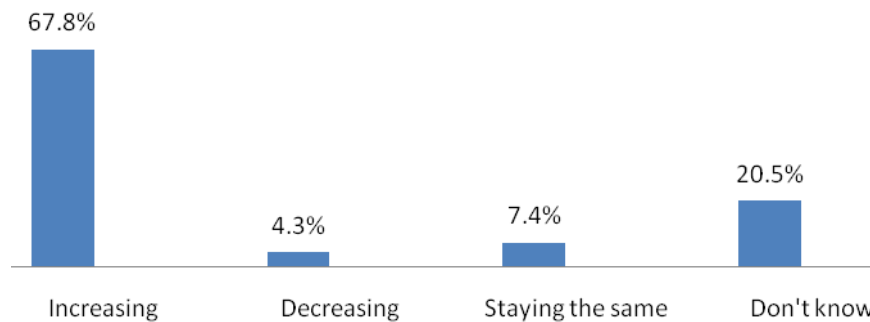


Figure 5.27: Trend of e-mail phishing (UK)

3. *Vulnerability to e-mail phishing*

The survey outcome shows that the UK is less susceptible to e-mail phishing attacks since most respondents do worry about e-mail phishing, most use protective software and most know how to detect such attacks and the action to take once tricked. Only a few failed the penetration test which aimed to phish their e-mail addresses.

Worries about e-mail phishing and the use of anti-phishing software are high in the UK. A high proportion of participants (89%) worry about e-mail phishing and about the same percentage (81%) use software to protect themselves from phishing (see Figures 5.28 and 5.29).

It is a good indication that most of the UK participants (73%) recognise how to detect phishing e-mails, only 20% of them failed in detecting the legitimate e-mails and a very few participants (7%) did not know how to spot such attacks (see Table 5.1). Most detected e-mail phishing in e-mails that convey a sense of urgency and surprise and

those which ask for their account details (see Figure 5.30). In addition, about one third of respondents carry out all the listed actions to protect themselves once tricked and only 18% do nothing. The rest would perform some of the listed actions, mostly changing account details, checking their financial statements and reporting to the bank or other bodies (see Figure 5.31). Although the majority (79%) declined the request for their e-mail addresses, some (21%) did fail in this test and disclosed their private information. However, only 3% knew that such a request was a type of phishing. A few (less than 1%) provided more than one e-mail (see Figure 5.32).

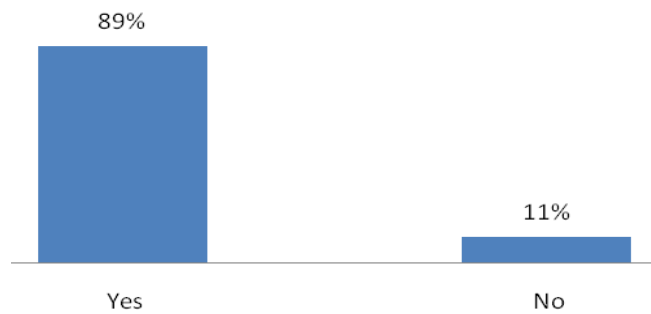


Figure 5.28: Participants' worry about e-mail phishing (UK)

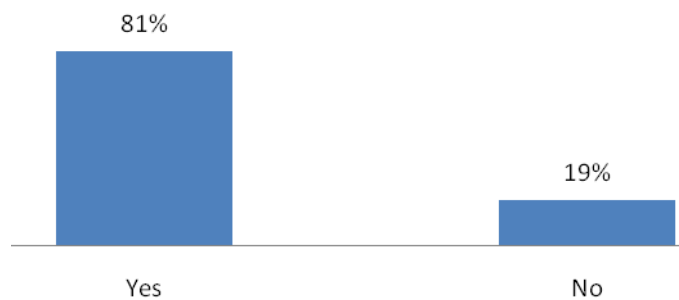


Figure 5.29: Use of anti-phishing software (UK)

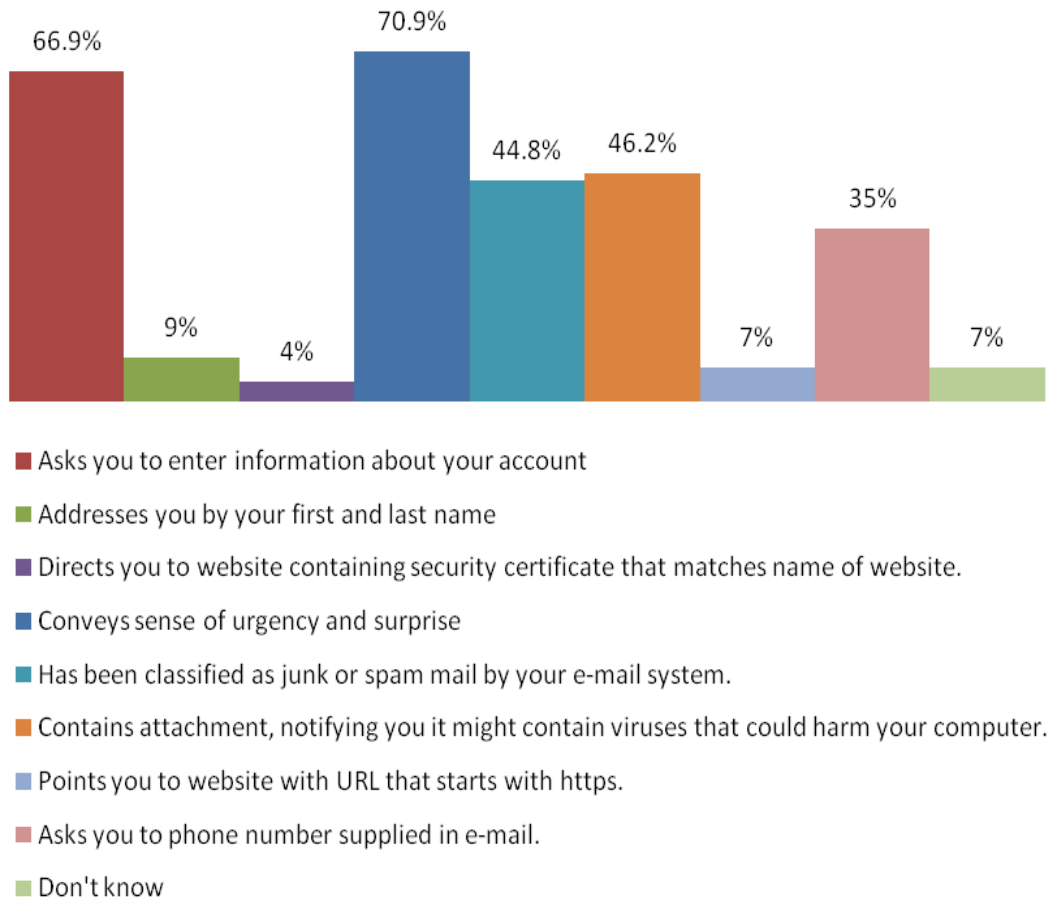


Figure 5.30: Participants' ability to detect phishing attack (UK)

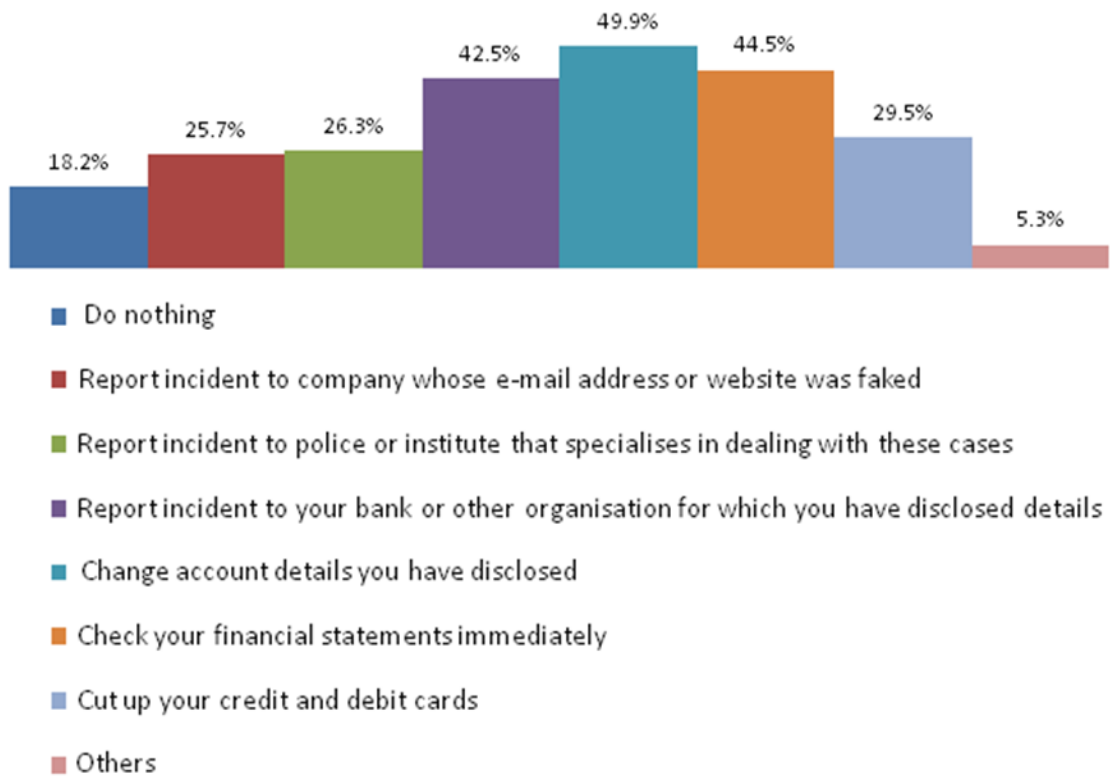


Figure 5.31: Participants' procedure once attacked (UK)

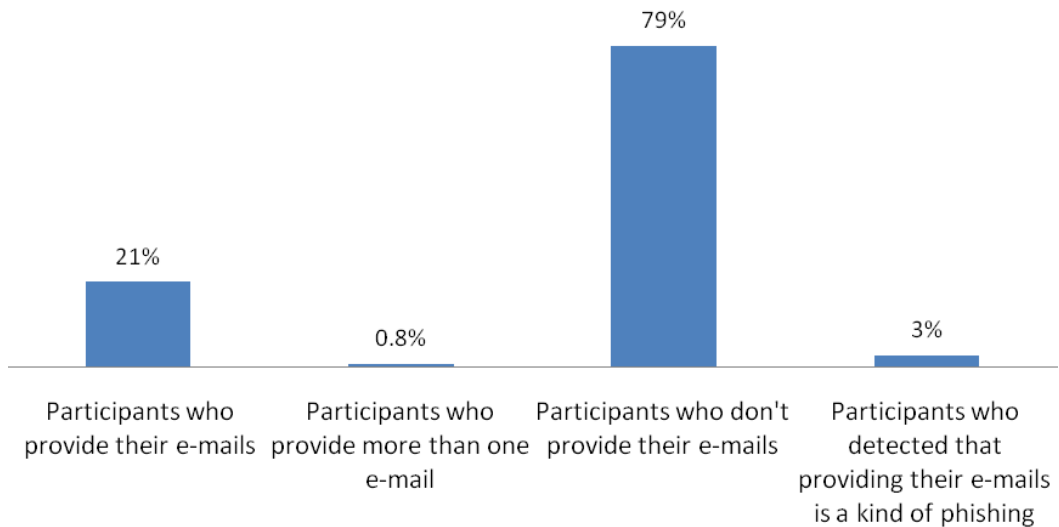


Figure 5.32: Participants' disclosure of own e-mail addresses (UK)

4. *Extent of e-mail phishing*

The responses show that the extent of e-mail phishing in UK is quite high, with only 17% of participants indicating that they never receive such e-mails. The majority (about 83%) indicate that they receive such e-mails on a regular basis, mostly monthly or weekly (see Figure 5.33). However, the majority of participants (68%) claim they have never fallen prey to e-mail phishing. About a quarter knew they had been tricked, ranging from once to more than 3 times and only 5% did not know (see Figure 5.34). Most who were tricked blamed the smart tricks phishers use, the fake websites that looked legitimate and a lack of anti-phishing software (see Figure 5.35).

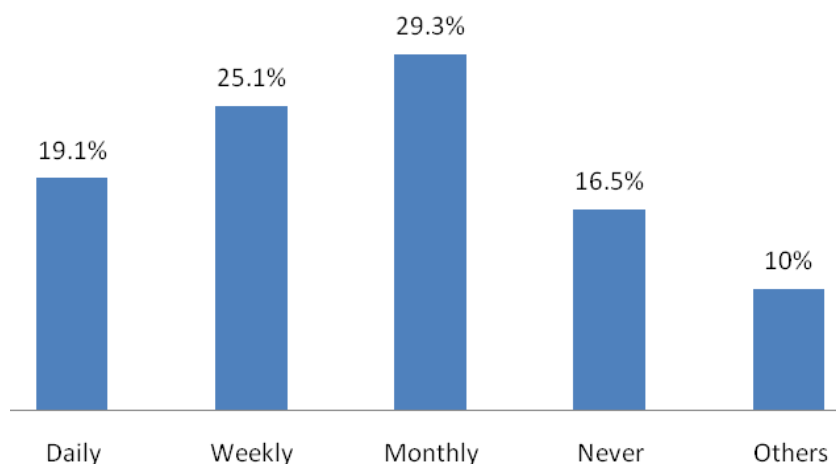


Figure 5.33: Frequency of receiving phishing e-mails (UK)

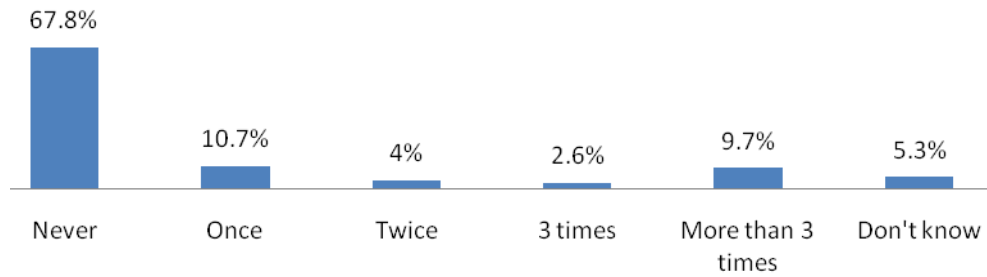


Figure 5.34: Frequency of being tricked by e-mail phishing (UK)

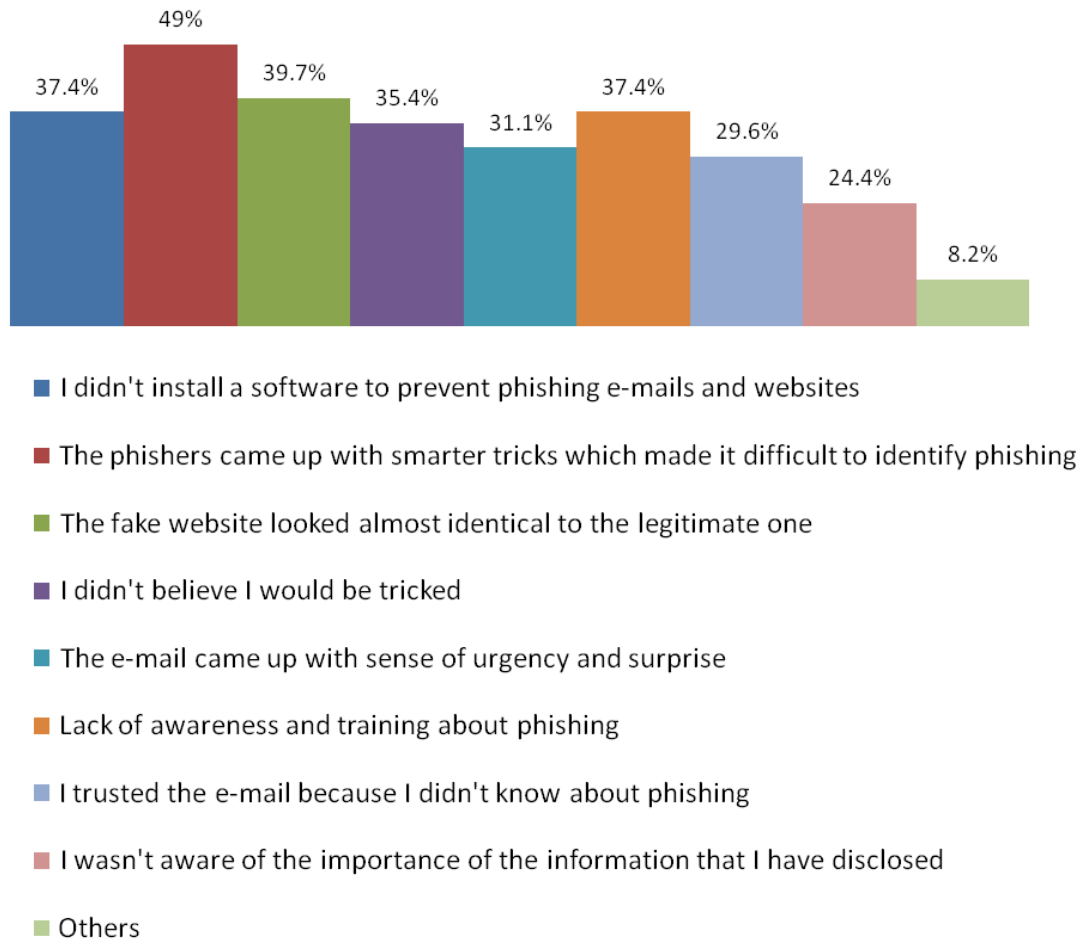


Figure 5.35: Reason for participants' being tricked by phishing (UK)

5. *Defence against e-mail phishing*

39% indicated that anti-phishing software is not enough to protect against all kinds of phishing, 24% do think existing technological solutions are effective enough and the rest do not know (see Figure 5.36). Also, the majority (77%) consider the awareness of the phishing threat as the best means of defence against such attack, then comes the use

of anti-phishing software, policies and guidelines and, finally, experience of getting affected by phishing was found to be an effective way of learning about phishing (see Figure 5.37). With regard to awareness, most participants prefer to be educated about phishing through the media, e-learning, newsletters, videos and seminars (see Figure 5.38).

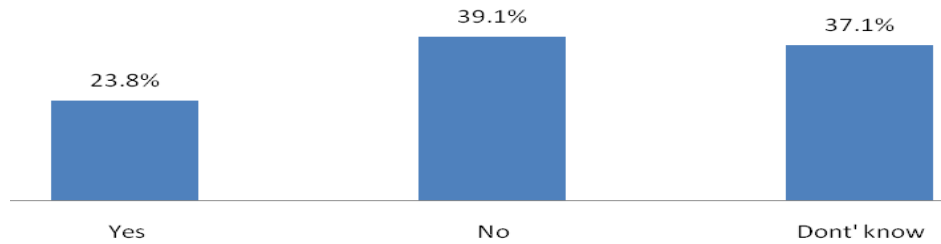


Figure 5.36: Efficiency of existing anti-phishing software (UK)

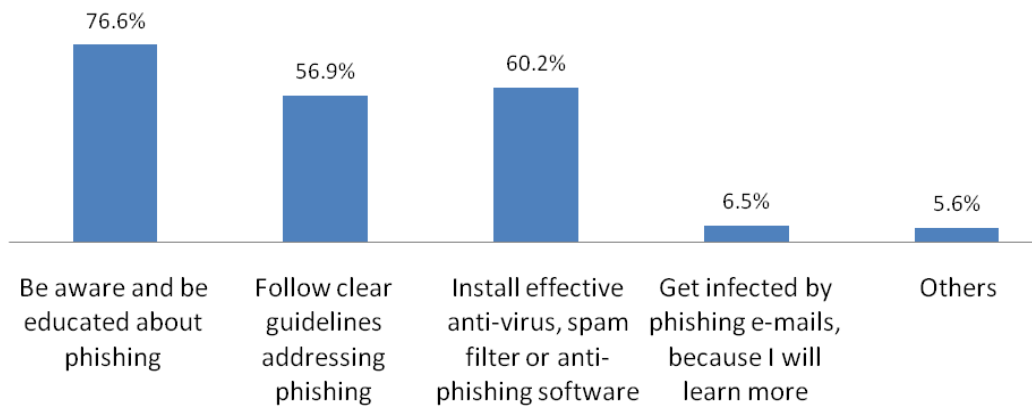


Figure 5.37: Best way to defend against phishing (UK)

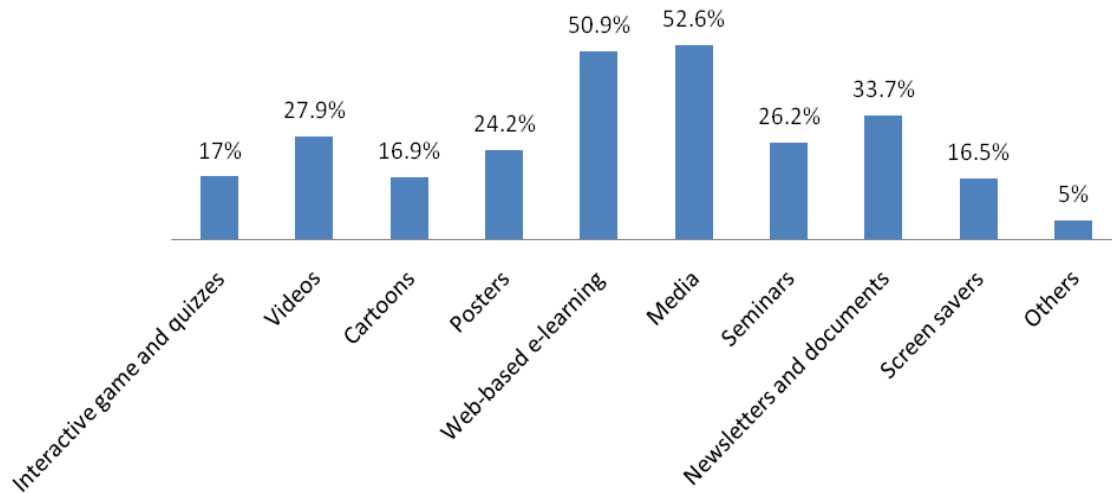


Figure 5.38: Participants' preferred method for awareness and education (UK)

5.7 Comparison of Questionnaire Outcomes for the UK and Qatar

The chi-squared test (χ^2) was used to compare the responses gathered in the UK and Qatar according to the following hypotheses (Bluman, 2008: 578-584; Velleman and De Veaux, 2007: 608-615; Kirkman, 1996; Bock et al., 2007):

H0= Responses and country are independent. Therefore, it implies no significant difference between the UK and Qatar result.

H1= Responses and country are related. Therefore, it implies a significant difference between the UK and Qatar result.

In conclusion, the test results show that there is definitely a significant difference between responses in each country except for the following: e-mail phishing level of knowledge, use of anti-phishing software and reason for being tricked (see Appendix A for test results)

A comparison between responses in each country is given below:

1. Knowledge of e-mail phishing

The knowledge of e-mail phishing is about the same in Qatar as in the developed country, the UK. One third of participants in the UK and Qatar have the required knowledge on e-mail phishing.

There is a misunderstanding by Qatari participants on their level of knowledge of e-mail phishing. The majority of those interviewed thought that they had expert knowledge of e-mail phishing since they know how to use the computer and the Internet very well in chatting and accessing information or they have heard about the term phishing. Most have gained their knowledge from the Internet and media. However, the academic sector in UK plays a greater role in educating people about e-mail phishing compared to Qatar, with an additional 10% of British citizens having gained their knowledge from this source. Furthermore, the majority (over 60%) believe e-mail phishing is an increasing trend.

2. Vulnerability to e-mail phishing

Vulnerability to phishing in Qatar is very high compared to the UK, because of the following:

- UK citizens are more worried (about 20% more) about phishing compared to Qatari.
- Compared to Qatar, the use of anti-phishing software is higher in the UK. A high percentage of UK citizens (about 10% more than Qatari) use anti-phishing software to protect themselves from attacks
- The UK public are aware of phishing techniques and are better at detecting phishing e-mails than Qatari citizens. In contrast to Qatari citizens, only a few British participants do not know how to detect phishing e-mails, a greater percentage of British participants (28% more compared to Qatari) have successfully detected phishing e-mails and only a few (20%) failed to identify legitimate e-mails

compared to Qatari citizens, where the figure is doubled (44%). However, the level of detection for different phishing e-mails was nearly the same for both Qatari and UK participants, most of whom detected e-mails asking users to provide their account details and those conveying a sense of urgency and surprise.

- Compared to Qatari citizens, the British are more concerned once they have been tricked by phishing and about one third of them try to take all possible actions to protect themselves from possible consequences of such attack, whereas only 10% do so in Qatar. Nevertheless, the types of response for each action for both sets of citizens was similar, where most do change their account details, check their financial statements, cancel their credit cards and report the incident to their banks.
- The e-mail request indicated that British citizens are more aware of phishing since most (79%) do not fall for this trick compared to Qatari citizens, where the percentage of failure reached 38%. Even the identification of such a request as phishing was higher for UK citizens.

3. Extent of e-mail phishing

According to the questionnaire, UK citizens receive more phishing e-mails (about 10% more) compared to Qatari citizens. However, fewer (27%) UK citizens were tricked by them compared to Qataris, where the figure reached 50%. In addition, two thirds of UK citizens have never been tricked (67%) compared to just over one third of Qatari citizens (about 40%). Nevertheless, the reasons for being tricked were similar for both, where most users blamed the smart tricks used by phishers, the lack of technological protection (e.g. spam filters), users' not believing they would be tricked, the legitimate appearance of a fake website and a lack of awareness. However, the responses give an indication that UK citizens believe that lack of awareness was one of the main reasons for their being tricked (UK responses show a result of about 10% more compared to Qatar).

4. Defence against e-mail phishing

There are minor differences between the responses in Qatar and UK with regard to the variables related to defence against e-mail phishing. Although about one third of the participants in both societies were unsure about judging the effectiveness of existing anti-phishing technological tools, about the same percentage (more than one third) found anti-phishing technological tools not to be efficient in providing enough protection against phishing since most still receive the offending e-mails. Awareness and education were considered in both societies as the supreme method of defence against e-mail phishing, with the percentage somewhat higher in the UK compared to Qatar (about 10% greater in UK). With regard to the method of creating awareness, participants in both the UK and Qatar preferred education about phishing through media, videos, seminars, newsletters and posters, with less than 20% preferring interactive quizzes and games. However, it might be a good idea to have such a method where education is carried out with fun.

5.8 Summary

Surveys of Qatari and British e-mail users provided a profile of their awareness of e-mail phishing and their views on the best method of defence against this attack. The questionnaire design passed through several stages, first review and then pilot-test to achieve an effective and carefully designed questionnaire which was then completed in the UK and Qatar by a broad sample of respondents. It addresses the knowledge of e-mail phishing, vulnerability of participants, extent of e-mail phishing and defence against it. Later, the questionnaire results were gathered and analysed quantitatively according to defined variables. Interviews with participants supported the questionnaire outcome.

In conclusion, responses for Qatari e-mail users show that there is a problem of e-mail phishing in Qatar since most participants forecast that the e-mail phishing trend is increasing and many receive phishing e-mail regularly, with a high rate of successful phishing attacks.

In addition, Qatari citizens are generally vulnerable to e-mail phishing threat; the survey has recognised a number of the aspects which make Qatari citizens vulnerable to phishing, as follows:

1. There is a lack of knowledge and awareness deficiency on phishing threats, indicated by participants not being able to distinguish phishing attempts from legitimate e-mails, with the failure in detection reaching 57% and 44% for phishing and legitimate e-mails, respectively. In addition, about 38% disclosed their e-mail addresses upon request. Few (about one third) have the required knowledge (good to expert) of e-mail phishing. However, more than 70% were worried about the e-mail phishing threat, but there is still clearly a lack of knowledge on phishing. Therefore, these worries should be exploited in enhancing people's awareness of the phishing threat without intimidating them.
2. Although there is a high use (about 69%) of anti-phishing software, about half of the users were confused about the effectiveness and reliability of anti-phishing software in providing enough protection against the phishing threat.
3. The majority does not know how to protect themselves against phishing attacks and how to detect and react to phishing, e.g. do not understand security indicators and some think phishing is limited to online communications. Fewer than 10% of the participants take all required actions once they have been tricked by phishing and about a seventh of them do not react at all because either they did not know that there is a specialised body (Q-CERT) which handles Internet crimes in Qatar or they have little trust in the ability of the police and the company whose e-mail address or website was faked to investigate the case.
4. Qataris are affected by the manner of incentives and disincentives, since more than half of the participants do not distinguish phishing e-mails which convey a sense of urgency and surprise.
5. The surrounding culture leads Qatari citizens to be ashamed to report that they have been trapped by phishing
6. About 30% did not believe they would be tricked

The results show clearly that there is a need for enhancing Qataris' awareness of e-mail phishing, especially since 66% considered awareness to be the best defence against phishing, with 77% preferring to be educated through web-based e-learning and media and other tools such as seminars, posters, interactive games and cartoons. Therefore, the rest of this thesis focuses on awareness of e-mail phishing as a method to reduce phishing in Qatar. It can be concluded that responses for e-mail phishing level of knowledge, use of anti-phishing software and reasons for being tricked were similar for both Qatar and the UK. However, other responses were significantly different, with a much higher vulnerability to phishing in Qatar than in the UK.

The next chapter describes the experiments in Qatar to understand Qatari citizen's vulnerability to e-mail phishing and attempts to investigate further the cultural and country-specific factors which make phishing successful in Qatar. This will then be considered in the development of the proposed awareness framework.

Chapter 6 Penetration Tests and Laboratory Experiment

This chapter describes experiments in the State of Qatar to measure the vulnerability of Qataris to e-mail phishing and their ability to differentiate such attack from legitimate e-mails. Also, it outlines the factors which make Qatari citizens vulnerable to e-mail phishing attacks such as cultural, country-specific factors, interests and beliefs, effect of religion and personal characteristics. Some of these factors were already identified earlier in previous chapters but in this chapter Qataris' vulnerability to phishing is addressed in depth empirically. Also addressed in this chapter is whether there are specific criteria for phishing victims as discussed in Chapter 4 in interviews with experts in the field of e-crime.

6.1 The Phishing Experiments

Many researchers focus on studying why people could fall victims to phishing by means of experiments, either in the laboratory or in reality, using tests which aim to assess people's ability to distinguish phishing e-mails. These researchers have made some findings but they do not recognise the aspects which might make people vulnerable to phishing, including cultural, country-specific and other factors (see Chapter 2). Therefore, this research focuses on studying the possible factors which affect users' response to phishing, leading them to be possible victims.

Three experiments were used in this research: penetration test 1, penetration test 2 and a laboratory experiment. Different participants were used in each experiment in order to get a reliable outcome from experiments on how vulnerable they are to phishing. To measure and evaluate Qataris' vulnerability to e-mail phishing real and anonymous e-mail phishing penetration tests were applied to two sample groups: company employees and a convenience sample of Qatari citizens. The laboratory experiment is a form of phishing experimental laboratory using a sample of Qatari government employees to

identify their ability to distinguish legitimate e-mails from phishing ones and identify their vulnerability to phishing and why.

Following the experiments, interviews were held with employers, participants and experts in IT awareness and culture in order to get a better understanding of why Qataris are vulnerable to e-mail phishing attacks. Samples were chosen according to their convenience and job titles. Several interviews (see Chapter 3 for brief plan) were also held for each experiment with the following people:

Penetration test 1:

- Some of the 129 participants in the test
- The Managing Director of AAB (Abdulghani and Brothers), one of the most successful automobile businesses in Qatar
- The Manager of IT, the head of the IT section and the network administrator in the IT department at AAB.

Penetration test 2:

- The 30 participants in the test
- An Information Scientist working with Outreach and Training at Q-CERT (Qatar Computer Emergency Response Team), Qatar's coordination centre for dealing with Internet security problems.
- The Acting OA&T manager at Q-CERT
- The Senior Incident Manager at Q-CERT

Laboratory experiment:

- The participants in the experiment (30)
- A First Lieutenant and Network Engineer in the IT department of the Ministry of Interior, State of Qatar.
- A First Lieutenant and Software engineer in the IT department of the Ministry of Interior, State of Qatar.

- A First Lieutenant and Information Security Specialist in the IT department of the Ministry of Interior, State of Qatar.
- A Post-Doctoral Research Assistant and Teaching Fellow at Bradford University in the UK
- The Head of Middle East Operations at InfoGuard, a Swiss company specialising in information security
- An Information Scientist working with Outreach and Training at Q-CERT
- The Cultural Attaché at the Qatar Embassy in London
- A Researcher in Qatar culture from the Ministry of Culture, Arts and Heritage in Qatar

Finally, this chapter concludes by identifying the factors which make Qataris susceptible to falling prey to phishing attacks, some of which were discovered as well in previous chapters (Chapter 4 and 5).

6.2 Penetration Tests

The vulnerabilities of Qataris to e-mail phishing attacks was tested in reality through two penetration tests, one with a sample of Qatari employees from one organisation in Qatar and the other with a sample of the Qatari public. Both tests aimed at tricking them by taking advantage of their beliefs and interests. In these tests, spear phishing attacks were made on highly specific targets, instead of sending a huge amount of e-mails to large numbers of people (Microsoft, 2006).

6.2.1 Test 1

The aim of this study was to identify the state of awareness of e-mail phishing for a sample of Qatari employees and the possibility of phishers to reach sensitive organisational or private information by tricking employees with e-mail phishing

attacks using different techniques. The target for this test was a medium-sized Qatari organisation with an e-mail system regularly used by its employees in their daily operations.

6.2.2 Authorisation

Permission had been sought to do such a test in governmental and private organisations. However, due to its sensitivity, it was difficult to find a government organisation to authorise the study because legal and other permissions are required from a sequence of senior officials and governmental bodies, which is time-consuming and not guaranteed. Therefore, a private company was sought to support the study in their premises and, finally, a private company, Abdullah Abdulghani and Brothers (AAB), agreed to allow the study with its employees.

AAB is one of the most successful automobile businesses in Qatar, with a good reputation in the market through its customers, business partners and employees. It sells two makes of car, Lexus and Toyota, and has developed from its early beginnings with small sales and only 30 staff to vast annual sales and more than 1600 staff. AAB is managed by a Board of Directors currently consisting of the Chairman, Abdulrahman Abdullah Abdulghani, Vice-Chairman Abdulrahman Abduljaleel Abdulghani, and the Managing Director, Dr. Nasser Abdulghani Abdulghani. The authorisation for study was given by those three top managers. The company has maintained its position in the market through ensuring quality of product and services. Currently, AAB has undertaken a major BPR (Business Process Reengineering) programme in order to cope with the challenges ahead, keeping in line with the huge world competition and aiming for more than 8 million global sales by the year 2010 (AAB, 2003).

In an interview, the Managing Director stated that the AAB mission is to maintain the number 1 position in the automobile industry in Qatar and this would be achieved by enhancing its current solid reputation established over 40 years ago through providing the highest standards of quality customer service. He commented that the company will continue to meet its social responsibilities as one of the emerging leaders

in the business community, contributing to the national cause by actively participating in the country's economic, social and cultural activities. He added that AAB is supporting education and students, and would, therefore, accept the study on its employees, and it would be beneficial for the company in measuring their vulnerability to phishing attacks and their awareness of such a threat.

6.2.3 Test 1 Process

The process of the e-mail phishing penetration test involved three phases: planning and designing, running the test and, finally, analysing results and discussing findings to achieve the overall aim of the study (see Figure 6.1). Each phase is explained as follows:



Figure 6.1: Penetration test 1

6.2.3.1 Planning and Design

Planning this study was done with cooperation from the AAB Company. An in-depth discussion group was set up with the researcher and three employees from AAB's IT department: Mr. T. Nagarajan, Manager of IT, Mr. H. Fitrianto, Head of the IT section, and Mr. T. Nava, a Network Administrator. Discussions with these IT professionals were necessary to set up a plan for the study suitable for both the researcher and AAB.

Since only Qatari employees were targeted, it was necessary to ensure the study excluded non-Qataris. The Manager of IT stated that AAB has about 1,600 employees from different nationalities (Indian, Egyptian, Lebanese, etc.) and about 400 of them use the company e-mail system in their daily operations. It was necessary to exclude the other nationalities and Qatari top managers due to the sensitivity of such a study.

Ultimately, the study sample consisted of only 129 Qatari employees. Regarding the phishing e-mails, the Head of IT and the Network Administrator suggested using complex phishing attacks, ruling out straightforward ones like winning in a lottery, which is becoming well known to Qataris.

Finally, discussions concluded on using three phishing e-mails with different techniques to trick employees. Since AAB stated that communications within the company are usually in English and all employees have a good level of English, it was agreed that the e-mails should be in English. These e-mails were:

- E-mail 1: a request for account verification,
- E-mail 2: a request to download an attachment,
- E-mail 3: a request for private information by e-mail or SMS

Details of the planning of the three phishing e-mails are given in Appendix C pp. 355-365.

1. *E-mail 1: A request for account verification*

This e-mail conveyed a sense of urgency and it looked official (see Figure 6.2). It aimed to direct employees to disclose sensitive information (username and password) into a fake website which looked identical to the legitimate one (AAB company webmail) except that the URL (Uniform Resource Locator) was different from the original, genuine AAB webmail page <http://webmail.aabqatar.com/Login.aspx> (see Figure 6.2).

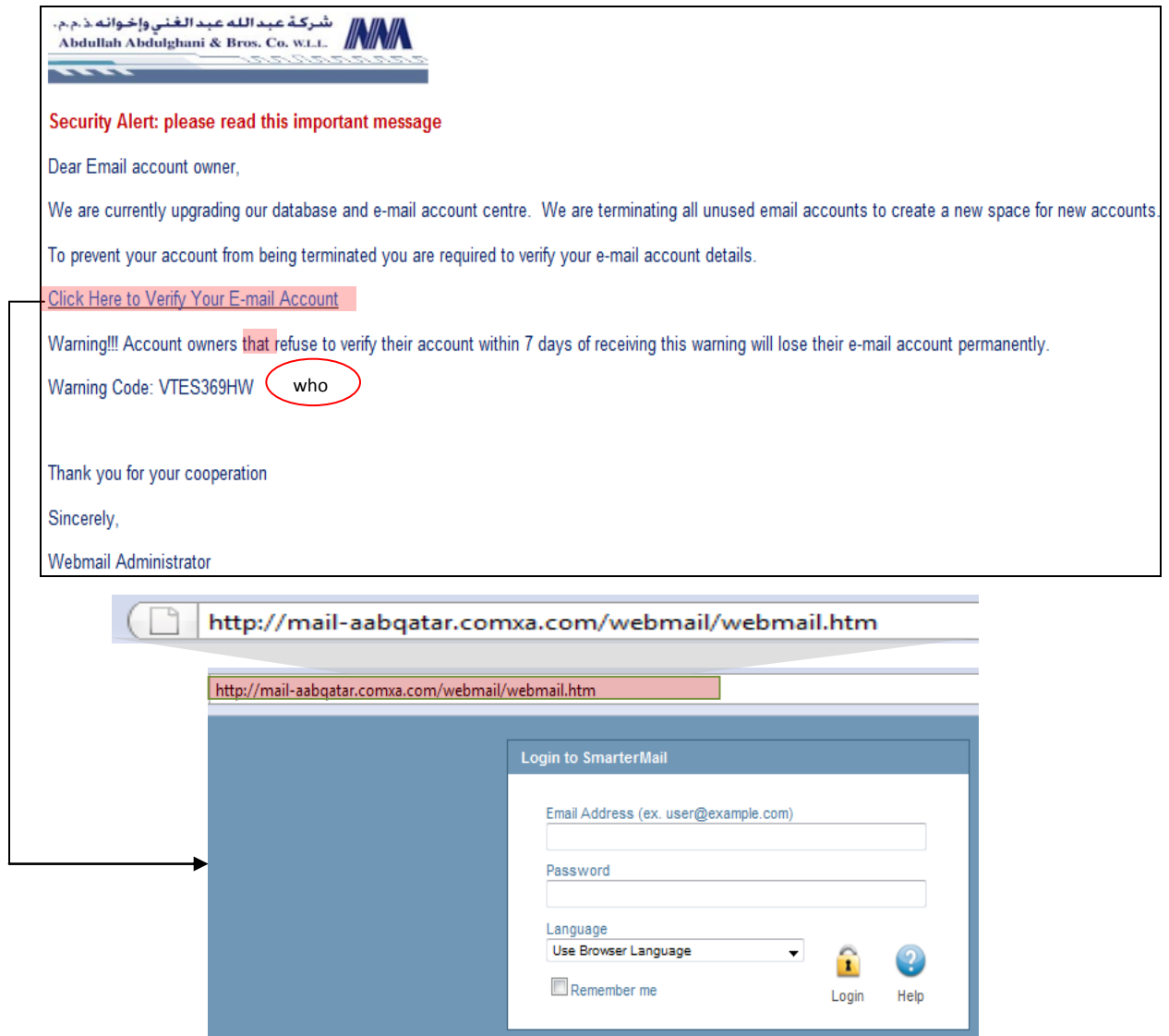


Figure 6.2: E-mail 1 (Account verification)

In addition, the e-mail message contained some grammatical errors not usually found in official e-mails (see Section 2.5.2.1.1) (see Figure 6.2, error highlighted in red). This was another clue which could identify the illegitimacy of the e-mail. The fake webpage had PHP (Hypertext Preprocessor) script to record any username and password entered in the fields; also, it contained a counter using a Google analytics tool to count visitors to the website (see Appendix C for design details). Furthermore, the test applied embedded training, where victims who failed in the test and had given their login details were directed automatically to a webpage which alerted them to phishing. The alert message is shown in Figure 6.3.



Figure 6.3: Embedded training alert message

E-mail 2: A request to download an attachment

This e-mail conveyed a sense of surprise and excitement to trick employees to download the attachment which is interesting for most employees in AAB, ‘The latest Toyota car model’ (see Figure 6.4). Although the attachment was safe, this e-mail assessed employees’ vulnerability to falling prey to phishing e-mails which may contain viruses or Trojan horses in an attachment. The attachment had a counter using the Google analytics tool to count the number of people who download the attachment file (see Appendix C, pp.359-360 for more details).

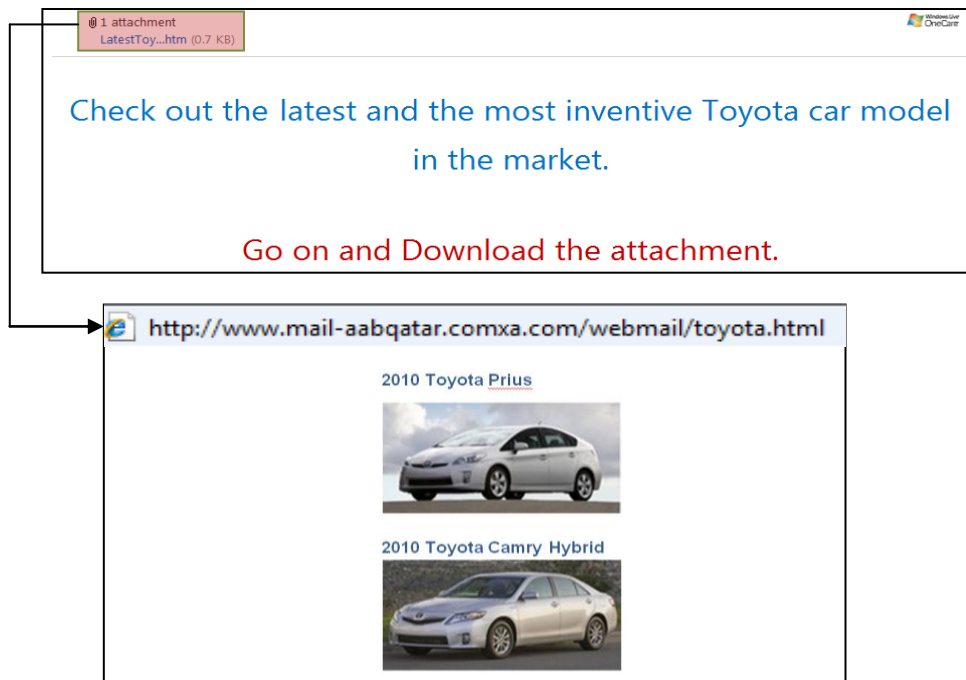




Figure 6.4: E-mail 2 (Request to download attachment)

E-mail 3: A request for private information by e-mail or SMS

This e-mail asked employees to disclose their name and country through offline communications (telephone) or an online communication (e-mail). The e-mail conveyed a sense of moral decency and urgency and tried to exploit people's emotions by discussing human cloning and requesting support for a petition against it (see Figure 6.5). Please see amendments in the Appendix C version.

Currently, a group of scientists in the United States is engaged in cloning children.

It is well known that human cloning is unacceptable in terms of the humanitarian, ethical and social grounds. Many religious scholars believe that human cloning undermines the sanctity of human life.

If you are against human cloning please support our petition by sending your name and your country to this e-mail (human_rights@live.co.uk) or by sending an SMS to this number  (00447846622760) 

After 14 days this information will be presented to the Commission on Human Rights towards stopping this project.

You can save humanity, please don't hesitate in supporting our petition.

Figure 6.5: E-mail 3 (Request for private information by e-mail or SMS)

Due to the confidentiality of such a study, it was agreed that the IT team in AAB would have full control of the reality study by providing them with all the files and databases required to have control of all of the information disclosed in the study (i.e. access to the web host supplied in e-mails 1 and 2, access to the e-mail address and phone number and e-mail address supplied in e-mail 3). Moreover, to ensure the privacy and security of the study, they undertook the implementation and provided the researcher with the results. In order to ensure a fair study, the AAB team used an unknown e-mail address to send the three e-mails to the 129 Qatari employees.

6.2.3.2 Running the test

Before running the study, it was necessary to ensure that the three e-mails were received in the mail inbox and not in the junk or spam mail, in order to assess employees' responses to attacks that breached the technological phishing defences (e.g. spam filter and anti-virus software). In addition, a test was made to determine whether the AAB

e-mail system allows the sending of valid confidential information such as usernames and passwords from its e-mail system.

It was found that the three e-mails sent to the IT Manager were received in his e-mail inbox which means they were not filtered by the AAB e-mail system and that it also allowed the sending of employees' valid account information. For comparison, the author applied the same test to the Loughborough University e-mail system; it was encouraging to discover that the system does not allow sending of valid Loughborough e-mail account information (i.e. username and password).

It was agreed to send the three e-mails one at a time and a reminder after one week to remind employees and to present a sense of urgency. After two weeks, the results of the study were gathered. The researcher required the following information from the study:

From the Microsoft Outlook Read Notification:

This gives the number of employees who read the three e-mails. However, this is still not very reliable because the recipients have to confirm the read notification. Nevertheless, it gives an indication of the approximate number of employees who have read the e-mail.

From the website counter (Google analytics tool):

This gives the number of employees who entered the website supplied in e-mail 1 and downloaded the attachments in e-mail 2.

From the website database in e-mail 1:

This gives the number of employees who would disclose their account information (username and password)

From the e-mail address and phone number supplied in e-mail 3:

This gives the number of employees who would disclose their private information on either communication channel (phone or e-mail)

From AAB's IT call centre:

This gives the number of employees who reported the case or called for assistance.

Due to the confidentiality of the information required in e-mail 1, AAB did not agree to the inspection and validation of the disclosed information (i.e. username and password).

6.2.3.3 Analysis of the Results and Discussion of the Findings

The results of the study gathered from the AAB team (see Table 6.1) were a shock for AAB, as nearly half (44.2%) of the employees had failed in the reality study. Most failures were with e-mail 2 and then e-mail 1, with only a few failing on e-mail 3. The IT Manager noted that there were no replies by SMS which might be due to its cost.

However, the percentage of people who read the e-mails was quite low: 29%, 27.1% and 21% for e-mails 1, 2 and 3, respectively. The AAB team explained this low figure with the possibility that some employees might ignore the e-mails because they detect them as phishing and some might not be interested. They also referred to the inopportune timing of the study in summer when most employees were on vacation and did not check their e-mails. However, that was the most convenient timing for both the researcher and the AAB team. Nevertheless, the percentage of people who became victims in the attack as a proportion of those who read the phishing e-mails was very high, at 95-99%. Furthermore, more than 97% of people who entered the URL given in e-mail 1 did then verify their account information. This implies that most victims do not have the ability to recognise phishing attempts from an e-mail message with a fake website by checking the URL. It was reported by AAB that out of the 72.1% of employees who took positive action by calling the IT department for assistance on the received phishing e-mails, there was a high percentage (59%) for e-mail 1 and none for e-mail 3.

The AAB team reported receiving more calls from employees requesting help on e-mail 1 because it looked official, as though it was from the AAB Webmail Administrator, and a lot of employees were concerned, whereas the other two were not related to AAB, especially e-mail 3 about human cloning. They added that they did not expect that nearly half would succumb to phishing, and e-mail 2 made them concerned that their employees are vulnerable to viruses or Trojan programs. In addition, e-mail 1 comes

next in the number of failures and it was a shock for the AAB team that 15% of the 129 employees had disclosed their confidential information. On the other hand, fewer employees fell prey to e-mail 3 (only 4%), which is a good point to consider. However, AAB mentioned that e-mails 1 and 2 are more hazardous than e-mail 3 which asked for general private information (name and country) that will not cause major consequences for the company compared to viruses accessing employees' PCs or to unauthorised persons' access to employees' e-mail accounts. In conclusion, the ABB team deduced that there is a need for a programme to enhance employees' awareness of phishing.

Table 6.1: Results of Reality Study 1

Reality study 1 results		
Total e-mails sent to Qatari employees	129	
E-mail 1		
Received read notification from users	54	41.8%
Users opened URL given in e-mail	49	38%
Users verified their e-mail account	19	15%
Users called the IT department	22	59%
E-mail 2		
Received read notification from users	35	27.1%
Users downloaded attachment given in e-mail	33	26%
Users called the IT department	5	14%
Email 3		
Received read notification from users	27	21%
Users replied by e-mail	5	4%
Users replied by SMS	None	
Users called the IT department	None	

The penetration test has identified the factors which make Qatari employees susceptible to phishing attacks. The factors, having been discovered from the test outcome, were further explored through interviews held with the AAB IT team. The results are summarised in Table 6.2.

Table 6.2: Vulnerabilities identified in Penetration Test 1

Factors making Qatari employees susceptible to phishing	Evidence
Most do not react/ report phishing incidents.	79% did not report to the IT department
Qataris are affected by incentives and disincentives which can lead sometimes to circulating and exchanging of phishing e-mails and sites among people, which give phishing credibility. There is a lack of knowledge on Internet threats, in particular, phishing threats and on how to protect themselves against phishing attacks and how to detect phishing.	Interview with employer and IT team at AAB. 44% failed in the test where all e-mails involved incentives and disincentives matters. About half have lack of awareness of phishing.
They trust official communications, especially through their employers	15% failed on e-mail 1 which involved the use of official communication and trust of employers
A few Qataris are motivated by religious and moral considerations, being helpful, emotional and good willed in their philanthropy, compassion and clemency, especially for people in need. Maybe it was not interesting and attractive for this group for particular reasons.	4% have failed on e-mail 3 which exploits people's emotion.
Qataris have a curiosity and seek out knowledge and discovery, especially in matters close to their interests. Qataris have a susceptibility to different kinds of temptations, to satisfy their desires and needs	26% failed on e-mail 2. Interview with the employer and IT team in AAB.
Discussions with the employer	
It is in their nature of Qataris to feel too embarrassed and stupid to mention or report phishing and that they have fallen prey to it.	Interview with the employer and IT team in AAB.
Many Qataris have not absorbed the technology, especially with the rapid development experienced in Qatar. Some have overconfidence in technological tools, especially anti-virus software, for protecting against all kinds of phishing.	Interview with the employer and IT team in AAB. However, this is in conflict with the survey results in Chapter 5 where Qataris were found to be confused about the reliability of such tools

6.2.4 Conclusion

The penetration test showed that the state of awareness of e-mail phishing for Qatari employees in AAB needs to be improved since about 44% failed in the test, which means there is a possibility of phishers' reaching sensitive organisational information or private information. It was found that phishing e-mails with attachments are more successful in tricking employees than official-looking ones which asked for confidential

information and e-mails which exploit people's moral feelings. In addition, the result shows that victims were unable to recognise phishing attacks from the fake URL given or from the e-mail message being from an unknown sender or from an e-mail which contains a deceptive message with either a request for information or downloading of files which contain viruses.

Although this study was made with a small sample of employees in one organisation in Qatar, it was valuable since it assessed Qatari employees' responses to phishing e-mails in reality. However, there was a need for another penetration test where the researcher would have more control, could use different phishing techniques, make the study on a sample of Qataris with different backgrounds (age, education, occupation and computer knowledge) and interact with them. The second penetration test was therefore carried out.

6.3 Penetration Test 2

Phishing has two parts: as well as the technical aspects, there is social engineering, where phishers try to study the community and the characteristics of victims for use in tricking them and attaining their goal.

From the literature and from the interviews held with the officer of the Computer Crimes Unit in the Ministry of Interior and the information security specialists in Q-CERT in the field of e-crime and awareness (see Chapters 2 and 4), it can be concluded that phishers usually study the interests of potential victims to use them to attract their targets. This study aims to assess the vulnerability of Qatari citizens to being tricked when phishers try to attract them using their interests. The intention was to conduct an anonymous experiment which targeted a selected sample of Qatari e-mail users aged over 12 with different backgrounds in age, education, occupation and computer knowledge.

6.3.1 Test 2 Process

The spear phishing penetration test went through different stages from planning and designing through conducting the experiment to, ultimately, analysing the results and discussing the findings (see Figure 6.6).



Figure 6.6: Penetration test 2

6.3.1.1 Planning and Design

As it is difficult to recognise the interests of strangers, with a view to using them to snare their victims in phishing attacks, it was decided that the experiment would take advantage of the researcher's family and relatives.

In the planning and design phase, experts in IT and awareness were involved in defining an effective plan for the experiment. A discussion took place between the researcher and experts from Q-CERT (Qatar Computer Emergency Response Team), Dr. D. Phelps, an information scientist working with Outreach and Training, N. Al-Abdullah, the acting OA&T manager and M. Kamal, the Senior Incident Manager.

The group of experts found the proposed experiment to be novel and interesting but had some concerns on the legality and authority of the experiment. However, since the experiment used the researcher's family and relatives, she found no problems in conducting it since it was not harmful to the 'victims'. However, the discussion concluded that it would be useful for participants to certify their approval after the experiment to confirm retrospectively that they did not object to participating (see Appendix C).

The experimenter had identified a list of family members and relatives and then chose only the ones meeting the experimental criteria (Qatari e-mail users aged above 12), as mentioned earlier. Finally, 30 participants of different background (age, education, occupation and computer knowledge) were chosen to be targeted victims for the experiment.

The participants were reasonably representative of the population as a whole and they varied in their background as follows:

Age: 6 below 18, 19 in the range 18-29, 3 in the range 30-50 and 2 over 50

Education: 15 school, 12 higher education, 3 postgraduate education

Occupation: 16 students, 7 employees, 4 both employees and students, 7 others (e.g. retired or housewife) and 2 businessmen.

Computer knowledge based on researcher's judgement: 8 poor, 8 average, 7 good and 7 with expert knowledge

Before designing the phishing e-mails, the interests of each victim were identified, according to the researcher's knowledge gained from the long family relationship with the victims. The judgement of computer knowledge was based on whether they had an e-mail account and a computer and what they used the Internet for. Also the length of time of their computer experience was taken into account. For example, if the victim had recently acquired a computer and an e-mail account but had not previously used a computer, then it is more likely that they would have poor computer knowledge (see Appendix C).

The researcher tried to phish the targeted victims without them noticing by taking advantage of her knowledge about them, such as their e-mail address and interests. See Appendix C for full details of the experiment planning and design. The study was kept private and in total 30 separate phishing e-mails were sent, one to each target participant, with each e-mail tailored at the intended victim's interests, supported by different techniques to attract them, such as conveying a sense of urgency and excitement. For example the participants who have an interest in cars were sent offers of winning free cars in order to attract their interest. Arabic or English e-mails were sent to participants depending on the e-mail topic and the participant's English level; only four e-mails were in English.

6.3.1.2 Running the Test

The researcher chose to do the experiment in Ramadan since it is the month of blessing, worship and spirituality and also in this month there are a lot of deals, offers, and releases of new TV series and films for the coming Eid celebration. It was therefore considered to be an opportune time for the experiment to try to phish people by exploiting the circumstances and the activities of this month.

Ramadan is one of the five pillars of Islam which all Muslims are expected to follow. It is the month when the Qur'an was first revealed to the Prophet Mohammed. In Ramadan, Muslims fast from eating, drinking, smoking and indulging in anything that is in excess or ill-natured, from dawn until sunset. It is the time for spiritual reflection and prayer, therefore Muslims are expected to do good actions (e.g. avoid lying and greed and help poor people). After Ramadan, Muslims celebrate 'Eid Ul Fitr' where Muslims break their fast. It begins with a special Eid prayer and then Muslims wear their finest clothes and meet each other, have special meals and exchange gifts. This has some similarities to Christmas celebrations in the UK. At Eid, it is obligatory to give 'Zakat al-Fitr', an amount of money for charity, to help poor people to celebrate Eid (Gaffney, 2003: 394-400).

To measure the victims' response to phishing attacks, counters were added to the websites and attachments in the phishing e-mails, using the Google analytics tool. Also the researcher viewed the victims' replies to phishing attacks either through e-mails, SMS or through registration to websites. To give more chance for replies, the experiment lasted for about two weeks: e-mails were sent in the middle of Ramadan and the data collected after Eid.

6.3.1.3 Analysing Results and Discussing Findings

The result of the experiment shows a quite high level of user failure, 17 out of the 30 participants (56.7%) having been tricked by the phishing e-mails. To have a better understanding of participants' responses, semi-structured interviews were held with

participants after the experiment. The reasons for their failure in the experiment varied for each participant. Some of the reasons were:

- The amazing offer made in the e-mail,
- Over-confidence of the participant that they will not get phished,
- The e-mail's appeal to their interest,
- A lack of awareness about the global extent of phishing and trust in the native language (they did not think phishing attacks would be made in Arabic),
- A lack of awareness of possible phishing attacks and techniques (some thought that phishing will ask only for confidential information such as a password and bank account),
- The existence of similar e-mails in this month (e.g. offers of discounts),
- The appeal to participants' good will (e.g. the participant never thought there would be phishing associated with 'Zakat al-Fitr', required of every Muslim).

Not all participants who did not fail in the experiment detected that the e-mail was a phishing attack. Only 5 out of 30 recognised that it was a phishing attempt. The attacks were recognised because:

- It was from unknown sender
- They had been tricked before
- They had heard about similar e-mail attacks

The rest did not fail in the test for the following reasons:

- They had not had the chance to check their e-mails
- The need for registration

- Their preference for a physical shopping experience
- The influence of religion and the circumstances of the month which overcame the interest of the participants (e.g. one of the participants did not download the music they were interested in because they believe that it is not right to listen to music in Ramadan since it is the month for worship of God).

None of the participants had looked at the security indicators such as https or security certificate and most were unaware of these terms. According to the interviews with participants, about 70% of them did not know the term 'phishing' and the rest did but to a varied extent. This implies a lack of awareness of this threat. In addition, about 60% of participants revealed that they open e-mails from unknown senders and junk mails if they attract their attention.

About 67% had anti-virus software installed in their PC, but only about a half ever updated their anti-virus software. Only a few (13%) had installed spam filters and the rest did not even know what spam filters are. The majority of those who had anti-virus software were surprised that they could be tricked with phishing even with the software installed, since they thought it should be a reliable solution to overcome any threat targeting their computers.

Although 7 out of the 30 participants were computer 'experts', the failure rate was quite high (4 out of the 7) in this group. According to the chi-squared test (see Appendix C, P.369), there is a relationship between participants' computer knowledge and their ability to detect phishing e-mails. However, for more reliable results there is a need for further investigation with a larger sample size (see Appendix C, p.369).

This implies that generally, the responses show experts in computing can also fall prey to phishing, e.g. an e-mail sent to one of them on the coming Arabic drawing exhibition made him fall for it because it attracted his interest in drawing. However, other experts did not fall prey to such e-mails because they had a higher level of knowledge of

phishing and therefore knew not to respond to e-mails from unknown senders. Nevertheless, it can be concluded that there are no specific criteria for being a victim of phishing and everyone might be vulnerable, even experts in computers. This implies a need for enhancing all people's awareness of phishing. There is a common English saying that 'A little learning is a dangerous thing' (Alexander Pope, 1711). This is because people who may be frequent users of computers may think they are more expert than they really are and this can lead to overconfidence in their own phishing detection abilities.

Finally, the test has identified factors which make Qatari employees susceptible to phishing attacks and these are listed in Table 6.3. Many of the factors are similar to those identified from Penetration Test 1. The additional knowledge from both tests has allowed some categorisation of factors in Table 6.3.

Table 6.3: Vulnerabilities identified in Penetration Test 2

Factors which make Qataris susceptible to phishing	Evidence
<p style="text-align: center;">Embarrassment</p> <p>It is in the nature of Qataris to feel too embarrassed and stupid to mention or report that they have fallen prey to phishing.</p>	Interviews with participants
<p style="text-align: center;">Lack of Knowledge of Phishing</p> <p>Many Qataris have not absorbed the rapid advances in technology in Qatar, this leads to:</p> <ul style="list-style-type: none"> • Qataris lack knowledge of Internet threats and, in particular, phishing threats • Many do not expect to be phished • They believe they do not have anything worth stealing • Some do not know how to protect themselves against phishing attacks and how to detect and react to phishing 	<p>Interviews with participants showed 70% did not know the term phishing</p> <p>60% open e-mails from unknown senders and junk mail.</p> <p>Although 67% have anti-virus software on their PC, only 33.3% keep it up to date. Only 13.3% have spam filters</p>
<p style="text-align: center;">Trust in the Security of their Country</p> <p>They only expect phishing to be limited to certain topics or geographical areas – they feel safe in Qatar and therefore think phishing does not reach Qatar</p> <p>Qataris are more likely to be influenced by and trust e-mails in their native language (Arabic)</p>	Interviews with participants
<p style="text-align: center;">Overconfidence in Technology and the Internet</p> <p>Some Qataris have overconfidence in technological tools, especially anti-virus software, for protecting against all kinds of phishing.</p> <p>Some have overconfidence in the technological revolution and believe that everything on the Internet is true.</p>	Interviews with participants
<p style="text-align: center;">Religion, Morality and Generosity</p> <p>Qataris are motivated by religious and moral considerations, being helpful, generous, emotional and good willed in their philanthropy, compassion and clemency, especially for people in need, in particular in the religious seasons, and when disasters and famines occur around the world.</p> <p>Qataris have a love for spreading good, e.g. spreading good ideas, which can be used by phishers to distribute phishing e-mails</p>	<p>When the tests were held in a religious season it was discovered that religion has major effect on people's responses to the test</p> <p>Interviews with participants</p>
<p style="text-align: center;">Trusting Nature</p> <p>Qataris are trustful and not do not have bad faith in people, believing that others will be equally driven by religious and moral considerations</p> <p>They believe in e-mails that exploit religion and people's generosity at times of natural disasters</p> <p>They trust official looking communications from trustworthy institutes in the society</p> <p>Confidence and trust in friends gives phishing e-mail credibility if sent from a person they know.</p>	<p>When the tests were held in a religious season it was discovered that religion has major effect on people's responses to the test</p> <p>Interviews with participants</p>
<p style="text-align: center;">Curiosity and Temptation</p> <p>Qataris have a curiosity and seek out knowledge and discovery, especially in matters close to their interests.</p> <p>Qataris have a susceptibility to different kinds of incentives and temptations to satisfy their desires, needs and beliefs, such as magic, superstition, envy, horoscopes, astrology</p> <p>Qataris excitement over incentives and temptation can sometimes lead to circulation and exchange of phishing e-mails and sites among their contacts, which gives the phishing credibility.</p>	<p>57% failed in the test which exploited their interests and needs.</p> <p>Interviews with participants</p>
<p style="text-align: center;">Personal Characteristics</p> <p>Qataris can be overconfident that they, themselves will not be tricked</p>	Interviews with participants

6.3.2 Conclusion

The experiments show that more than half of the participants (57%) were vulnerable to fall prey to phishing attacks. The detection rate was fairly small (about 17%) and the rest did not fail the test for other reasons, such as not having the chance to check their e-mails. It was observed that religion has an effect on participants' responses to phishing and sometimes it even comes as a first priority over their interests, especially in the month of Ramadan when people's good will and emotions could be exploited by phishers. Furthermore, the study illustrated that Qataris are vulnerable to e-mail phishing when it plays on their interests, emotions and religion.

More than 50 per cent of participants were not aware of phishing and opened e-mails from unknown senders and from junk mail and had not installed spam filters to help to protect themselves against phishing. Although it was pleasing that about 67% have anti-virus software, there is a problem that most do not update it regularly and have over-confidence that these programs will remove all online threats. This shows that there is a lack of awareness of phishing and how to defend against it.

Also, results indicate that there are no specific criteria for being a victim of phishing and everyone might be vulnerable, even experts in computers, though a few experts in phishing were more able to protect themselves. Therefore, there is a need for enhancing people's awareness of phishing to improve their protection level against it.

6.4 Laboratory Experiment

The laboratory experiment aimed to discover the factors which might affect Qataris' responses to e-mail phishing attacks such as the cultural, country-specific factors. Also it attempt to assess Qataris' responses to phishing in a laboratory experiment compared to previous penetration tests.

6.4.1 Experimental Process

A procedure with four stages was carried out: planning and designing, conducting the study, evaluating participants' responses and, finally, analysing results and discussing findings (see Figure 6.7). Each stage is explained as in Figure 6.7.

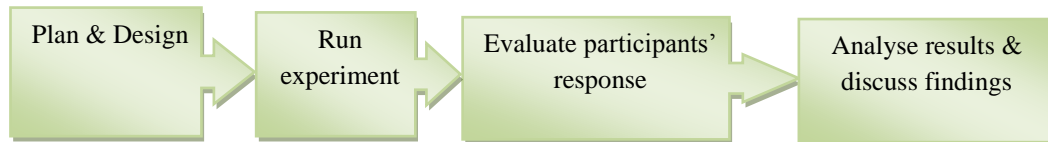


Figure 6.7: Laboratory experiment process

6.4.1.1 Planning and Design

In the planning stage, a group of six experts in IT and education were involved in the planning and designing of the experiment to ensure it was efficient and well planned (see chapter introduction for details of experts involved).

Planning and designing the study took two weeks, as it involved discussions on identifying an effective experiment which would suit participants and fulfil the aim of the study. One or two, 1 to 2 hour discussions were held with each person. A group discussion was held with the 3 First Lieutenants in the Ministry of Interior for reasons of convenience and their relationships with each other, whereas the rest were met individually.

It was agreed by the group to plan and design an experimental lab study where study participants would be asked to identify the phishing e-mails from a list consisting of an unknown mixture of phishing and legitimate e-mails

There was much debate on the reasonable number of e-mails for the study, finally the decision was to have only 10 since this is a practical number for participants not to get bored and at the same time enough for the researcher to assess participants' recognition of different phishing attacks.

There was a suggestion of having the study as a kind of quiz where the e-mails would be displayed one by one and participants would be asked to make their decision of either phishing, legitimate or skip. However, there was another suggestion which was to provide the study with the effect of a real environment by inspecting real e-mails received instead of images presented in a quiz. Ultimately, the group decided on the latter, where the researcher signed up a multiple e-mail address and sent the experimental e-mails into those accounts to set up the test. Later, she provided participants with the login details for the e-mail accounts to access and inspect the e-mails and then indicate their decisions of either phishing or legitimate in the paper-based answer sheet provided.

With regard to the e-mails designed for the study, it was decided have 10 e-mails, 4 in English, 5 in Arabic and 1 in both languages. The final 10 e-mails were 6 phishing e-mails in Arabic and 4 legitimate ones in English. However, this does not indicate that phishing e-mails should be in Arabic or vice versa, the decision on the language depended on the topic of the e-mail itself (e.g. bank e-mails are usually in English whereas Zakat requests are in Arabic). The test applied contextual training, where victims at the end of the test were given some knowledge on the phishing threat, similar to that shown in Figure 6.3.

In total, 30 new participants from different backgrounds (age, education level, e-mail phishing knowledge and occupation) were involved in the study, similarly to the previous one. In this study, the researcher used convenience sampling, taking advantage of friends and colleagues in her workplace to take part in the study.

Participants were asked to give their demographic details which were as follows:

E-mail phishing level of knowledge: 10 poor, 8 average, 7 good and 5 with expert knowledge

Age: 15 in the range 18-29, 11 in the range 30-50, with only 4 over 50

Education: 8 school, 19 higher education, 3 with postgraduate education

Occupation: 13 students, 14 employees, 2 both employees and students and 3 others (retired, housewife, unemployed)

Before designing the phishing e-mails, it was crucial to search for both legitimate and phishing ones and then choose those that would best fulfil the aim of the study. E-mails assigned for the experiments were adapted from legitimate e-mails and phishing e-mails gathered from searching and or were new e-mails associated with Qatar (e.g. an e-mail about Doha Bank and Q-tel) designed by the researcher. Legitimate e-mails were gathered from legitimate communications from Microsoft, Doha Bank, Dohasooq (the first e-commerce initiative by a leading financial entity in the Middle East) (Dohasooq, 2007) and Facebook which has recently become popular in Qatar as a form of communication. The e-mails offered the following: a discount for Doha Bank Travel Insurance, a free anti-phishing tool from Microsoft (namely, Microsoft Phishing Filter Add-in for MSN Search), fabulous prizes from Dohasooq and an invitation from Facebook. Although the invitation from Facebook would be from an unknown person, it might be legitimate since it directed the recipient to go to the official Facebook website.

Table 6.4: Six Phishing E-mails Used in Identification Test

E-mail topic	Techniques of phishing e-mail
Fulfil your Zakat online	Uses Qataris' emotions and religion and their trust in the Zakat fund institute and also requests victims to distribute the e-mail with their mailing list by using the belief in God's blessing and the need for help in spreading doing good. This type of phishing takes advantage of victims in distributing the phishing e-mail without their noticing the deception, which will then end up with more victims falling in the attack since the next victims might trust the e-mail because it comes from a person they know. This trick leads to building more confidence in the phishing e-mail.
You can know the person who loves you	Conveys a sense of excitement and interest through using people's emotions and love. As in the previous email, it makes a demand to distribute the e-mail to 15 people, leading to further exposure to the e-mail content.
Q-tel downloads mozaic	Identical to an official and legitimate e-mail sent from an ISP in Qatar (Q-tel), but which directs to a fake website similar to the Q-tel official site with only a small difference in the URL. Conveys a sense of official communication from a trusted institute.
Buy/sell your shares online	The Doha Securities Market (DSM) created in 1995 has become well known in Qatar from 2005, after establishment of the Financial Markets Authority (QFMA) and Doha Securities Market Company (DSMC) which plays a big role in securities' trading. However, in June 2009, Qatar Exchange (QE) had a successor (DSMC), with the aim of creating an international exchange based on international best practices (Qatar Exchange, 2009). To take advantage of this event, e-mails sent to invite people to use new QE website for online securities' trading, misusing trust built in the secure Qatar share market website.
Help to enhance e-services in Qatar	Uses trust in MOI e-services with an apparent official communication employing the Ministry of Interior (MOI) logo to direct people to fake website very similar to URL of MOI website. It also, conveys a sense of intimidation and urgency to pay bills as soon as possible to avoid the bills increasing.
Carrefour promotions	Identical to a legitimate e-mail sent by Carrefour supermarket, well known in Qatar, that keeps customers updated on recent promotions, products and services, but instead of directing customers to original Carrefour site, actually directs them to fake URL similar to legitimate one but with numbers appearing at beginning. The e-mail uses an existing Carrefour image but embeds a fake URL hidden under a button. This e-mail uses sense of excitement and interest and takes advantage of time when children are going back to school.

The phishing e-mails aimed to measure the vulnerability of Qataris to phishing by using different techniques to trick Qataris such as by playing on their emotions and religion. Ultimately, the study involved inspecting the 10 e-mails listed in Table 6.4 (see Appendix C for more details).

6.4.1.2 Running the Experiment

The study was made with a sample of people chosen according to pre-defined criteria (Qatari e-mail users over 17, since at this age they are mature and responsible for their actions, where most have a source of income and a bank account which most e-mails in the study ask for, with different backgrounds in terms of level of knowledge of e-mail phishing, age, education and occupation). It was decided in the discussion group that 30 participants were enough as a sample for the study. The researcher found difficulty in recruiting participants for the study and therefore the decision was made to take advantage again of friends and relatives. Since the sample was quite large for the researcher to handle in one session, the study was held in her workplace in 3 sessions, with 10 people each time, according to their availability. The study was prepared in advance, where the 10 e-mails sent to e-mail addresses assigned for the experiment, then it was necessarily to ensure that all e-mails were received in the inbox. Later, the study commenced with an explanation for participants on the aim and procedure of the study, showing them an example of how to complete the test. The participants were allowed 20 minutes to complete the test, as the discussion group concluded that a maximum of 2 minutes should be spent in inspecting each e-mail.

The participants were asked to log in into the e-mail account to view the 10 e-mails received and to identify the phishing e-mails from a complete list of the e-mails on an answer sheet provided. Participants were instructed to inspect the e-mails carefully but without paying attention to the sender's e-mail as all e-mails were sent from the experimenter's account for the purpose of the study (see Appendix C for more details).

6.4.1.3 Evaluating the Participants' Responses

Unlike the previous studies, in this study, full interaction with participants was possible during the experiment. To facilitate assessment of the study, participants were scored out of 100 according to their responses in the answer sheet, a score of 10 being assigned for each correct answer. Later, all scores were collected and counted along with the wrong detections made by each participant, which was important for the evaluation.

The participants' responses were evaluated to identify the factors which make Qataris vulnerable to e-mail phishing. The participants were also asked to provide their opinion on the study, giving the reasons for their responses and identifying the influence of any culture effect in making phishing successful in Qatar. This was achieved by holding in-depth discussions with individual participants after the experiment based on their scores and wrong detections and the following semi-structured discussion points (see Appendix C for more details about the evaluation phase):

1. Were you aware of the phishing threat before?
2. What was the reason for your taking more time than allocated? (For participants who took more time than allocated to complete).
3. Which of the given e-mails did you spend more time on to detect whether it was phishing or legitimate? And why?
4. Look at your wrong detections, what are the reasons for your incorrect response? (For participants with scores less than 100).
5. Which was the most tempting phishing e-mail?
6. Which of the given e-mails was difficult or tricky to detect as phishing or legitimate? And why?
7. Why do you think Qatari people could be vulnerable to falling prey to e-mail phishing attacks (e.g. effect of native language, kindness, etc.)?
8. How do you think Qatari culture affects people's responses to phishing attacks? Why is that? What are the possible cultural factors?

9. What do you think is the most successful trick that phishers could use on Qataris? Why?
10. What have you learnt from the study? Have you achieved any new knowledge about phishing?
11. Did you find it useful? And what did you like and dislike about it?
12. Do you have any comments or suggestions on how to improve the study?

After discussions with all participants, the factors which make Qataris vulnerable to phishing attacks were identified. The outcomes were then presented to experts in Qatar culture for review and to further focus on the cultural effects. Semi-structured interviews were held with the Qatar Cultural Attaché in the UK and a researcher in Qatar culture from the Ministry of Culture, Arts and Heritage.

6.4.1.4 Analysis of Results and Discussion of the Findings

The data gathered from the evaluation were analysed quantitatively and qualitatively to identify participants' susceptibility to phishing and the cultural and country-specific factors which make Qatari citizens susceptible to this kind of attack. The participants' level of detection was classified according to their scores in the study as follows: excellent (100), very good (70-90), good (50-60) and poor (below 50) (see Table 6.5).

Table 6.5: Score rating for laboratory experiment

Participants' detection level	Scores	Number of participants N=30	% of participants
Excellent	100	3	10
Very good	70-90	9	30
Good	50-60	11	37
Poor	Below 50	7	23

The responses show that 20 (67%) of the participants had a good or very good detection level, only 3 (10%) had an excellent level and the rest had a poor level. Although this shows a reasonable level of detection by participants, a single instance of a wrong

detection of phishing can lead to failure against this attack and to major consequences. Similarly, wrong detection of legitimate e-mails might lead to other consequences such as wrong reactions and ignorance. Therefore, there is a need to increase all participants' level of detection to excellent.

In addition, 40% of detections were wrong. The wrong detections for phishing e-mails were fewer (36%) than legitimate ones (46%), which indicates that participants were less able to distinguish legitimate e-mails which might lead sometimes to ignoring legal e-mail. However, more than one third are vulnerable to an e-mail phishing attack which is more risky than ignoring legitimate e-mails (see Table 6.6).

Table 6.6: Results for the Laboratory experiment

No.	E-mail topics	Number of Wrong detections	% of total Wrong detections
<i>Phishing e-mails</i>			
1	Fulfil your Zakat online	22	18%
2	You can know the person you love	11	9%
3	Q-tel downloads mosaic	8	7%
4	Buy/sell your shares online	15	13%
5	Help to enhance e-services in Qatar	5	4%
6	Carrefour promotions	4	3%
<i>Legitimate e-mails</i>			
7	Doha Bank Travel Insurance	20	17%
8	Protect from viruses and phishing	19	16%
9	You can win fabulous prizes in Dohasooq	11	9%
10	Invitation from Facebook	5	4%

Accordingly, false positive and false negative rates were measured as follows:

False positive rate = no. of false positives/no. of legitimate sites

False negative rate = no. of false negatives/no. of phishing sites

According to the test results, the false positive rates were slightly higher with an average of 13.8 (46%) than false negative rates which reached an average of 10.8 (36%). This implies that there is confusion in discrimination between phishing attempts and legitimate e-mails.

However, the number of wrong detections varies for each e-mail in the study. For phishing e-mails, the e-mail with the request to fulfil Zakat online and the e-mail for online securities trading had high wrong detection compared to other phishing e-mails. The participants revealed in their interviews that this was because they were written in the participants' native language, participants trusted the institute, the e-mails exploited their emotions, beliefs and religion and there were very minor differences between the fake and the real URL.

On the other hand, two legitimate e-mails were wrong designated as phishing by at least five participants, the Doha Bank travel insurance and Microsoft protection from viruses and phishing. The reason given was that Microsoft and the banks were commonly targeted by phishing. Participants were confused in making the right detection for the legitimate Facebook invitation because of the known recent exploitation of Facebook by phishers (Acohidio, 2009; Dodge, 2009; Mills, 2009; Schofield, 2009) (see Table 6.6).

The discussions indicated that many people do not normally take enough time to recognise phishing attempts by inspecting security indicators, and some were even guessing. However, the pattern of results could not be derived from pure random selection by the participants so they had clearly considered their answers in the tests. These were to be expected as the participants were aware of the importance of their contribution and were asked to read everything carefully and were given enough time to do so. However, some mentioned that they did not have sufficient knowledge about security certificates and how to check their validity and their decisions, therefore, were made according to their intuition rather than from reading the e-mail content itself. Participants were generally more cautious in this test due to the fact they knew it was a test, and this led them to consider the possibility that most e-mails could be phishing, which the discussions revealed would not be how they would react in their normal daily activity.

The majority found that the most tempting phishing e-mail was the one about "You can know the person you love"; this was exciting and a clever trick which attracted people's emotions and beliefs about love.

Following the experiment, participants and experts in Qatar culture were then invited into discussions. The participants found the experiment very useful since it enhanced

their knowledge of phishing, especially on how to detect phishing attempts against legitimate e-mails. In addition, discussions with participants and experts in Qatar culture highlighted some of the false beliefs such as over-confidence in the reliability of anti-virus software to detect phishing, over-trust of e-mails apparently from official and trusted institutes in Qatar and belief in a limitation of use of certain topics for phishing, especially religious ones. However, some participants recommended repeating the experiment with more participants to get more reliable results.

From the experiment conclusions were also drawn on the aspects which make Qataris susceptible to phishing threat. Some factors confirmed the findings of the penetration tests but there were some additional factors. In Table 6.7 the factors repeating the findings of the penetration tests are in italics, though the evidence in the right hand column is new evidence from the laboratory experiment and the follow-up interviews. New factors are underlined.

Table 6.7: Vulnerabilities identified in laboratory experiment

Factors which make Qataris susceptible to phishing	Evidence
<p style="text-align: center;">Embarrassment</p> <p>It is in the nature of Qataris to feel too embarrassed and stupid to mention or report that they have fallen prey to phishing.</p>	Interviews with participants, the Cultural Attaché and the expert in Qatar culture
<p style="text-align: center;">Lack of Knowledge of Phishing</p> <p>Many Qataris have not absorbed the rapid advances in technology in Qatar, this leads to:</p> <ul style="list-style-type: none"> • Qataris lack knowledge of Internet threats and, in particular, phishing threats • Many do not expect to be phished • They believe they do not have anything worth stealing • Some do not know how to protect themselves against phishing attacks and how to detect and react to phishing. 	40% of the decisions were wrong because of a lack of ability to detect legitimate and phishing e-mails 90% of participants made at least one wrong decision Interview with participants, Cultural Attaché and the expert in Qatar culture
<p style="text-align: center;">Trust in the Security of their Country</p> <p>They only expect phishing to be limited to certain topics or geographical areas – they feel safe in Qatar and therefore think phishing does not reach Qatar</p> <p>Qataris are more likely to be influenced by and trust e-mails in their native language (Arabic)</p> <p><u>They believe they have no enemies who want to hurt them</u></p>	Interview with participants, Cultural Attaché and the expert in Qatar culture
<p style="text-align: center;">Overconfidence in Technology and the Internet</p> <p>Some Qataris have overconfidence in technological tools, especially anti-virus software, for protecting against all kinds of phishing.</p> <p>Some have overconfidence in the technological revolution and believe that everything on the Internet is true.</p>	Interview with participants, Cultural Attaché and the expert in Qatar culture
<p style="text-align: center;">Religion, Morality and Generosity</p> <p>Qataris are motivated by religious and moral considerations, being helpful, generous, emotional and good willed in their philanthropy, compassion and clemency, especially for people in need, in particular in the religious seasons, and when disasters and famines occur around</p>	73% were tricked by the e-mail to fulfill Zakat online Interview with participants, Cultural Attaché and the expert in Qatar culture

the world. Qataris have a love for spreading good, e.g. spreading good ideas, which can be used by phishers to distribute phishing e-mails	
<p style="text-align: center;">Trusting Nature</p> <p>Qataris are trustful and do not have bad faith in people, believing that others will be equally driven by religious and moral considerations</p> <p>They believe in e-mails that exploit religion and people's generosity at times of natural disasters</p> <p>They trust official looking communications from trustworthy institutes in the society</p> <p>Confidence and trust in friends gives phishing e-mail credibility if sent from a person they know.</p>	<p>73% were tricked by the e-mail to fulfill Zakat online</p> <p>18% were tricked by the e-mail appearing to be from the MOI</p> <p>Interview with participants, Cultural Attaché and the expert in Qatar culture</p>
<p style="text-align: center;">Curiosity and Temptation</p> <p>Qataris have a curiosity and seek out knowledge and discovery, especially in matters close to their interests.</p> <p>Qataris have a susceptibility to different kinds of incentives and temptations to satisfy their desires, needs and beliefs, such as magic, superstition, envy, horoscopes, astrology.</p> <p>Qataris excitement over incentives and temptation can sometimes lead to circulation and exchange of phishing e-mails and sites among their contacts, which gives the phishing credibility.</p> <p><u>Qataris love adventure</u></p>	<p>36% fell prey to the e-mail on "You can know the person you love"</p> <p>The majority failed at least one test where the emails attracted their interests</p> <p>Interview with participants, the Cultural Attaché and the expert in Qatar culture</p>
<p style="text-align: center;">Personal Characteristics</p> <p>Qataris can be overconfident that they themselves will not be tricked</p> <p><u>They lack concern about consequence of phishing, especially if not on their own computer (e.g. work PC)</u></p>	Interviews with participants
<p style="text-align: center;">Friendliness and Courtesy to Others.</p> <p><u>Qataris are friendly and like making friends and knowing people</u></p> <p><u>Qataris are courteous to other people, including strangers and even to extent of giving confidential information when asked.</u></p>	Interview with participants, the Cultural Attaché and the expert in Qatar culture
<p style="text-align: center;">E-Law</p> <p><u>There is lack of clear e-law to protect citizens from electronic crimes</u></p>	Interview with the Cultural Attaché
<p style="text-align: center;">Other Country-Specific Factors</p> <p><u>Qataris motivated by tribal, sectarian or partisan concerns since Qatari society has a tribal structure</u></p>	Interview with the Cultural Attaché and the expert in Qatar culture

Following the discussions with participants an interview was made with the London Qatari Cultural Attaché, who made a valuable input in confirming the findings. He also had seen phishing become popular in Qatar. However, he found responsible institutes are paying attention to protecting against phishing and enhancing public awareness. He pointed to the rapid development in Qatar in recent years, which has raised the profile of Qatar and therefore phishers found it an attractive place for them, especially in the absence of e-law. However, the e-law is near to reality which will assist in solving the problem of phishing in the State.

He added that since Qatar is a conservative country with its customs, traditions and culture, the culture therefore has a major effect on people's responses to phishing attacks. He added Qataris are vulnerable to phishing due to cultural, country-specific factors, religion, and personal interests and characteristics. He supported the factors which make Qataris vulnerable to phishing discovered by the researcher. In addition, he pointed out more factors as follows:

1. Motivation by tribal or sectarian or partisan concerns since the society has a tribal structure
2. Feeling of safety, especially that Qatar is a safe country
3. Love of adventure
4. Love of spreading good, e.g. spreading good ideas which can be used by phishers, which is called a pyramid system.
5. Belief that he/she has no enemies who want to hurt him/her
6. Lack of concern about the consequence of phishing, especially if you are not using your computer (e.g. work PC)

Phishers try to use all of these factors and exploit them to their advantage to persuade and trick their victims to fall prey to phishing. Since Qataris are emotional and Islam plays a big role in their life and in being good willed, religious topics are more persuasive, especially if it influences their emotions, especially in religious seasons such as Ramadan and in existing disasters. He pointed out that phishing attacks which exploit Qataris' emotions, morals and religion, especially in religious seasons and disasters, are more successful in Qatar. Adding, it is obvious that phishing emails with a religious theme do indeed occur in reality in Qatar. For example, he once received an e-mail requesting a charitable contribution for Palestine Muslims who were suffering and needing help from their brothers in Islam to survive.

Finally, he stated that Qatar, as other developing nations, is in the stage of development and since the development is rapid, people might not have absorbed this revolution and this will take time.

He added that although there is lack of awareness of the phishing threat due to the rapid revolution experienced in technology in Qatar, the government is working on assisting the society to absorb this revolution by enhancing their knowledge and improving the education curriculum. He predicted that the younger generation will be more aware. Furthermore, the country has a lot of money and it is valuable to invest in awareness because it is the best way to defend against phishing.

He noted that even experts in computer are not all aware of phishing attacks and he mentioned that he had fallen prey to e-mail phishing before, when he got wrong advice from a computer expert. He received an e-mail from an unknown sender requesting him to verify his MSN e-mail account or it would be blocked and a computer expert confirmed that this e-mail was legitimate. The phisher had then stolen his e-mail account and impersonated the Cultural Attaché, sending an e-mail to all contacts requesting help and money by using his name. He stated that he has now become more cautious about phishing because he had learned from that lesson.

Since Qatar is a safe and peaceful, this leads many Qataris to feel they are safe and to trust people. He added that there is more influence and trust in messages written in the native language (Arabic) than in English because using Arabic will be more understandable for victims, phishing e-mails are less common in Arabic than in English and, in some cases, Arabic will express the message more effectively, especially if it uses religious citations from the Holy Quran.

6.5 Collating the Results of All Tests

From the in-depth group discussions with participants in the experiment, interviews in the region and especially with the Cultural Attaché of Qatar in the UK, and observations from experiments in the region, it was recognised that Qatar has a tribal community structure. It is governed by customs and traditions and is tied to the Islamic religion which plays a major role in people's life. The culture of Qatar is affected by all of these factors. A representation of the multiple factors affecting Qataris' response to e-mail phishing as well as personal characteristics (e.g. greedy, careless) is given in Figure 6.8.

However, the personal characteristics or personality are also affected by the culture to a varied extent, depending on the individual.

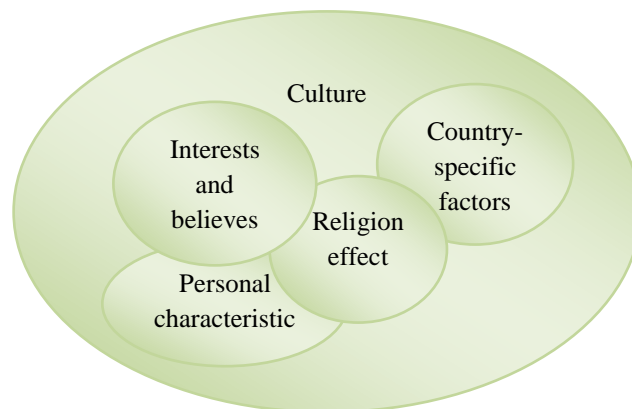


Figure 6.8: Why are Qataris vulnerable to phishing?

This only gives a general guide as it might be found that there are other factors or influences and overlaps that are not shown in the figure. In conclusion, there are many factors which make Qataris vulnerable to phishing as revealed in previous chapters and in the empirical work presented in this chapter. These factors are now presented in Tables 6.8 to 6.12. Each table corresponds to a different influence shown in Figure 6.8. Some factors occur in more than one table, reflecting the overlap between these broad categories of influencing factors.

In the tables the following column header abbreviations are used:

Sur: Survey

T1: Penetration test 1

T2: Penetration test 2

LE: Laboratory experiment test

IP: interview with participants

IE: interview with experts in the field

Table 6.8: Vulnerabilities of Qataris to Phishing Identified in this Research:**Culture Factors**

Why Qataris are vulnerable to phishing	Sur	T1	T2	LE	IP	IE
Embarrassment						
It is in the nature of Qataris to feel too embarrassed and stupid to mention or report that they have fallen prey to phishing.	✓				✓	✓
Friendliness and Courtesy to Others						
Qataris are friendly and like making friends and knowing people Qataris are courteous to other people, including strangers and even to extent of giving confidential information when asked.					✓	✓
Trusting Nature						
Qataris are trustful and not do not have bad faith in people, believing that others will be equally driven by religious and moral considerations Confidence and trust in friends gives phishing e-mail credibility if sent from a person they know. Qataris are more likely to be influenced by and trust e-mails in their native language (Arabic) They believe they have no enemies who want to hurt them					✓	✓
They believe in e-mails that exploit religion and people's generosity at times of natural disasters		✓	✓	✓	✓	✓
They trust official looking communications from trustworthy institutes in the society		✓	✓	✓	✓	
Curiosity and Temptation						
Qataris have a curiosity and seek out knowledge and discovery, especially in matters close to their interests. Qataris have a susceptibility to different kinds of incentives and temptations to satisfy their desires, needs and beliefs, such as magic, superstition, envy, horoscopes, astrology.	✓	✓	✓	✓	✓	✓
Qataris excitement over incentives and temptation can sometimes lead to circulation and exchange of phishing e-mails and sites among their contacts, which gives the phishing credibility Qataris love adventure					✓	✓

Table 6.9: Vulnerabilities of Qataris to Phishing Identified in this Research:**Country-specific Factors**

Why Qataris are vulnerable to phishing	Sur	T1	T2	LE	IP	IE
Lack of Knowledge of Phishing						
Many Qataris have not absorbed the rapid advances in technology in Qatar, this leads to: <ul style="list-style-type: none"> • Qataris lack knowledge of Internet threats and, in particular, phishing threats • Many do not expect to be phished • They believe they do not have anything worth stealing • Some do not know how to protect themselves against phishing attacks and how to detect and react to phishing 	✓	✓	✓	✓	✓	✓
Overconfidence in Technology and the Internet						
Some Qataris have overconfidence in technological tools, especially anti-virus software, for protecting against all kinds of phishing. Some have overconfidence in the technological revolution and believe that everything on the Internet is true.	✓				✓	✓
Trust in the Security of their Country						
They only expect phishing to be limited to certain topics or geographical areas – they feel safe in Qatar and therefore think phishing does not reach Qatar Qataris are more likely to be influenced by and trust e-mails in their native language (Arabic) They believe they have no enemies who want to hurt them					✓	✓
Lack of an E-Law						
There is a lack of clear e-law to protect citizens from electronic crimes						✓
Other						
Qataris are motivated by tribal, sectarian or partisan concerns since society has a tribal structure					✓	✓

Table 6.10: Vulnerabilities of Qataris to Phishing Identified in this Research:**Religious Factors**

Why Qataris are vulnerable to phishing	Sur	T1	T2	LE	IP	IE
Religion, Morality and Generosity						
Qataris are motivated by religious and moral considerations, being helpful, generous, emotional and good willed in their philanthropy, compassion and clemency, especially for people in need, in particular in the religious seasons, and when disasters and famines occur around the world.			✓	✓	✓	✓
Qataris have a love for spreading good, e.g. spreading good ideas, which can be used by phishers to distribute phishing e-mails					✓	✓
Trusting Nature						
Qataris are trustful and not do not have bad faith in people, believing that others will be equally driven by religious and moral considerations				✓	✓	✓
They believe in e-mails that exploit religion and people's generosity at times of natural disasters		✓	✓	✓	✓	✓

Table 6.11: Vulnerabilities of Qataris to Phishing Identified in this Research:**Interests and Beliefs**

Why Qataris are vulnerable to phishing	Sur	T1	T2	LE	IP	IE
Curiosity and Temptation						
Qataris have a curiosity and seek out knowledge and discovery, especially in matters close to their interests.		✓	✓	✓	✓	✓
Qataris have a susceptibility to different kinds of incentives and temptations to satisfy their desires, needs and beliefs, such as magic, superstition, envy, horoscopes, astrology.		✓	✓		✓	✓
Lack of Knowledge of Phishing						
They believe they do not have anything to be stolen or worth stealing					✓	
Trusting Nature						
They believe in e-mails that exploit religion and people's generosity at times of natural disasters They believe they have no enemies who want to hurt them					✓	✓

Table 6.12: Vulnerabilities of Qataris to Phishing Identified in this Research:**Personal Characteristics (two examples)**

Why Qataris are vulnerable to phishing	Sur	T1	T2	LE	IP	IE
Qataris can be overconfident in their own mind that they will not be tricked	✓				✓	✓
They have a lack of concern about the consequence of phishing, especially if it is not on their own computer (e.g. work PC)					✓	

6.6 Summary

Experiments demonstrate the need to enhance the state of awareness of e-mail phishing for Qataris. This is particularly shown by the 44% failure in detecting phishing by Qatari employees at AAB in the reality experiment, where it was found that they trusted e-mails from an unknown sender and were incapable of distinguishing phishing attacks, in particular phishing e-mails with attachments, which led them to be vulnerable to viruses.

Furthermore, in the penetration test with a sample of Qataris, more than half of the participants failed to detect phishing attempts, with a detection rate of about one in six e-mails. It was concluded that there are no specific criteria that can identify potential victims of phishing and even experts in computing are vulnerable, especially when the topic attracts their interest. There is clearly a lack of awareness of how to detect, react and protect against phishing. For example, some Qataris have overconfidence in the reliability of anti-virus software to detect all phishing attempts, and some do not install spam filters and open e-mails from unknown senders and junk mail.

In the experimental study, the detection rate for phishing e-mails was higher (64%) than penetration tests which reach 56% and 43% for tests 1 and 2, respectively. This is because all participants knew they were in an experiment and they may have considered it as a challenge and wanted to display their knowledge. In contrast, participants in test 1 were more aware of phishing threat than in test 2, because they were employees who use computers in their daily work.

The study shows the need to raise participants' level of detection to excellent (i.e. 100% of correct detections) since any wrong detection for legitimate or phishing e-mails might lead to huge consequences. Although the correct detections were higher than the wrong ones, not all participants took enough time to recognise phishing attempts by inspecting security indicators and some decisions were made by guessing. Some participants were more confused about making the right detection since they were more cautious than they needed to be, which led them to consider legitimate e-mails as

phishing. Discussions with the majority of experts and participants indicated that Qataris trust phishing e-mails in their native language rather than in English, they have overconfidence in official and trustworthy institutes in Qatar and they believe that phishing will be limited to certain topics and, especially, do not expect phishing in e-mails connected to religion.

The experiments have demonstrated that Qataris are vulnerable to e-mail phishing, in particular when it exploits their interest, emotions, beliefs and religion. According to the discussions with participants following experiment 2, this is especially true in the religious seasons or when there is a disaster, when religion sometimes even becomes a first priority over their interests. This shows they are more likely to become victims of phishing in the religious season than in other seasons. However, this still requires further investigation to prove it. Since Qataris are living in a conservative society committed to its culture, the response to e-mail phishing was discovered to be affected by the culture of Qatar which is influenced by the tribal community structure, customs, traditions and religion which play a big role in people's life. In conclusion, Qataris were found to be vulnerable to e-mail phishing attacks due to multiple factors: the culture, country-specific factors, religion, interest and beliefs, as well as personal characteristics.

This chapter identifies the need for awareness to enhance people's recognition of phishing attempts, and how to react and defend against them, and shows that any awareness programme needs to take into consideration the factors which make Qataris vulnerable to phishing.

The next chapter demonstrates the grounded theory applied to the development of an anti-phishing awareness framework as a means to reduce the risk of e-mail phishing in Qatar.

Chapter 7 Findings and Recommendations

Since much literature confirms the available phishing technological solutions cannot be relied on as it is hard to predict human behaviour, so many researchers turn to awareness as another line of defence. Awareness can be enhanced either through a set of recommendations, advice or best practices or through an educational awareness programme. In this research, the focus is on enhancing awareness of e-mail phishing by applying both recommendations and education and training as part of an overall awareness framework (see Chapter 2).

This chapter describes the grounded theory applied in this research based on gathering and analysing the findings from all previous phases of research to create an e-mail phishing awareness framework. This framework consists of set of recommendations produced for the Qatar government, for organisation officials responsible for ensuring information security and for Qatari citizens, and an effective educational framework of best practices to counteract the problem of e-mail phishing in Qatar. This chapter defines the recommendations part of the framework, the educational framework is discussed in the next chapters. These recommendations have been evaluated by experts to identify their potential effectiveness in reducing the e-mail phishing threat in Qatar.

7.1 Findings

The main contribution of this research is to propose an effective e-mail phishing awareness and educational framework to reduce the threat of e-mail phishing in Qatar society. This was identified using grounded theory based on findings from previous chapters (see Figure 7.1). A summary of the main outcomes from each chapter is given in Table 7.1.

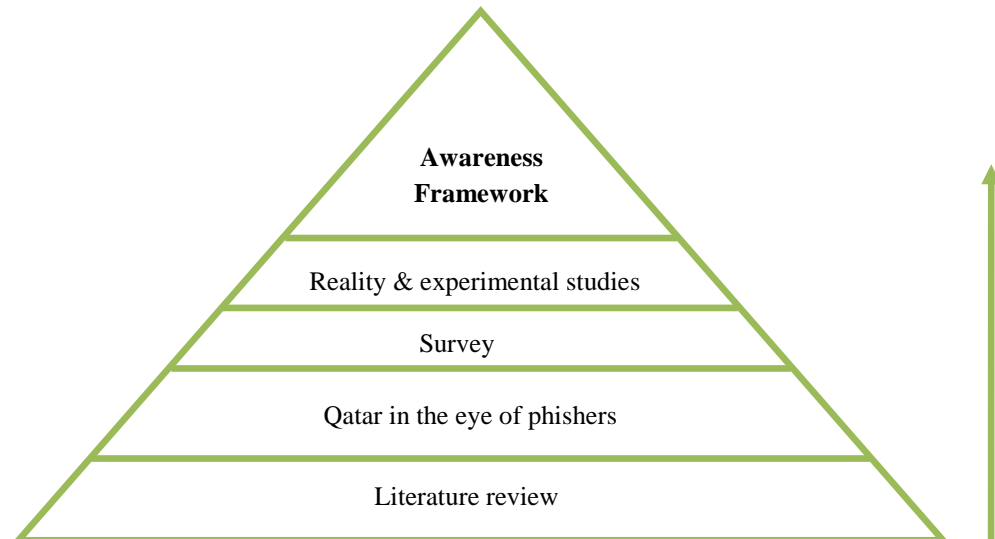


Figure 7.1: Grounded theory

All of the findings in Table 7.1 have clearly demonstrated that Qataris are vulnerable to e-mail phishing attempts due to many factors, many of which are cultural and country-specific. There is clearly a lack of awareness of e-mail phishing in Qatar and there is therefore a need to enhance Qataris' awareness. Consequently the need arises for an effective e-mail phishing awareness and educational framework based on a set of viable recommendations directed at the Qatar government, organisation officials responsible for ensuring information security in Qatar, and Qatari citizens. A set of recommendations were therefore identified for those target groups as given in the next sections.

Table 7.1: Main outcomes of the research

Chapters	Main Outcomes
Literature review (Chapter 2)	There is no research reported on phishing or any e-crime in Qatar. There are no statistics about phishing trends in Qatar
Qatar in the eye of phishers (Chapter 4)	<p>The E-mail phishing problem exists in Qatar and is becoming more common. There is a need to define a strategy of defence against phishing with major focus on enhancing awareness since technological solutions are unreliable against the smart tricks used by phishers to bypass these solutions. Various techniques of awareness such as e-learning, seminars, posters, SMS, e-mail and media, have been suggested with an emphasis on the latter and the idea of developing an anti-phishing game. Experts in education state that it is important to develop an effective, well planned and interesting awareness programme, as the majority of interviewees believed that Qataris are unaware of phishing which makes them vulnerable to such threat.</p> <p>There are many aspects which make Qatar attractive for phishers to commit their crimes: the rapid economic development, the growth of Internet users, the effect of culture and the lack of an e-law. The lack of an e-law was identified as one of the major problems organisations face in overcoming phishing attacks. In addition, culture was found to have an effect on people's falling prey to e-mail phishing attacks, especially when phishers exploit their kindness, goodness, trust, morals, emotions and religion.</p>
Surveys (Chapter 5)	The survey has shown. Qataris are generally vulnerable to e-mail phishing threat because of lack of awareness about phishing; they are even more vulnerable to phishing than UK citizens. Few know how to take the right actions and many do not report phishing because of cultural effects such as feelings of embarrassment and stupidity. They considered awareness to be the best defence against phishing and they prefer to be educated on phishing through web-based e-learning and media and other tools such as seminars, posters, interactive games and cartoons.
Penetration tests and laboratory experiment (Chapter 6)	<p>Many of Qataris are incapable of differentiating between phishing e-mails and legitimate ones as they did not take enough time to detect phishing attempts by inspecting security indicators and some decisions were even guesses. In the laboratory experiment, the detection rate for phishing e-mails was higher than in penetration tests, indicating that people are less cautious in reality. Experiments revealed that there are no specific criteria for being victims to phishing and even computer experts are vulnerable, mainly when it attracts their interest. There is an obvious lack of awareness on how to detect, react and protect against phishing. This shows the need for an awareness programme which makes people aware of the phishing threat without causing them to be too worried since this might also lead to wrong detections.</p> <p>Qataris are vulnerable to fall prey to e-mail phishing attacks due to multiple factors: the culture, country-specific factors, religion, interest and beliefs, as well as personal characteristics, which were discovered mainly in the experiments. Examples of aspects which make Qatari vulnerable are: lack of awareness, having overconfidence in the reliability of anti-viruses to detect all phishing attempts, overconfidence in e-mails that appear to be from official and trustworthy institutes in Qatar, trust of the native language and belief that phishers limit their use of certain topics, and certainly not religious ones. Also, they were found to be vulnerable to e-mail phishing which exploits their interests, emotions, beliefs and religion, especially in religious seasons.</p>

7.2 Recommendations

7.2.1 Recommendations for Qatar Government

1. Findings from previous chapters show clearly the need for enhancing people's awareness in Qatar. Although there are some existing awareness programmes on e-crime, there is a need to pay more attention to enhancing awareness of the phishing threat, since it is becoming more frequent and because of the rapid development in technology leaving people unable to absorb sufficiently the threats of the technology revolution. It is, therefore, recommended that there should be a greater focus on awareness to reduce the risk of phishing in Qatar. Effective awareness can be promoted through different instruments such as posters, videos, publications and especially the media in enhancing public awareness on such threats since they are popular in Qatar and trusted.
2. Interviews with experts in the field have revealed that there is no explicit e-law assigned in Qatar. Currently there is a fairly small section within the Penal Law No.11 of 2004 (Ministry of Public Prosecution, 2004) which covers computer crimes. This section does not cover all types of e-fraud that currently exist and it does not even criminalise phishing attacks (e.g. it does not criminalise viruses which are distributed over the Internet, by e-mail or even by a USB memory stick; it only criminalises viruses distributed through floppy disks and CDs). It is quite old for this type of law and has not been updated since its enactment in 2004. However, the government have recognised the need for a separate e-law and currently members from Q-CERT are working within a group led by ictQATAR to draft an electronic law for Qatar.

While the Qatari government's readiness to develop an e-law in Qatar is recognised, it is recommended that a comprehensive e-law should be developed to establish a framework and legislation to criminalise attackers, in particular phishers, to protect online consumers from possible electronic threats and to support actions taken in such cases (e.g. blocking phishing sites).

It is also recommended that the e-law should cope with Qatar-specific factors and culture (e.g. forbidding anti-Islamic items) equivalent to e-laws in developed countries, such as the UK's Data Protection Act of 1998 and Computer Misuse Act

of 1990, and in other neighbour nations, such as the UAE's e-law. By taking advantage of the experience of others, mistakes in the drafting of such laws can be avoided. In addition, compared to the current law, the new law should be more robust and adaptable to cater for the fast improvement in technology, by referring to general concepts, such as storage devices, instead of using specific technologies or brand names, such as Floppy disks.

3. Since interviews demonstrate that e-crimes usually come from abroad, it is recommended that the government works to build cooperation with the countries from which these crimes have been exported and to exchange information in this regard to reduce the risk of phishing attacks which originate from outside Qatar.
4. Currently, the computer crimes unit in the Ministry of Interior is responsible for researching and investigating reported e-crime, taking all actions required in cooperation with other organisations in Qatar and abroad such as blocking the phishing site, and also for providing a report of the case to the Ministry of Public Prosecution. However, it was discovered from interviews with the Ministry of Interior and the Public Prosecution that the latter finds difficulty in understanding most of the terms used in the Ministry of Interior's report which they largely depend on to decide whether to prosecute the accused or not.

Therefore, it is recommended that public prosecutors, justices and lawyers should be involved in educational sessions and courses to enhance their knowledge of e-crimes, so they can understand how to deal with such crimes, how to investigate them and how to enforce the law.

5. Since there is lack of research on e-crime in Qatar and on phishing in particular, it is recommended that a research centre on e-crimes is created to focus on identifying the factors which make such attacks successful in Qatar and investigating how to defend against such attacks, paying attention to the culture effects in Qatar.
6. Investigation shows that there are no tangible figures or statistics on the trend of phishing in Qatar and it is therefore recommended that a statistical database of e-crimes, particularly phishing attacks, is created to identify the extent of such threats to be used for research purposes. The Ministry of Interior are in the best

position to create such a database since reports of all e-crimes in Qatar are reported there.

7. It was discovered that many attackers and phishers in particular, use Qatar's iparks because it is hard to identify the attacker since the iparks are open to the public and are without any controls. Therefore, to reduce insider phishing attacks coming from iparks, it is recommended that access to the Internet at an ipark should require some kind of ID proof, such as a Visa card, ID number or a kind of registration process. For example, users could enter their phone number to receive an SMS with a password for free access to the Internet. Although people might complain about this procedure, it will help protect them and others from possible e-crimes.

7.2.2 Recommendations for organisation officials responsible for ensuring information security

1. Officials need to recognise that technological solutions can not be relied on to protect people against phishing and, therefore, awareness will act as another level of defence in parallel with technological solutions and policies. Therefore, it is recommended that an effective awareness programme on phishing threats is developed to enhance the defence level of employees or clients. The programme should use different techniques to raise awareness, such as e-learning, seminars, posters and SMS. The awareness programme has to be well planned and interesting, such as involving interactive quizzes or games which will bring fun to the training. It should make people aware of the phishing threat without causing them to be too worried since this might lead to wrong detection and rejection of legitimate e-mail communication. It is recommended that organisations have a security awareness team which works on developing awareness of threats facing the organisation from both inside and out, taking into account the national culture and the culture of the organisation itself. There should also be an evaluation process defined to evaluate the effectiveness of the programme, such as by holding anonymous penetration tests and carrying out surveys before and after the awareness programme is implemented.
2. Since it was established that people would learn more about phishing when they have encountered or have been tricked by such attacks, it is recommended that

e-mail phishing penetration tests are carried out to measure an organisation's vulnerabilities and to be part of a programme to enhance awareness on phishing. Due to legal and ethical issues associated with such an audit, it is recommended that an independent, approved and trusted organisation with experts in information security should carry out audits on request. This trusted organisation could be Q-CERT or any organisation specialised in information security similar to First Base Technologies in the UK. The trusted organisation would provide an important service of a reliable and confidential audit which would give a certification of the client organisation's defence level against phishing, including the level of awareness of phishing of their employees.

3. It is recommended that each organisation should study its own needs and set up some guidelines to help their employees in their defence against phishing. The guidelines must be clear and reasonable to follow, for example suggesting that employees do not open e-mails from an unknown sender. It is recommended that employees are motivated to follow the guidelines with incentive schemes offering certificates, awards, rewards and even promotion.
4. It is recommended that the e-mail server for the organisation should not allow employees or clients to send confidential information, particularly the username and password to access the organisation network, to anyone by e-mail. This safeguard exists in the Loughborough University e-mail system.
5. Interviews showed that only a few organisations have an incident management centre responsible for dealing with any incidents, such as a phishing attack, advising their clients/employees on how to react. Therefore, it is recommended that a team of experts should be formed to become an incident management centre to record incidents and provide effective advice. This will act as a measurement tool for the effectiveness of the organisational strategy of defence against phishing and it will also provide data for studying the pattern of phishing attacks to update and refine the defence strategy, the technological tools, policies and awareness.

7.2.3 Qatari Citizens

For Qatari citizens, recommendations are in the form of the following separate pieces of advice, mostly based on the factors revealed earlier which make Qataris vulnerable to e-mail phishing.

1. You should know that technological solutions are not 100% reliable to detect e-mail phishing attempts, especially since phishers use smart tricks to bypass them. There is no technology that can protect you fully from phishing. Your suspicion is your only friend.
2. You should make sure you know how to detect and react and protect yourself against phishing attacks.
3. You should make an effort to continuously update and improve your knowledge of phishing since reports of this kind of attack are becoming increasingly common in Qatar and elsewhere.
4. You should take the time to recognise phishing attempts by inspecting security indicators. So just be suspicious – all the time. Trust no machine.
5. You should recognise that there is no limit for topics used by phishers. They can exploit people through many different topics, even religious ones.
6. You should report phishing incidents without feeling embarrassed to help in reducing such threats.
7. You should not over-trust e-mails written in your native language (Arabic) as phishing e-mails can be written in any language. And look at the Arabic; is it good Arabic – as you would write it? In English, non-English ‘English’ can be easily spotted. The same applies in Arabic.
8. You should not have overconfidence in your own level of knowledge of phishing since this might lead you to fall prey to it.
9. You should not be too worried about phishing since this might lead to wrong decisions even on legitimate e-mails. You should always be cautious but not too worried.

10. You should not have overconfidence in the reliability of anti-virus software to detect all phishing attempts.
11. You should not have overconfidence in official and trustworthy institutes in Qatar because phishers could target them.
12. You should not be overconfident or too trusting about the information available on the Internet because not everything there is true.
13. You should not put too much trust in a known e-mail sender addresses because phishers could impersonate the trusted users. An e-mail return address may not be the real sender.
14. Be particularly careful about phishing e-mails that exploit your interests, emotions, beliefs and religion, especially in religious seasons and following disaster events.
15. If an offer seems very good, beware, temptation is a common trick used by phishers.
16. Don't be affected by incentives and disincentives that phishers could utilise.
17. Don't give away your e-mail address unless you are sure about the legitimacy of the people you are giving it to, even if they seem to be asking for it in a good cause, because it could be used to distribute phishing e-mails and give them credibility.
18. Don't over-trust official looking communications since phishers could misuse them to persuade you they are legitimate.
19. Don't let courtesy lead you to disclose your confidential or private information
20. Don't think phishing could not reach you, because there is no limited geographical area for phishing as it could reach any place around the world with a simple click. Although Qatar is a safe country, anyone using the Internet is vulnerable as the phishing attack may come from a different country.
21. Don't fall prey to phishing that plays on your religion, emotion and goodness. So if you receive a request from a charity you should check with the Ministry of Endowments and Islamic Affairs that it is a registered charity centre.

22. Don't over-trust or have good faith in people, especially those you don't know
23. Don't ever think you don't have anything to be stolen or worth stealing. Phishers may be just out to steal your identity
24. Don't forget that phishers attack thousands of people around the world, few of whom they will know, so even though you have no enemies you are still a possible target for phishing
25. Don't fall prey to phishing e-mails which have a tribal, sectarian or partisan appeal

7.3 Evaluation of Recommendations

To evaluate the proposed recommendations, the following 12 experts in the field of e-crimes and Qatar law and culture were asked for their opinions: (see Appendix D)

- An officer of the Computer Crimes Unit, Economic Crimes Prevention Division, General Admin. of Public Security Criminal Investigation Dept., Ministry of Interior, Qatar.
- A manager of the Public Relations Dept., Ministry of Interior.
- The Senior Incident Specialist, Incident Management, Q-CERT, Qatar.
- An Analyst, Critical Infrastructure Protection, Q-CERT, Qatar.
- A Public Awareness Manager, Q-CERT, Qatar.
- A manager of ISPs, Qtel, Qatar.
- The Head of Prosecution, Ministry of Public Prosecution, Qatar
- A judge at the Courts of Justice under the category of the Senior Civil Court Judges, The High Judicial Council, Department of Administrative & Financial Affairs, Qatar.
- The Computer Systems Administration course leader, Bradford University, UK.

- The Chief of Operations, First Base Technologies, leader in providing information security and testing services, UK
- The Cultural Attaché, Embassy of Qatar in the UK
- A researcher in Qatar culture, Ministry of Culture, Arts and Heritage
- The Managing Director of HandShaikh Ltd., UK, which provides cross-cultural seminars and consultancy for business with Arabs. He is also a researcher in Gulf culture and author of the book *Don't they know it's Friday?*.

The Cultural Attaché of Qatar and the Managing Director of HandShaikh Ltd were asked to evaluate only recommendations for Qatari citizens since they are experts in Qatar culture. Since the Chief of Operations of First Base Technologies is not part of the Qatar government, he was not involved in the evaluation of Qatar government recommendations. The remainder of the mentioned experts participated in the evaluation of all three sets of the proposed recommendations.

In addition, to involve Qatari citizens in the evaluation, a convenience sample of 30 Qatari e-mail users above the age of 12 were selected from a cross section of the researchers friends, colleagues and relations to assess people's acceptability of the recommendations and to feedback.

The following recommendations were considered:

- The proposals assigned for Qatari citizens (see Section 7.2.3)
- The need for implementing an awareness programme by government and organisation officials responsible for ensuring information security to enhance public awareness of the phishing threat.
- The provision of a kind of identity verification, such as a visa card, ID number in some form of registration process before accessing the free Internet in iparks.

- The carrying out of e-mail phishing penetration tests to measure an organisation's vulnerabilities to such threat.
- The setting up of some clear and reasonable guidelines to help in defending against phishing, bearing in mind that employers should be motivating their employees without intimidating them to follow such guidelines.
- The addition of a level of security on an e-mail account which would not allow an e-mail user to send their confidential information (e.g. username and password) to anyone over the e-mail.

Semi-structured interviews were held with the above evaluators. All were first shown the recommendations, and then face-to-face individual discussions were held to evaluate the recommendations according to their effectiveness, feasibility and ease of implementation. The following questions were asked:

1. Overall, are the recommendations useful and do you think they will help in reducing the risk of e-mail phishing in Qatar? Why?
2. Are they feasible? Why?
3. Are there any difficulties that might be experienced if they were implemented (e.g. in cost or resources)?
4. Do you have any further suggestions or comments?

7.3.1 Recommendations for Government

Both experts and public evaluators believed that generally the recommendations were potentially extremely effective and, if they were implemented successfully, they would certainly help in reducing the risk of e-mail phishing in the state of Qatar as they are well defined and based on research carried out in the region.

The experts in the law and e-crime from the Ministry of Interior, Q-CERT and Qtel believed all recommendations to be valuable, especially because they cover different

target groups, they were clear and were derived from a research base. They added that Qatar e-law is on the way to reality and the Q-CERT team is involved in co-operation with associated organisations including ITU (International Telecommunication Union), Ministry of Interior, Ministry of Public Prosecution, High Judicial Council and others. It is important to consider the dependability and adaptability of the law, especially with the fast improvement in technology. The new e-law has taken into consideration experience of other countries in e-law. Basically, it is a combination of e-law of Australia, America, UK, UAE and Saudi Arabia, customised to be unique for the state of Qatar.

The experts agreed that building an e-law from scratch would be time-consuming and prone to error, and therefore it is worthwhile to learn from others' experiences in e-law. In addition, they stated that the effectiveness of the e-law would be known only after the law comes into practice, but this could be achieved with co-operation from all sectors, including governmental and private organisations and Qatari citizens. The experts agreed it would be important to announce and publicise the implementation of the law and make it an open source to the public. The law could be improved regularly once it is implemented. They expected that the new e-law would deter people with malicious intent who attempt to deceive and exploit others through electronic telecommunication, especially phishers. However, the Head of Prosecution and Justice suggested that although the new law would definitely provide a framework for Qatari citizens, it would be difficult to implement, especially for crimes committed from other countries, such as Nigeria, where it is hard to reach the phisher and punish them even if there is co-operation, since there is no stability in the country. Therefore, the experts suggested that it would be better to make people aware of the threat and be cautious with e-mails from those countries, and to wait a while until these countries become more stable and before Qatar tries to build strong co-operation.

With regard to the need for public prosecution, the experts agreed that judges and lawyers will need to enhance their knowledge on how to deal with e-crimes and how to understand and implement the new e-law, but they suggested it should be an optional

course for those interested in becoming experts in e-crime. It would be sufficient to have a team of experts in e-crime and then refer all e-crime cases to them.

Most of the experts believed there is a need for a research centre on e-crime in Qatar, especially now that Qatar is investing in education and research and there is a huge revolution in technology. However, they noted that although establishing such a centre is feasible, it would require huge resources from experts in the field, money and tools. However, they believed it would be possible with support from the government and other institutes, especially educational institutes, and the support would grow with the reputation of the centre.

The experts argued about the implementation of a phishing database in practice. Half of the experts suggested that although keeping a record of phishing incidents on a database seems to be an easy step, most organisations do not do it. It is part of the Qatari culture that people do not want to report, they just want to react and solve the problem, believing anything more is a waste of paper and time. Moreover, the experts in Q-CERT commented that there are databases that already exist, such as Q-CERT's incident database. However, the records are not gathered into a single database, so they agreed that once all incidents are gathered into a single database and classified, this could be used for further research. The experts in Qatar culture agreed on the need for such a database, pointing out that Qataris usually prefer to react to incidents rather than reporting and documenting things. However, some experts still had doubts about creating a statistical database of every single e-crime incident, suggesting it would be unrealistic in daily operation even though this might be beneficial for a research base. Experts from the Ministry of Interior added that such a database required sufficient resources, including a team of experts working on gathering all incidents, classifying them and reporting them.

The majority of Qatari citizens and experts pointed out the need for an effective awareness framework to enhance public awareness of the phishing threat, especially through the media. However, the public relations experts from the Ministry of Interior and Q-CERT mentioned the difficulties of acquiring resources for such a programme

and gaining cooperation from the many institutes in Qatar (e.g. educational institutes, media and governmental organisations) needed to facilitate a successful awareness programme.

Regarding the iparks, the experts agreed that as the iparks are currently not monitored, they have become the source of many e-crimes inside Qatar since there is no method of tracing the user. They agreed that adding a kind of registration process to prove the identity of the user would be a valuable solution. They agreed the SMS registration would be a good idea since a lot of Qatari citizens have mobile phones, even children, and all mobile phones in Qatar are registered, making it easy to trace the user in cases of Internet misuse. Q-tel pointed out that using an SMS service is becoming common in Qatar; it already exists in the Ministry of Interior and in many banks and institutes. People would therefore accept it, it would not be difficult to implement and it would be reliable as SMS messages would be received within seconds for the user since there is no difficulty with mobile signals in any of the iparks.

The provision for such service should come from Q-CERT since ipark is one of their projects. Also, there should be a co-operation with telecommunication service providers since they have control over telecommunication channels in Qatar, including Internet and mobile phones. Q-CERT agreed that this recommendation is feasible but it would require a lot of resources and cooperation with Internet service providers. They pointed out that there would be the need to provide a unique username and password for each registered user which would expire immediately when the user disconnected from the Internet. It was agreed that although this might be annoying for people to have a different login each time it was used, it would be safer, since it would ensure the identity of the user is known each time. There would be a risk that mobile phones could be stolen and used by phishers for this purpose, but as there is no 100% solution, the user would have to immediately report any such loss so that the SIM card could be blocked.

Generally, most of the Qatari citizens thought that adding registration would be valuable and necessary but it might not be accessible for people who do not have mobile phones. More than 70% of evaluators claimed that they would still use the ipark even if registration is required, because they are used to SMS services, and they found it fast and effective, especially with their experience with SMS banking services where, within a few seconds of performing any transactions on their bank account, they receive an SMS to verify the transactions. In contrast, less than 10% of evaluators disagreed believing that adding a registration might make the use of the ipark too complicated for the user.

Finally, some of the experts highlighted the need to motivate the government to accept the proposed recommendations and approve their implementation without delay so that these recommendations could be effective in reducing the risk of phishing in the State of Qatar.

7.3.2 Organisation recommendations

All of the experts found all the recommendations for organisations valuable, although they thought it might be feasible only if there is sufficient budget for the organisation to fund the approach. Funding and resources were considered to be the largest obstacle to implementation, especially for providing an incident management centre. Although the experts agreed that such a centre is essential, they thought many organisations would be reluctant to spend a lot on it. They considered it likely that organisations would only react once an incident had happened, usually referring to responsible organisations to perform the required actions, such as the Ministry of Interior and the banks, because they are trusted and are experts in dealing with such cases.

The experts from Q-CERT, Q-tel, the Ministry of Public Prosecution and the Ministry of Interior stated that within the organisation there should be an incident management centre which would report, react and work on the incidents, but still there is no shame in requiring help from responsible organisations such as Q-CERT and the Ministry of Interior. The expert in computer crime from the Ministry of Interior stated that if each

organisation had an incident management centre, the Ministry's duty would be simplified since the centre would know with whom to interact and this would help the Ministry to further investigate the case. These experts confirmed that they thought many organisations would be reluctant to spend enough money to provide an incident management centre or a good quality education and awareness programme.

All of interviewees stated that their organisations did not use penetration tests to measure employees' vulnerability to possible threats such as phishing because of legal and ethical issues. However, a few (under 10%) pointed to the importance of planning and measuring the extent of the problem by holding such phishing penetration tests to assess the current strategy of defence and to work to improve it. Nevertheless, some of the experts stated that penetration tests would be possible if they were carried out by a trusted organisation, such as Q-CERT. They noted that the need for penetration tests would depend on the organisation size and information held. For example, the ministries hold sensitive information so it would be essential to perform such tests regularly, whereas other organisations may not necessarily require any tests.

The experts agreed that a certificate to say that an organisation has been audited by penetration testing and has passed to a high level of defence against phishing would be very useful. However, the certificate would need to be approved nationally and internationally for credibility, as this would motivate organisations to do such an audit. In contrast, over half of the Qatari citizens interviewed disagreed with holding penetration tests because it would be annoying, create distrust in an organisation and they do not like to be watched and audited regularly since this might negatively influence their work performance. As a result of this evaluation, an extra recommendation was added that organisations should explain to employees the importance of such an audit and of having an approved defence certificate.

With regard to the need for defining understandable and reasonable guidelines to avoid phishing, both experts and citizens thought these were important. However, they

mentioned that some employers go too far and define guidelines that are unreasonable and difficult to follow. For example, some organisations require a compulsory reset for their network password every three months which, although it is more secure, employees find difficulties in remembering and this leads them sometimes to write it on a sticky note in front of their desks. This therefore makes them vulnerable to social engineering attacks. As a result of this feedback, a further recommendation was made that organisations need to understand that there is a potential threat from setting up unreasonable guidelines and that they need to assess the feasibility of the guidelines to make sure all of them are short and understandable and are presented clearly to employees. Most of the interviewed citizens suggested that the recommendations should include motivating employees to follow such guidelines, although few organisations in Qatar currently have any culture of motivating employees whether by financial or any other means.

With regard to adding a security level to an e-mail account which will not allow the user to send confidential information (e.g. username and password) to anyone by e-mail, the majority of interviewees thought it was a valuable and feasible suggestion. The experts agreed that it is technically feasible and organisations would find it a safeguard feature. However, some citizens disagreed and stated that they sometimes send their log-in details to their trusted families or friends. Despite this dissent, it was decided that this recommendation should remain, as it is safer not to trust anyone, since everyone is responsible for any negative action performed from their computer or their account.

7.3.3 Qatari citizens' recommendations

Most evaluators found the recommendations were useful to help reduce the risks from phishing but they felt there may be too many points for the average person to consume. They suggested consolidating some points to make the list shorter. Some suggested that a piece of advice that contains the threat should also contain the cure. So there is a need to tell Qatari citizens what they should do. Otherwise, you're only sending a scare that might drive people away from using technology. Therefore, they suggested re-wording the recommendations into positive things to do because people are reluctant to follow

negative recommendations. However, around 80% thought that the recommendations were well defined since they covered poor practices followed in their own daily on-line activities.

Some of the experts stated that some of the recommendations were not illustrated sufficiently, such as the reason why technological solutions are not 100% reliable in detecting e-mail phishing attempts and how official institutes could be phished. Also, the recommendations should suggest how to detect, react and protect oneself against phishing attacks, how one should continuously improve one's knowledge of phishing and how to inspect security indicators. Most experts noted that the recommendations were understandable but it would also be valuable to include some real examples, perhaps with screenshots, to help illustrate the points made.

In response to the researcher's explanation that the suggested recommendations were based on the discovered factors which make Qataris vulnerable to phishing, including the cultural aspects, the experts in Qatar culture agreed that the culture plays a huge role in making Qataris vulnerable to phishing, especially that Qataris are generally trustful, generous and helpful. Also, the experts warned there may be difficulties in presenting recommendations to Qatari citizens which may require approval from government or other organisations. Also, it would be difficult to measure the effectiveness of the recommendations in reducing the e-mail phishing problem in Qatar in reality.

In addition, the Cultural Attaché of Qatar in the UK, stated that there is a difficulty in resolving phishing problems in Qatar because Qataris prefer not to think about the problem until they face it themselves, i.e. they are re-active rather than pro-active.

7.3.3.1 Revised Recommendations for Qatari citizens

Generally, there were no changes made for Government and organisational recommendations which all evaluators endorsed. As a result of the feedback from the experts and the sample of citizens, the recommendations for citizens were modified to make them more understandable and fewer in number as follows:

1. You should know that technological solutions are not 100% reliable to detect e-mail phishing attempts, especially since phishers use smart tricks to bypass them.

You should know how to detect, react and protect yourself against phishing attacks. In addition, you should not have overconfidence in your own level of knowledge of phishing since this might lead you to become a victim. You need to continuously improve your knowledge of phishing and, to help in reducing such threats, you must report phishing incidents without feeling embarrassed. You will find a lot of information and tips on phishing online from United States Federal Trade Commission (FTC), SCAMwatch which is run by the Australian Competition & Consumer Commission (ACCC), Anti-phishing.info and Anti-Phishing Working Group (APWG). Just be suspicious – all the time. Trust no machine.

How to avoid phishing?

- Install antivirus software and spam filters and keep them up-to-date (e.g. the Firefox and Microsoft Internet Explorer (IE7) phishing filters)
- Do not trust offers that seem too good to be true. Phishers usually trick people by conveying a sense of urgency, surprise, exploiting their goodness and interest. Also they usually employ official mail; however, look at the language as they tend to make spelling and grammatical mistakes.
- Do not open an e-mail classified as junk mail unless you trust it.
- Do not download an attachment from an unknown sender, it may contain viruses.
- Be suspicious about e-mails that ask for private or confidential information
- Spend enough time to recognise phishing attempts by inspecting security indicators. This is done by first inspecting the URL of the site to see whether it is an unprotected web page (the URL begins with http) or it is protected with SSL/TLS (begins with https), then the padlock icon to see whether it is locked (protected with SSL/TLS) or unlocked (unprotected with SSL/TLS) and finally the legitimacy of the security certificate. This can be accessed by double clicking on the padlock where

you must then ensure that the certificate is valid and issued for the entitled site by a trusted certificate authority (CA) such as VeriSign and Thawte.

- Consider security alerts appearing from your operating system, anti-virus, Internet browser and spam filters.
- Finally, do not respond to suspicious mails

How to react on being phished?

To reduce the possible negative impacts from phishing, you must follow the following remedial actions once you fall victim to phishing:

- Report incidents to the Ministry of Interior, your bank or to Q-CERT which is a responsible organisation dealing with Internet crimes in Qatar
- Check your financial statements immediately
- Cancel your credit and debit cards
- Change the account details you have been disclosing
- If your PC was infected, run a virus check
- Finally, it is recommended that you share your experience and make others aware.

You should recognise that there is no limit for language or topics or geographical area for phishers, they can exploit people through different topics, even religious ones, written in any language, even Arabic, so do not think phishers could not reach you. They attack people around the world, so even though you have no enemies you are still a possible target for phishing.

2. You should not over-trust e-mails which appear to be official communications from known and trusted addresses because phishers could steal their identities and impersonate the real users to commit their crimes. So you should not have overconfidence in e-mails that appear to come from official and trustworthy

institutes in Qatar. Remember that not all information available on the Internet is true.

3. Do not fall to temptation or incentives from e-mails that exploit your tribal, sectarian interests, emotions, good will, beliefs and religion, especially in religious seasons and following disaster events. For example, if you receive a request from a charity you should check with the Ministry of Endowments and Islamic Affairs that it is a registered charity centre and if you receive an e-mail requesting help, taking advantage of your tribal loyalties.
4. There is no need to be too courteous. Just because the sender seems friendly, you are not obliged to reply. The sender may be being friendly just to tempt you. Don't over-trust or have good faith in people you don't know.
5. Don't forward e-mails if you are not sure about their legitimacy even if they seem to be aimed at spreading goodwill because this could help in distributing phishing e-mails and give them credibility.
6. Don't ever think you don't have anything worth stealing, even a few small coins or simple information such as your name is worthwhile for phishers.
7. You should not be too cautious or worried about phishing since this might lead to wrong decisions, even on legitimate e-mails. Don't think every e-mail from an unknown sender is phishing, it could be legitimate and safe.

7.4 Summary

This chapter presented the recommendations for the Qatar government; for organisation officials responsible for ensuring information security and for Qatari citizens to diminish the e-mail phishing threat in Qatar. The recommendations were derived from grounded theory based on findings from the research carried out in the field. The proposed recommendations were evaluated by a sample of Qatari citizens and experts from Qatar and the UK in the fields of e-crime, Qatar law and culture. They concluded that the recommendations were potentially very effective and would help in reducing

the risk of e-mail phishing in the State of Qatar if implemented successfully since they are based on sound research.

With regard to the recommendations for a Qatar e-law, the experts stated that this initiative is already under way with the team from Q-CERT working in co-operation with associated organisations nationally and internationally. The law has taken into consideration the experience of other countries in e-law, dependability and constant improvement and is to be available to the public. More than half of the interviewees pointed to the need for having a team of experts in e-crime involving public prosecution, justices and lawyers. Since Qatar is investing in education and research, they should consider the possibility of creating an e-crime research centre.

The common obstacle to implementing most of the recommendations for government would be the need for resources of money, staff and tools and support from government and other institutes. In addition, as Qatari citizens tend to react to incidents rather than reporting and documenting them, this has led to the difficulties in building a record of phishing incidents within any organisation. The Ministry of Interior supported the concept of keeping a record of incidents but pointed out the need for a team of experts working on gathering all incidents to classify and analyse them to produce reports on the extent of the problem.

All of the experts and most, though not all, of the citizens agreed there is a need for an effective awareness framework to enhance public awareness of the phishing threat in Qatar, especially through the media. Regarding the ipark, both experts and citizens agreed that adding a registration process to prove the identity of the user would be a valuable solution and that SMS registration would be very effective, although it might not be accessible for people who do not have mobile phones.

The experts thought all recommendations for organisation officials were valuable but some suggested that many organisations would be reluctant to support the spending to provide an incident management centre, a measurement tool to measure employees' vulnerability to phishing and an education and awareness programme. In addition, there were conflicting views regarding the phishing penetration test. Some thought it would be beneficial to assess the effectiveness of the organisational strategy of defence against phishing, while others disagreed because of legal and ethical issues, the distrust that may be created and the negative influence on employees' work performance.

There were also conflicting views on the provision of strict guidelines, with employers believing this will enhance their security level, whereas others thought it might be unrealistic. Even where the guidelines are strictly enforced, employees may still find ways to bypass them and this could potentially make them vulnerable to other attacks such as those of social engineering. Therefore an organisation should consider the importance of motivation to inspire their employees to cooperate.

With regard to the recommendations defined for Qatari citizens, most evaluators agreed they were useful since they are based on the factors which make Qataris vulnerable to phishing. However, there were too many and some were not explained adequately. Therefore, the recommendations were simplified and clarified to take into considerations the evaluators' feedback.

In conclusion, the recommendations were thought by a sample of experts and Qatari citizens to be potentially effective for reducing the risk of e-mail phishing attacks in the State of Qatar. However, some obstacles were identified that might be faced when implementing the recommendations and these should be considered and planned for when putting the recommendations into practice. However, it is of some concern whether the recommendations would actually be effective when implemented. The researcher is unable to implement all of the recommendations into reality since this would require many resources and the approval of government and many institutes in Qatar. Some experts identified the need to motivate the government and target groups to acknowledge the proposed recommendations and implement them to reduce the risk of

phishing in the State of Qatar. The limitations of time and resources for this research and the need for approval at many levels means it will not be possible to evaluate all of the proposed recommendations. However, the recommendation for implementation of an effective e-mail phishing awareness programme could be evaluated by implementing aspects of the suggested programme to show that awareness could help in reducing phishing risk in Qatar. Research outcomes through all phases have illustrated the need for developing an anti-phishing awareness and educational framework for the State of Qatar to help reduce the e-mail phishing threat.

The next chapter describes the development of a comprehensive and interesting e-mail phishing awareness framework, along with the evaluation of its effectiveness in enhancing people's knowledge and defence level against the phishing threat. The framework is designed to be suitable for all Qatari citizens and has taken account of the findings of previous research (see Chapter 2) with regard to awareness, such as considering participants' background, not intimidating people and the factors which make Qataris vulnerable to phishing.

Chapter 8 An Educational Programme for Phishing Awareness

Many research papers support the need for education and training on the phishing threat to improve online users' defence against phishing and therefore reduce the effect of phishing through awareness (see Section 2.5.2.2). It can be concluded from the literature that there are different educational and training methods which apply learning principles which have been shown to be effective in improving users' abilities to detect phishing attempts. The literature review suggests that a comprehensive e-mail phishing educational framework should involve embedded training, contextual training, learning programmes and e-learning. Development of such a framework has taken account of this. Accordingly, training materials are presented in different forms including a game, quizzes, posters, presentations, cartoons and through the media to provide effective education against phishing threat. The developed awareness framework includes different training techniques as shown in Figure 8.1.

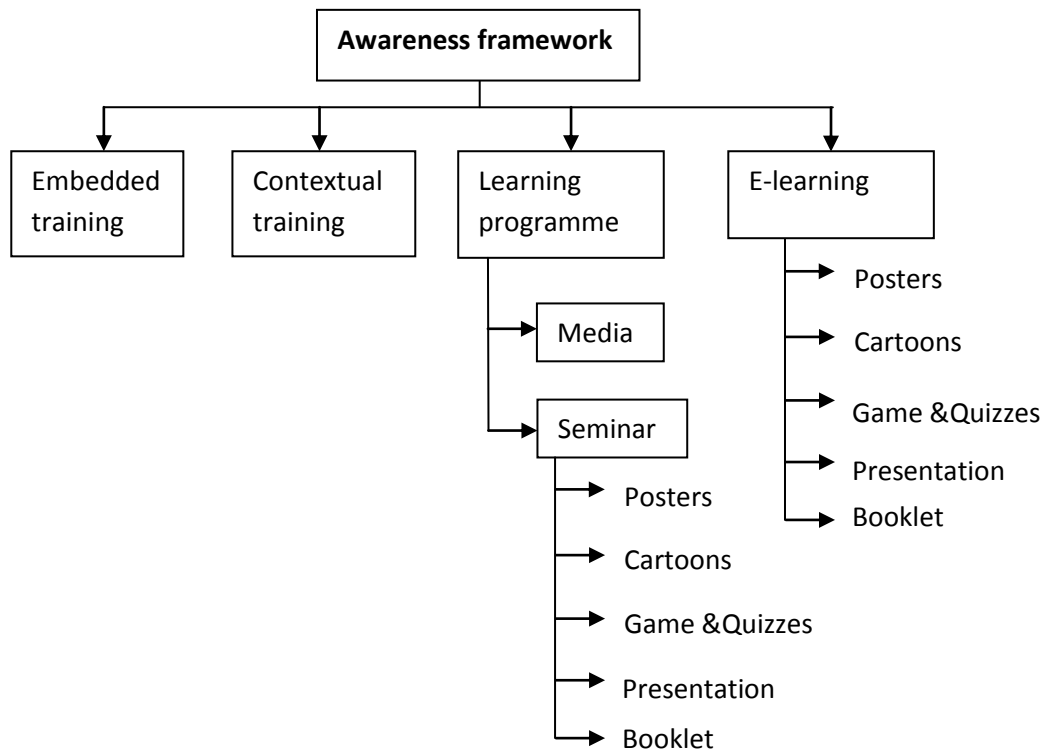


Figure 8. 1: Awareness framework

This chapter describes the development of an effective educational learning programme on e-mail phishing to enhance people's awareness and thereby reduce the problem. Learning programmes could be executed widely through media or locally through learning sessions and can involve multiple educational components including posters, leaflets, cartoons, quizzes, games and giving presentations (see Section 2.5.2.2).

A programme session for Qatar was developed to make its citizens aware of the e-mail phishing threat and how to recognise, react and protect themselves against it. Different learning tools (e.g. posters, game, quizzes and cartoons) are suggested to create an interesting and enjoyable educational session based on established learning principles, without intimidating the participants, and taking into account the factors which make Qataris particularly vulnerable to phishing.

8.1 Development of an Educational Programme

It was decided to develop a two-fold, anti-phishing, learning programme, presented as learning sessions and e-learning, involving different learning tools such as posters and quizzes and also as a TV programme. The author was motivated to use the media to enhance public awareness on phishing since many researchers have proved the influence of media awareness on people's behaviours and on increasing their knowledge on many issues (Goddard and Saunders, 2001; Levy, 1999; Krugman, 1996; Andrews, McLeese and Currant, 1995: 929-930; Burrows, 1988). In addition, this research applies effective methods in the e-mail phishing learning sessions along with e-learning, benefiting from tutorials and training found in the literature and the information they involve. The different learning tools in the e-learning and learning session are: scenario-based cartoon posters, cartoons, presentation slides, quizzes and an anti-phishing game for testing the effectiveness of each part of the learning tools. The educational tools were also assembled as an e-learning website to provide flexibility of learning and to facilitate the evaluation process for the learning session. The components of the anti-phishing programme passed through a development phase and were then put into a programme session and e-learning site to assess the effectiveness of each component. In

addition, the use of media, in particular a TV show on the danger of phishing, was tried and evaluated.

In the development phase of the learning programme, two experts in awareness were met individually: the public awareness manager in Q-CERT and the manager of the Public Relations department in the Ministry of Interior. Those experts are responsible for enhancing public awareness in Qatar and discussions with them were aimed at building a learning programme. It was concluded that such a programme should be simple, understandable, attractive and interesting. In addition, it should cover all the topics required about e-mail phishing without being too long (e.g. what e-mail phishing is, its impact, how to react, recognise and protect against phishing, in simple guidelines that are understandable and easy to follow). They supported the need for different tools (e.g. game, poster, cartoon, etc.) for developing awareness and in both Arabic and English, since Qatar is a multi-ethnic country. Furthermore, they agreed on the need to make people aware of phishing without intimidating them and to take account of people's background and the factors which make Qataris vulnerable to phishing.

The manager of the Ministry Public Relations department particularly emphasised the need to provide a framework associated with Qatar using the media and posters for enhancing public awareness. On the other hand, the expert from Q-CERT put more emphasis on the effectiveness of training sessions, applying the training in an interesting way to teach the principles involved.

8.1.1 Poster Development

To test the effectiveness and discover the advantages and disadvantages of using posters as a means of creating awareness, three posters were developed.

Poster 1: Be aware of phishing

The first poster was intended to be an attractive poster which demonstrates effectively the dangers of phishing through a visual image that is easily understood, with a simple description of phishing underneath. Since ‘phishing’ sounds the same as ‘fishing’, this suggested the concept of phishing for potential victims as a shark that preys on small fishes. Therefore, there was a need to either capture a picture of the moment where the shark is attacking its prey or to use an existing picture. Due to the difficulties in obtaining such a picture, an existing one was used and, after a search, it was decided to use a picture from the well known 3D cartoon film, *Finding Nemo*. The image has the copyright of Walt Disney in the USA, so permission was sought from Walt Disney to use the image and this was granted for use in this research project. The Photoshop application was used to create a scary atmosphere by adding an abandoned ship.

The poster reflects the conflict between good and evil and demonstrates the risk of phishing, where phishers tempt their victims into troubled waters to attain their goal. The predator shark symbolises the phisher who hunts for victims, depicted as the two small fishes on the poster, one of which is the well-known cartoon fish ‘Nemo’, which were led into a terrifying place in the ocean with an abandoned ship. This symbolises the seriousness of the consequences of phishing attacks and also the need for awareness. There is a common saying in Arabic ‘If you are not a wolf, the wolves will attack you’, which means there is a need to be aware and cautious. The poster was entitled *Be aware of phishing* and it contains a profile sentence about phishing: *Phishing with a ‘Ph’ is an attack which seeks to trick people in order to gain their confidential or private information for promised goods, services, money and more* (see Figure 8.2). Although the poster uses the well-known characters of the *Nemo* film, discussions with the experts confirmed that while it is attractive and reflects its purpose, it is not unique to Qatar and does not contain sufficient details of phishing, its techniques and how to protect against it. Therefore, a second poster was developed, containing more information and a greater association with Qatar.



Figure 8.2: Poster 1- Be aware of phishing

Poster 2: Let's make phishing disappear!

The second poster *Let's make phishing disappear!* introduces the term 'phishing' and gives recommendations on how to avoid it. In addition, it demonstrates that phishers use many tricks to attain their goal by showing three examples of phishing e-mails, each using different techniques. E-mail 1 works on people's emotion and religion with an apparent request from a charity fund to download an attachment in the e-mail which

might contain viruses. E-mail 2 uses the format of an official communication, conveying a sense of urgency, intimidating the victim with the threat of shutting down all unused accounts and demanding that the victim verifies his/her hotmail account in a fake website. E-mail 3 uses a sense of surprise and the format of an official communication, asking for a reply to gain a lottery prize of £600,000. To make this poster unique to Qatar, the researcher has used a character well-known to Qataris, the awareness officer 'Naseh' who reflects the culture of Qatar in the traditional dress of a Qatari policeman (see Figure 8.3). Copyright clearance for using the character was obtained from the Public Relations department of the Qatar Ministry of Interior which uses Naseh for promoting traffic awareness (see Appendix E). Therefore, Naseh is used as a trusted symbol for Qataris to make them aware of the phishing threat. In addition, the background of the poster contains some Islamic inscriptions in a maroon colour which links to the white and maroon of the Qatar flag. The experts favoured this poster because they believed it contains more information about phishing in a way associated with Qatar and makes people aware without intimidating them, whereas the previous poster was more terrifying rather than helping to create awareness. However, young people who were interviewed after they took part in the awareness session (described later in this chapter) took the opposite view and found it less attractive.

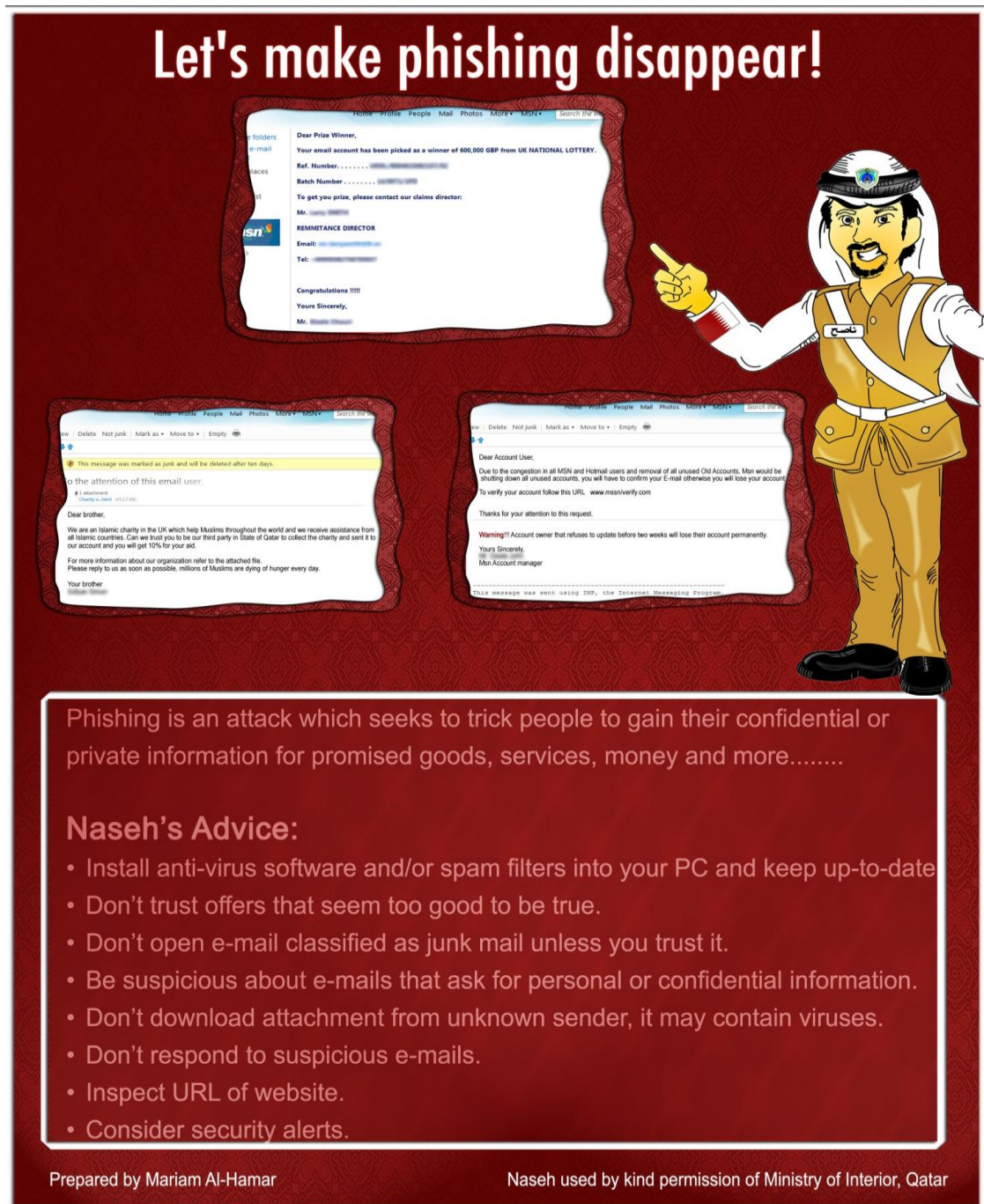


Figure 8.3: Poster 2- Let's make phishing disappear!

Poster 3: Story board

This poster provides a story board which makes people aware of phishing through the scenario of an interesting story. It takes the best idea from the two previous ones: the memorable cartoon with well known characters and a more informative poster

associated with Qataris. The main characters of the story board are from the *Freej* cartoon, which is the Middle East's first ever and much loved 3D animated TV series, which presents the Gulf culture, thus making the storyboard interesting, attractive and unique. Permission to use the *Freej* characters was granted by Lammtara, the official creators of the *Freej* cartoon.

Freej is produced in the UAE (United Arab Emirates) by Mohammed Saeed Harib (Saffarini, 2006) and is centred on four elderly Emirati women trying to live a peaceful life in a secluded neighbourhood in the midst of the ever-expanding modern day city around them. The show's main characters and the booming city unveil new social issues every day that they would have to tackle and solve in their own simple way. The *Freej* official website is available at <http://www.freej.ae/>. Since the poster uses the *Freej* cartoon, the target group for this story board were the people who watch it, a wide range of the population including children and adults.

The story board looks attractive and was entitled *Phishing in Freej*. It has illustrated different types of phishing attacks by showing that phishing can come through different communication channels: e-mail, mail, phone and others. Also it shows the tricks phishers use against their victims such as exploiting their interest and how victims react once they receive such an attack by giving an example of an aware and unaware victim and, finally, it gives some tips to avoid the phishing threat (see Figure 8.4). All of the posters had versions in both English and Arabic in order to be understood by a large number of Qatari citizens. For the Arabic version of the posters, see Appendix E, pp. 418-420.

Raising Awareness of Phishing

AGHA AKBAR ASGHAR GROCERY

I need some money, mmm.... Why not phish someone today?

It's so easy, let's trick them. You've won 1 M QR in a raffle; your money is ready to be paid to you. Just phone this number 555... Now I'll send it.... Hal Hal Hal!

Ohhi, I don't believe it, you'll be a millionaire!

I received an e-mail that says I've won a 1M QR in a raffle. But I haven't joined in a raffle!

Ohh Ohh

Um Al-lawl, read this for me.

It's a trick! They are trying to phish me. Let's delete it.

Dear Um Khamas, We are writing this letter to inform you that you have been chosen to sing in the National Celebration Day. Call us.....553545434

Of course, I will call them now

What? I'll be so famous worldwide and rich!!

Um Al-lawl, read this for me.

What? My Bank? OK (Doha Bank....)

HELLO, I'm Um Khamas

Congratulations, please give me your Bank Account

No, No! Be careful It might be phishing. Phishing seeks to trick people to gain confidential or private information for promised goods, services, money and more.

HERE ARE SOME TIPS TO AVOID PHISHING:

- Install anti-virus software and/or spam filters into your PC and keep up-to-date
- Don't trust offers that seem too good to be true.
- Don't open e-mail classified as junk mail unless you trust it.
- Be suspicious about e-mails that ask for personal or confidential information.
- Don't download attachment from unknown sender, it may contain viruses.
- Don't respond to suspicious e-mails.
- Inspect URL of website.
- Consider security alerts..

Prepared by Mariam Al-Hamar

Freej characters used by kind permission of Lammtara, UAE

Figure 8.4: Poster 3- Story board

8.1.2 Cartoons

Discussions with the experts have confirmed that presenting a cartoon about phishing is a good idea to make people aware of such threatening attack. Therefore, two cartoons about phishing were drawn. The first, *In phishing you are the fish, so don't bite!*, illustrates phishers and how they trick people to fall prey to their attacks. The phisher was presented as a fisherman but, instead of delivering a catch of fish, he cast a deceptive e-mail as bait to entice people to bite on its hooks. Fish presented in the cartoon demonstrate a sample of victims available on the Internet; some have money and valuable information to be stolen by phishers and others might have nothing but they could still be targeted by phishers to be used, for example, to distribute phishing e-mails or to use the victims' computers from which to perform their crimes (see Figure 8.5). The second cartoon, *Don't fall for it, they try to phish you*, illustrates victims of phishing, how they react once they receive a phishing e-mail and what makes them vulnerable to falling prey to such attack, especially when it conveys a sense of urgency and surprise. The poster demonstrates that people should not trust offers that seem too good to be true and they have to be aware of phishing and its tricks (see Figure 8.6).



Figure 8.5: Cartoon 1

Don't fall in it, they try to phish you

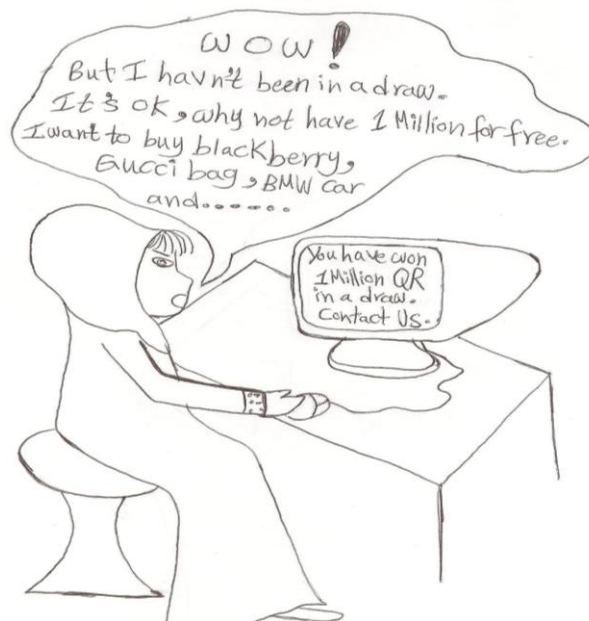


Figure 8.6: Cartoon 2

8.1.3 Presentation Slides

Presentations can give more details about the phishing threat and, in particular, e-mail phishing. Therefore, a series of simple, understandable presentation slides about the phishing threat was developed for use in a seminar tutorial. So that the presentation is associated with Qatar, it uses the awareness officer, Naseh, as a trusted symbol representing Qatari police. The presentation delivers enough of the information required about phishing to enhance people's defence level against such attack and covers the following topics in the form of brief questions: what is phishing? what is the impact of phishing? why is phishing successful? how do you avoid phishing? and how should you react once you are tricked? It also shows an example of a phishing attack and how it could be recognised. Since the awareness officer is commonly used for traffic awareness, traffic signs are used to present the suggested guidelines on how to avoid phishing attempts. They will also help participants to remember the guidelines (see Figure 8.7). Also, the meaning of the same guidelines is represented in a related diagram which makes the presentation more interesting and easy to understand and remember. For a full version of the English and Arabic presentation, see Appendix E. The manager of the public relations department at the Ministry of Interior was shown the presentation after development and found it potentially effective, understandable and well presented.

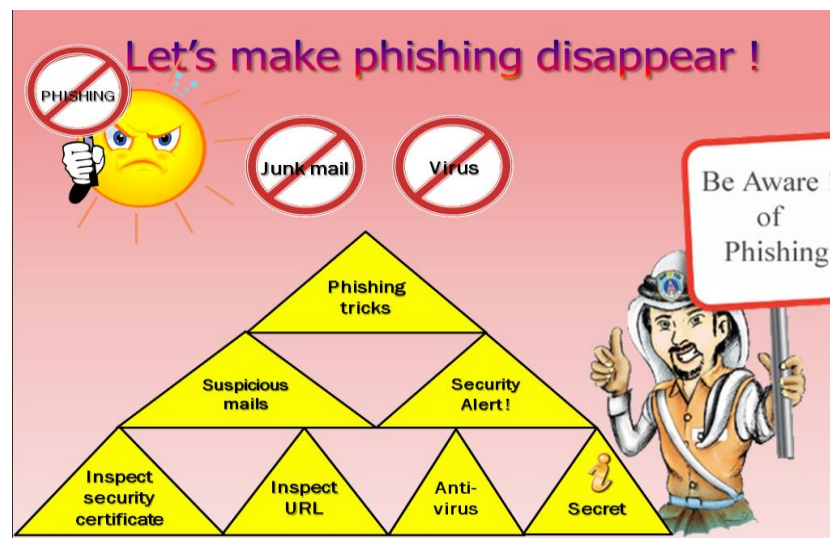


Figure 8.7: Presentation slide

8.1.4 Booklet

The idea of the booklet came from the experts in awareness from the Public Relations department of the Ministry of Interior who suggested it would be likely to be effective in making people aware of the phishing threat. It is essentially the presentation slides in a different form in an A5 booklet as a handy means of making people aware of the phishing threat.

8.1.5 Quizzes

Quizzes aim to measure people's knowledge in a particular subject area and, in the case of phishing, they could be used to measure people's vulnerability to e-mail phishing according to knowledge of phishing, behaviours and reactions and ability to recognise phishing attempts. Therefore three automated and interactive quizzes were developed to achieve this aim. Quizzes were also used to evaluate the effectiveness of the awareness framework by comparing the results of participants in some aspect of the framework with the results of people who had not participated.

8.1.5.1 Quiz 1

This quiz is to assess people's vulnerability to e-mail phishing based on knowledge of e-mail phishing attacks provided earlier in the presentation slides, as five open-ended questions related to phishing, as follows:

1. What is phishing?
2. What is the impact of phishing?
3. Why is phishing successful?
4. How do you avoid phishing?
5. How should you react on being tricked or on encountering phishing?

In this quiz, users do not get any feedback on their answers since it is hard to give scores because of the open questions used. However, it will give an indication of the

amount of knowledge users have on the phishing threat before and after the learning session.

8.1.5.2 Quiz 2

This quiz measures vulnerability to e-mail phishing based on behaviours and reactions. It will also assess whether those behaviours have improved after the learning session. From the literature review, various behaviours were discovered which might make people vulnerable to phishing (e.g. not installing anti-virus software, opening junk mail) (see Section 2.5.2.1). These behaviours were then put into the form of a quiz with 20 Yes/No questions. The questions, with the correct choices, are as follows:

1. Are you aware of the phishing threat? Yes
2. Do you install anti-virus software or a spam filter in your PC? Yes
3. Do you upgrade your anti-virus software regularly? Yes
4. Do you regularly run a check for viruses on your PC? Yes
5. Do you inspect URLs in e-mails? Yes
6. Do you open e-mails from unknown senders? No
7. Do you open junk mails? No
8. Do you use the same password for more than one application? No
9. Do you give your confidential information (e.g. password, bank account) to anyone, even your friends or relatives, on request? No
10. Do you download attachments from unknown senders? No
11. Do you check a file's extension before you download it from the Internet? Yes
12. Do you inspect the digital certificate of the website before entering confidential information? Yes
13. Do you enter your personal or financial information into pop-up windows? No
14. Do you trust e-mails that do not address you by your name? No
15. Once you receive a suspicious e-mail, do you contact the company directly instead of going to the URL or phone a number in the e-mail? Yes
16. If you think you have received a phishing e-mail message, do you report it (e.g. to the police or a bank)? Yes

17. Do you type addresses directly into your browser instead of clicking on a hyperlink supplied in the e-mail? Yes
18. Do you consider the security warnings? Yes
19. Do you switch off your firewall application or anti-virus software when notification messages keep appearing to you frequently? No
20. If you think you have been tricked, do you do any of the following actions: Yes
 - Change the account details that you have revealed?
 - Check your financial statements immediately?
 - Cancel your credit and debit cards?

Even if one choice is wrong, this means the respondent is vulnerable to e-mail phishing. Each correct choice earns 1 point. At the end of the quiz, users are given their scores and their level of vulnerability to phishing along with the correct answers. Assessment of people’s level of vulnerability to phishing was based on total quiz scores in Table 8.1:

Table 8. 1: Scores assessment for Quiz 2

Scores (out of 20)	Vulnerability level
20	Very low vulnerability. Excellent, you are hardly ever vulnerable to phishing because you are well defended against it. Try to keep up to date on the subject of phishing. For more information go to http://www.antiphishing.org
19-15	Low Vulnerability. Very good, but it is better to pick up, as follows: (Give advice on correct behaviours which users get wrong)
14-10	Average vulnerability. Good, but you have to improve as follows: (Give advice on correct behaviours which users get wrong)
9-5	High vulnerability. Satisfactory, you have got lots to learn, as follows: (Give advice on correct behaviours which user get wrong)
< 5	Very High vulnerability. Unsatisfactory, you are easily hooked by phishing, you should recover as follows: (Give advice on correct behaviours which users get wrong)

8.1.5.3 Quiz 3: Anti-phishing Game

Sheng et al. (2007) present a useful and effective game for enhancing users’ defence levels against phishing based on the URL, which motivated the researcher to build a similar anti-phishing game, but which broadens the learning concept of ways to detect

phishing e-mails through security indicators and message content as well as URLs. Therefore, an anti-phishing game was developed to raise people's awareness of the threats associated with e-mail phishing and to teach them how to identify and avoid phishing e-mails using a range of indicators.

The deployment of the game encourages people to learn about phishing while playing an exciting game. This changes the concept of learning and awareness from formal teaching and boring lessons into fun and interesting learning through an interactive game carefully designed for this purpose. This quiz was introduced as part of an interactive game which will both educate the user and also help assess the user's ability to recognise phishing attacks through using an enjoyable tool.

Game Planning and Design

The anti-phishing game is a web game for educating e-mail users on how to identify e-mail phishing. To develop an attractive game, an iterative design process was used. The design has passed through different stages from early plans made on paper, through Flash prototypes until the final version of the game.

The game was implemented by the researcher using Flash MX 2004. This provides a great deal of flexibility, particularly when creating animations, making it easy to quickly update the content. Most workstations have the Flash player, so there is no need for additional downloads. Flash is integrated with Adobe applications such as Photoshop and Fireworks and Dreamweaver. In the anti-phishing game, MySQL was used to store the user's data and PHP was used as middleware to process the data. The main reason for choosing PHP is that it is open source software and is widely used and supported by ISPs (Internet Service Providers). MySQL was chosen because it supports multi-user connections, it is open source and, like PHP, it is widely supported by ISPs.

Game Mechanics

The game is designed to help users understand the mysteries of the world of phishing. From the literature review, it was concluded that there are three main factors in detecting e-mail phishing: the URL of the website, the security certificate and the message content. Accordingly the game was designed to address these factors (see Figure 8.8).



Figure 8.8: Factors addressed in game

This educational game teaches users how to detect e-mail phishing through 3 games, each focusing on one of the above factors (see Figure 8.9).

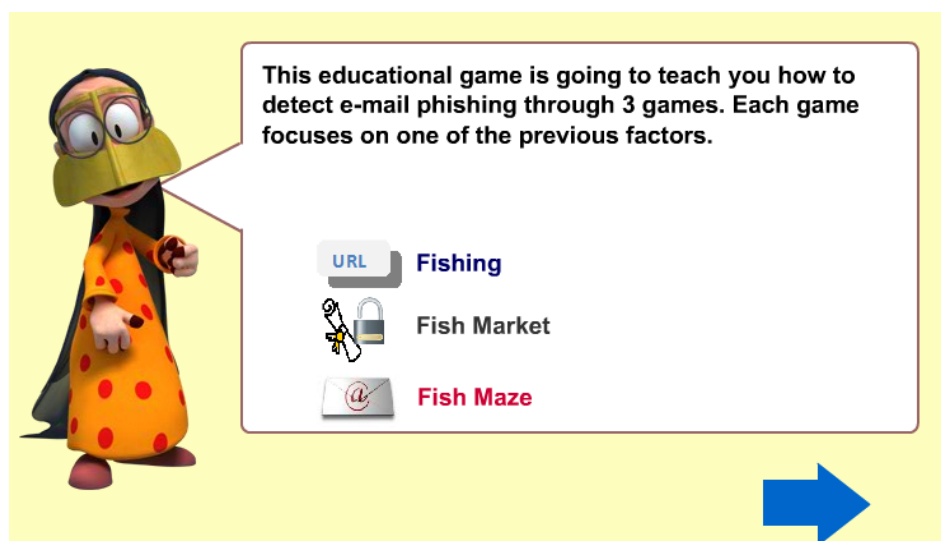


Figure 8.9: Three educational games

The game assesses users' abilities to distinguish phishing e-mails by these three main indicators, assessing the users' vulnerability to phishing from the scores of each game. These games were based on the 'Anti-Phishing Phil' game designed at Carnegie Mellon University by Sheng et al. (2007) in research on the factors which make people vulnerable to phishing, and on the phishing archive (MillerSmiles, 2006) which gives an overview on e-mail phishing tricks. The archival collection defined examples of phishing URLs which were found to be either IP-based URLs, extended URLs with sub-domains and misleading ones with visual similarities to legitimate URLs. The game was designed to include both legitimate and phishing e-mails to test the ability of the user to identify phishing. Five typical questions for Games 1 and 2 and 3 are shown in Table 8.2.

Table 8. 2: Typical questions for games

	Game 1 Do you trust the following URLs ?	Game 2 Do you deal or no deal ?	Game 3 Do you trust the following messages?
1	http://natwest.natwestbank-updates.com	Website: http://www.ebay.com/login. Owner: ebay,Inc. Verified by: Secure,Inc.	You receive an e-mail classified as junk mail by your e-mail system.
2	http://165.71.1.96/natwest/	Website: http://www.natwest.com/personal.ashx. Owner: Natwests,Inc. Verified by: VeriSign,Inc.	E-mail asks you to verify your account by directing you to official website
3	http://www.ebay.com	Website: www.paypal.com. Owner: Paypal,Inc. Verified by: VeriSign,Inc.	You receive e-mail from your bank which asks you to phone number supplied in e-mail for more information about new courses
4	http://entertainment-memorabilia.ebay.com/	Double-clicking lock icon on status bar takes you to security certificate issued to same domain name (www.microsoft.com) as Web site domain name in address bar.	E-mail asks you to reply with your account details through given e-mail address
5	http://tesco.co.uk	Website: www.amazoon.com. Owner: Amazoon,Inc. Verified by: VeriSign,Inc.	You receive e-mail which addresses you by your first and last name (e.g. Dear Prof. Ray Dawson)

Game Tales

The main characters of the game are from the *Freej* cartoon. These four characters (Um Saeed, Um Saloom, Um Allawi and Um Khammas) have been chosen along with the character Um Um Khammas, with the cat, who plays the role of the phisher in the game. Um Allawi is presented as the story-based agent who will assist the user during game (see Section 2.5.2.2). The game was designed in the form of a story to attract players and it uses sound and graphics to encourage better user interaction with the game. In all three games, the player has to try to save the fish from the phisher. Each character plays a role in the game, as shown in Figure 8.10.



Figure 8.10: Game characters screen

1. Fishing game

The main characters of the game are the Phisher ‘Um Um Khammas’ and the fish. The tale is that the phisher is fishing and the player can release the fish if he or she identifies the legitimate websites from the URLs provided. For each question the player gets right, he or she will earn 10 points and will save the fish from the phisher, otherwise the fish will be caught.

2. Fish market game

The character Um-Saed is shopping in the fish market and the sales lady, Um Khammas, is selling fish. The player has to help Um-Saed by selecting the right deal for the fish by figuring out the legitimacy of the security certificate. The player has to select the fish and then decide whether to deal or not deal. For each one the player gets right, he or she will earn 20 points and Um-Saed will get the fish, otherwise it will be taken by the phisher’s cat.

3. Fish maze game

The fish is in a maze and the player has to help it to reach the safety of its owner, the character Um-Saloom, by figuring out whether the message is trustworthy. For each one

the player has got right, he or she will earn 10 points and will save the fish, otherwise the fish will be caught by the phisher and the cat.

Game Description

The anti-phishing game begins with the initialisation of global variables while the game loads. It then asks the player to log in by entering his/her username and password. Alternatively, in the case of a new user, the player has to register before logging into the game (Figure 8.11). The game then brings the user to a welcome page (Figure 8.12) where he/she has the choice to go for a brief introduction of the game which is given along with a short movie clip which shows the phisher ‘Um Um Khammas’ who is fishing on the sea and the agent ‘Um Allawi’ tries to stop her and to raise users’ awareness of the phishing threat (Figure 8.13). Heinich et al. (1993) have stated that the use of animation would transform education and make it more motivating for students.



Figure 8.11: Log in and register screen

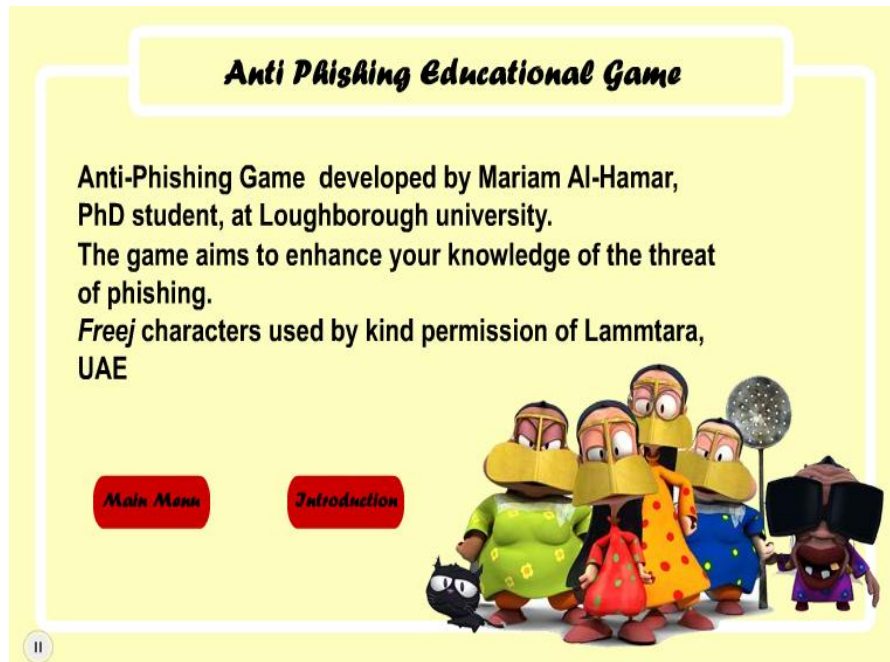


Figure 8.12: Welcome screen



Figure 8.13: Introduction movie clip

The game menu consists of four options (Figure 8.14):

1. Games which then presents the three games (Figure 8.18, 8.19 and 8.20)
2. Conceptual knowledge (Figure 8.16)

3. Procedural knowledge which gives the user some information about phishing threat to raise their defence level (Figure 8.17)
4. Quit option to exit from the game, leading back to the Log in and register screen (Figure 8.11).

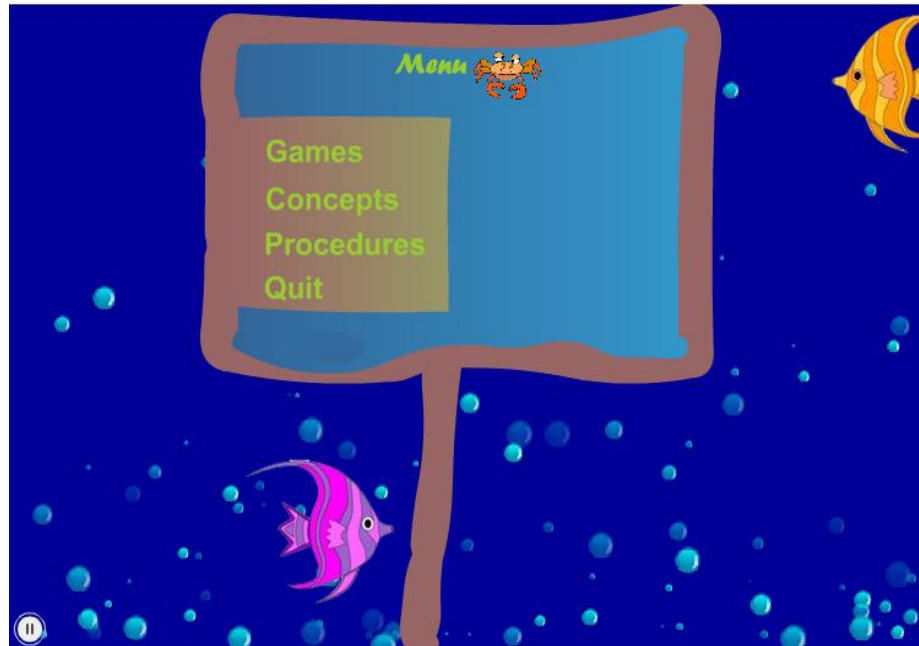


Figure 8.14: Game menu



Figure 8.15: Game instruction screen for the fish maze game

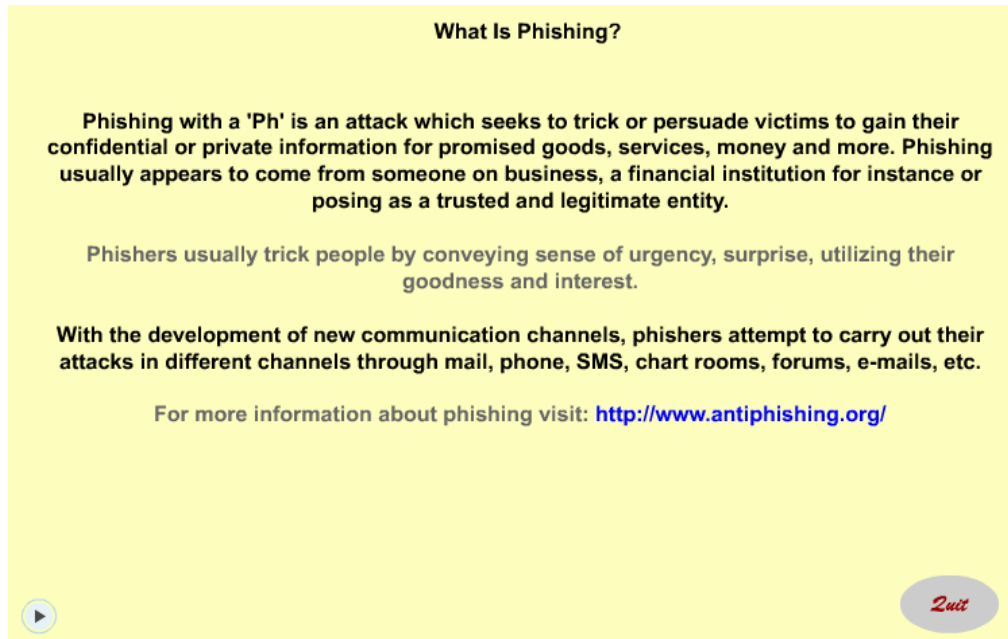


Figure 8.16: Conceptual knowledge screen

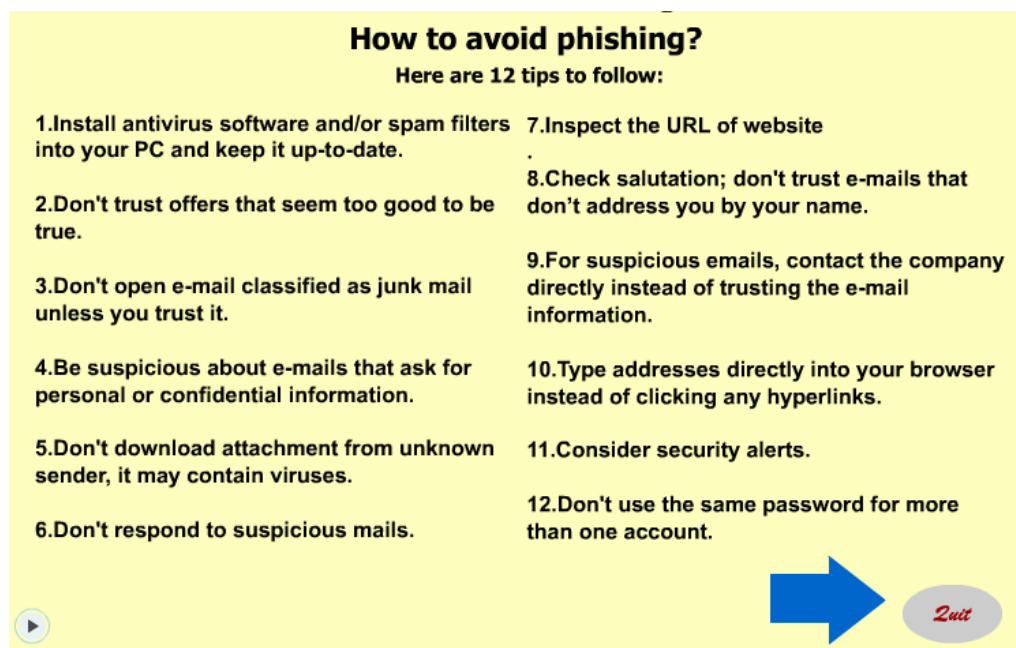


Figure 8.17: Procedural knowledge screen



Figure 8.18: Game screen for the fishing game



Figure 8.19: Game screen for the fish market game

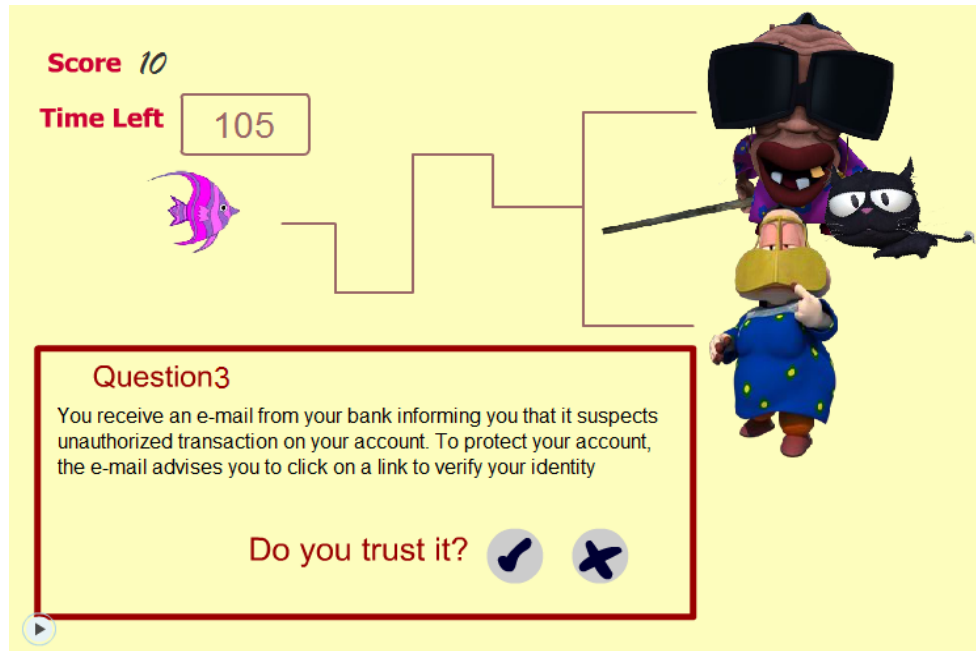


Figure 8.20: Game screen for the fish maze game



Figure 8.21: 'Game over' screen for the fishing game

Question No	Question	Result	Comments
1	http://tesco0.co.uk	Wrong	Phishing Alert! the URL doesn't belong to Tesco supermarket, however the domain looks similar
2	http://www.amazon.com.shopping.co/	Wrong	Phishing Alert! This site belongs to shopping.co, not amazon.com.
3	http://yahooligans.yahoo.com/content/games/	Wrong	It is part of yahoo because 'yahoo.com' is before the first slash in the URL
4	http://www.amazon.co.uk	Correct	The homepage of Amazon in the UK
5	http://group.barclays.britishbanks.com	Correct	Phishing Alert! This site belongs to britishbanks.com, not Barclays.
6	http://www.paypal.com	Wrong	The homepage of the payment site Paypal.
7	http://entertainment-memorabilia.ebay.com/	Wrong	This site is part of 'ebay.com' because 'ebay.com' is right before the first slash
8	http://natwest.natwestbank-updates.com	Wrong	Phishing Alert! the URL doesn't belong to NatWest bank, however the domain looks similar
9	https://www.amazon.com/gp/css/homepage.html	Correct	This site belongs to 'amazon.com'
10	http://secure.whsmith.co.uk/	Correct	Is belongs to 'WH Smith', a famous bookshop in the UK

Figure 8.22: Results screen for the fishing game

The games option consists of three games: Fishing, Fish Market and Fish Maze. Whichever game the user chooses, he/she will be able to see the game instructions which provide an introduction to the game and how to play it (Figure 8.15). Once the user chooses to play the game, the game timer will start counting down and the score is automatically increased when the answers are correct (see Figures 8.18, 8.19 and 8.20).

For testing purposes, the game questions are selected randomly from the sample of 20 questions in the data file to provide a reliable test. The games are flexible to enable them to be developed, so the questions could be easily enhanced and extended in the future for large groups of people. When the time is over, or all of the game questions are answered, the game is over and the user's score and rating (see Figure 8.21) are displayed according to the scores gathered (see Table 8.3).

Table 8.3: Scores assessment for game

Scores (out of 100)	Vulnerability level
100	Very low vulnerability. Try to maintain
90-80	Low vulnerability. Better to pick up
70-60	Average vulnerability. You have to improve
50-40	High vulnerability. You have lots to learn
<40	Very high vulnerability. You are easily hooked by phishing, you should recover

The user then has the option of replaying the game, quitting to the game menu or viewing the results (see Figure 8.22). The results page shows the game questions, whether the user has answered them correctly, incorrectly or not answered at all. Also, it shows brief comments on each question to provide users with an opportunity for reflection. The flow chart in Figure 8.23 gives an overview of the game process.

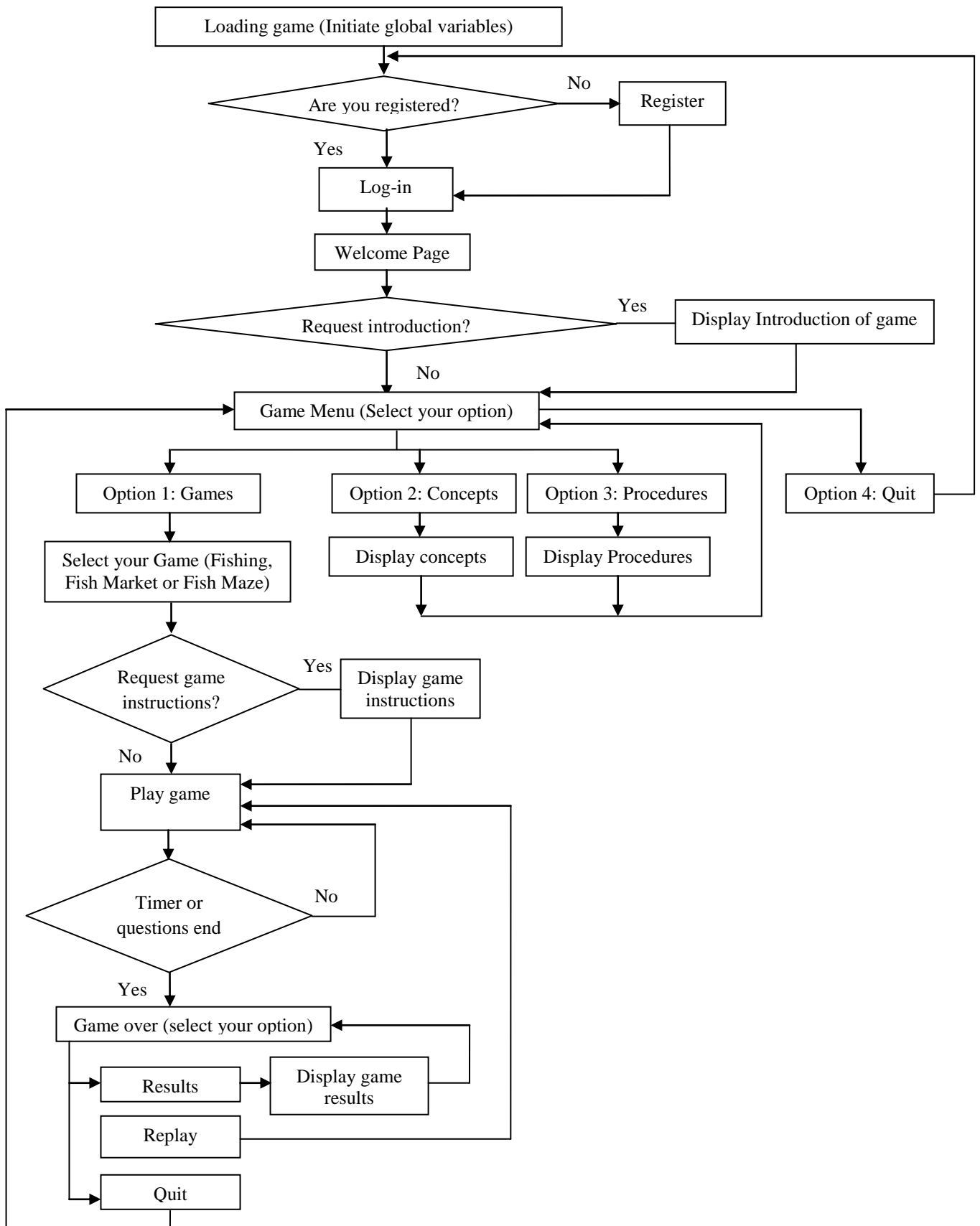


Figure 8.23: Game flow chart

8.1.6 Development of anti-phishing e-learning

With the rise of the Internet, there is a corresponding rise in the need for e-learning sites (Zenger and Uehlein, 2001). Although the traditional form of education is still important, e-learning and distance learning are now becoming a more prominent form of education since they add flexibility to the education process where people can learn through the Internet at any time convenient for them (Horton, 2000) (see e-learning in Section 2.5.2.2). Although e-learning is a useful educational tool, traditional education is still important since the student can have a full interaction with the teacher which is lacking in e-learning (Lord, 2001; Van Dam, 2001; Horton, 2000; Hall, 1997). However, a lot of research on e-learning is directed towards improving the effectiveness of the learning from educational websites, such as improving the accessibility, usability, visual representation, HCI (Human Computer Interaction) and live support (Martin, 2007; Zaharias, 2004; Feldstein, 2002).

Since the Internet has become a main source of information for many people, a usable e-learning website on e-mail phishing threat was developed. This site involves a range of educational tools including posters, cartoons, presentation slides and quizzes to educate people on such threat. In addition, the e-learning site facilitates evaluation of the awareness programme, since it involves user registration, along with a questionnaire, and it also constructs automated quizzes where the results are stored in a structured database for the researcher to use. The database stores users' profiles, behaviours, feedback and results. The questionnaire helps in evaluating the site with regard to its educational material, including whether it enhances users' knowledge of e-mail phishing, how users would best describe it, whether the information provided is regarded as good and important to know, which of the educational materials were more effective and, in general, if users have any comments or suggestions for improvement.

Users are asked to register before accessing the educational material. The registration process asks for user's age, education, occupation, nationality, level of computer knowledge and use of e-mail and choice of username and password. This information is

used in the evaluation phase of the awareness programme. A print screen of the login page of the e-learning site is shown in Figure 8.24 (see Appendix E and F for more details on e-learning design).

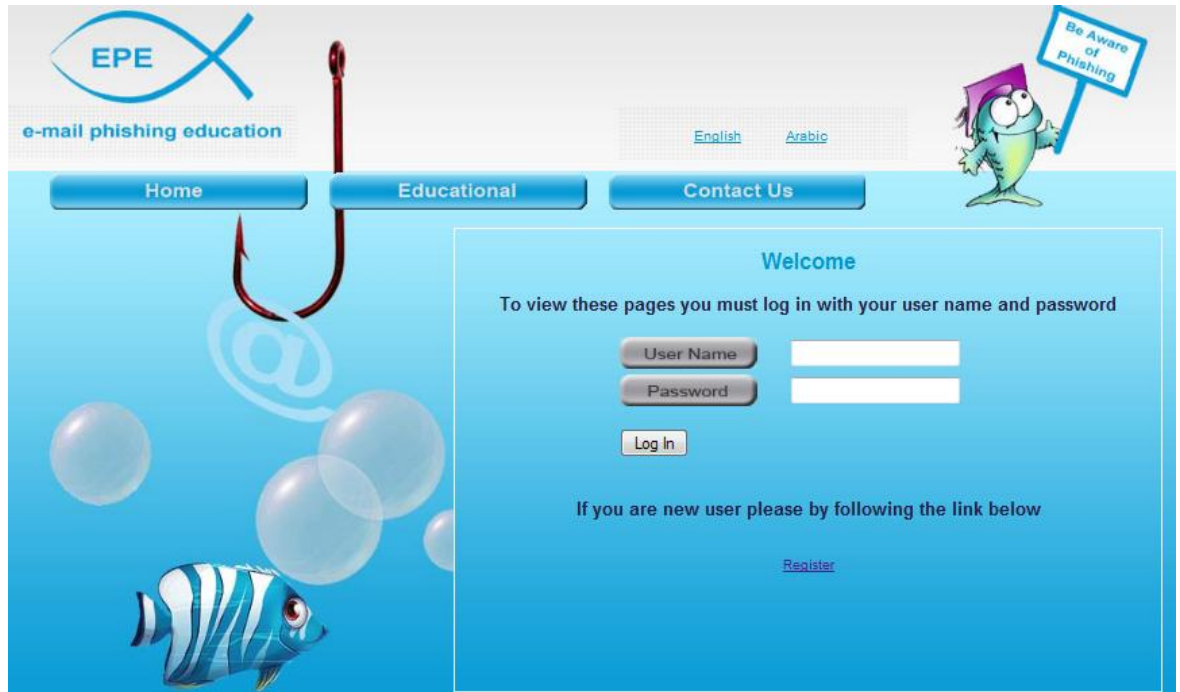


Figure 8.24: Login page of e-learning site

8.2 Running programme session

Both experts on awareness suggested that educational institutes should be targeted and, in particular, schools in Qatar, since children are the next generation but are probably less aware of phishing as they are unlikely to have much confidential information or financial income to be stolen. Therefore the researcher targeted the teenage student age group 14-18, as they often use the Internet and are sometimes thoughtless in their decisions and actions. As there are difficulties in getting authority from community schools since permission should come from the Ministry of Education, private schools were contacted where permission is granted by the School Director. Two schools in Qatar (Amna Bint Wahab and Al-Shima Secondary School) agreed to accept the awareness session since they found it would best fit into one of their computer lectures on the topic of security for year 10 (age 15-16). The computer lecturer explained that the session should last for one hour like a usual school session. Therefore the researcher tried to make the awareness session shorter and easy to evaluate for effectiveness in the

time available. The programme session involved presentation slides, posters, cartoons, games and quizzes, and filling in a questionnaire to evaluate the effectiveness of the programme. The researcher used e-learning in the session to run the quizzes and questionnaire to assist in analysing results.

The plan for the awareness session was as follows:

1. Students required to register on the e-learning site
2. Quizzes on the e-learning site to assess people's knowledge and vulnerability to phishing before the awareness session
3. The awareness seminar where the researcher showed the PowerPoint presentation slides, the posters and cartoons.
4. Students complete the quizzes again to evaluate whether their vulnerability to phishing had improved after the seminar.
5. Students answer the questionnaire given in the e-learning site. This was helpful to evaluate the effectiveness of each piece of educational material and of the overall awareness framework.

Finally, students were invited to make any suggestions or comments on the session and were given a guidance booklet about phishing which contains the information shown in the presentation slides. The outcome of the session is described in the next chapter.

8.3 Running the media programme

The media programme was another interesting way of creating awareness which reached more people worldwide. Running the media programme involved several stages as follows:

1. Setting up a television programme

The Al-Jazeera Children's Channel was approached for an interview with the director of production to discuss whether the media play a role in enhancing awareness of the Internet threat and in particular phishing. He mentioned that they had not covered such a topic but he thought it is important to discuss and improve public awareness of the phishing threat which shows a high potential for victims in the region and around the world. He agreed that the media has a major effect in passing a message to a large number of the population in a short period of time. He pointed to the importance of designing awareness material that is understandable, attractive, consistent, without bias and suitable for the intended targeted audiences, who are children who watch the Al-Jazeera Children Channel. The researcher was then invited to participate in a television show called *Nadhra ala* to speak about *Dangerous e-mails*, the programme produces phishing threat.

2. Presenting the Television Programme

The programme was in Arabic and involved the following participants: the female anchor, the researcher, 2 teenage phisher boys and 2 teenage girls around a table and a studio audience of about 30 other children. The programme took the form of a debate between programme participants, involved some *vox pop* (i.e. *voice of the people* which is usually gathered from interviews with the general public) reports with opinions of some children on the subject and there was also a poll question. The programme was subsequently translated with English subtitles (see Appendix G).

3. Summarising the Programme Outcome

The programme generally discussed the importance of the Internet in children's lives, what it is being used for, whether children know its advantages and disadvantages and what their views are on hackers, and in particular, on phishing. The programme asked whether they know how to protect themselves, are able to control what they see and learn through the Internet, are subject to supervision by their parents, whether they believe in online friendships and consider it a modern way to communicate with others

and build friendship, know the ways in which hackers can penetrate their computers and how to protect themselves from hacking and phishing. The programme also tried to find out why phishers are motivated to commit their crimes.

In summary, the programme had the following key items:

1. *vox pop* and discussion with the studio audience

The discussions with the participants and reports from some children show that most love the Internet because of its many advantages, such as improving education, research and communication, leisure, searching, saving a lot of time and effort in finding information, electronic commerce and the many services on the Internet.

There were different views expressed in the discussion by those who spend long hours on the Internet and those who believe that the use of Internet is important but with limits. Some were restricted by their parents to use it only at weekends and for a limited time in order to avoid its interfering with their studies. Some of those who spend long hours on the Internet reported pain in their back and eyes and they felt isolated from people in the outside world, which therefore affected their studies and daily duties. Some even admitted to being addicted to it but others become annoyed with spam messages, viruses and hackers.

2. The two boys in round table discussion

The boys claimed to be phishers and said that they are subjected to nuisance from unknown people and, in turn, they commit their crimes on people who bother them. When they decided to harm someone, it is normally premeditated and usually involves building a relationship with their victims through chatting and then enticing them to give their confidential information such as their username, password and security questions. If they hack a victim's e-mail address, they attempt to steal their victim's details without the victim's being aware of what has happened. However, the phishers felt they were not harming their victims. Their aim was often to copy their victim's

contacts or to boast to their victims that they have such private knowledge about them. They felt it was normal to send threatening e-mails to victims to intimidate and annoy them. They found it fun, exciting and a form of revenge. They did not believe they were doing anything wrong or that they were violating someone's privacy, although the phishers admitted they would get upset if they, themselves faced such an attack and they took safety measures to prevent other hackers from hacking their PCs.

Even after a long discussion, the phishers still seemed to be happy about what they were doing to others. The phishers seemed to have conflicting views of themselves, thinking they were 'half evil but hiding inside the clothes of a fine man'. In the end, they still admitted that they will continue to be expert hackers in the future and they will not stop phishing. This shows that they might already be addicted to phishing and they will continue to not consider the consequences of what they are doing, not only to others but also to themselves, as they could be criminalised. Thus there arises the responsibility of the government, in particular the Ministry of Interior, to pull them away from this field and shift them to a more constructive use of their skills, for example getting them to become 'white hat hackers' where they work on auditing the security level of the system by hacking into it to identify its weaknesses with the benefit of developing a secure system. This is done by many global organisations such as Microsoft which attract hackers to work in their premises towards improving their system. Parents clearly need to control their children's activity on the Internet so that they will not be driven into criminal and illegal actions.

3. The two girls in the round table discussion

The girls were against hacking but love to learn everything about the Internet including hacking. They claimed that anyone who practices hacking will begin to see it as something normal and his/her conscience will die, because every day they will harm people. They thought that they have not been hacked because they are peaceful and they have not harmed anyone else. However, the researcher stated that this might not be true because phishers could target anyone and they direct a lot of attacks at many people

they do not know. Even simple information or a small amount of money is valuable to phishers because they will build up their habit from one victim to another.

4. The researcher's contribution

The researcher pointed out that the Internet mostly becomes available for children in their own home, so there is therefore a need for parents to observe and control their children's Internet activity rather than preventing them from accessing the Internet. This control is available through many computer programs such as Parental Control. However, whatever methods of protection are available, phishers seem to become ever more powerful and devious. She mentioned the strategy of Qtel and Vodafone in shutting down and blocking these sites after research and verification of their malicious intentions. However, the solution is not in blocking those sites, because hackers or phishers will launch another site with a new name and will repeat phishing. Phishers seek to bypass the technological tools by trying to look at gaps and weaknesses in the program to bypass it. Therefore it is important to update anti-virus programs regularly. The researcher stated that the children who became phishers may be motivated by their love of excellence in their sabotage of others or perhaps they consider it entertainment. She warned that maybe they are now just enjoying what they do but, perhaps with time, they may become addicted, so the problem must be addressed through awareness.

5. Poll question with studio audience

The studio audience was asked to answer a question on what they mostly use the Internet for. The results were as follows: 12% use the Internet for research, 38% to enjoy the games and half (50%) use it for e-mail and social networks such as Twitter and Facebook. Despite the irony of the result, it really reflects the reality. This indicates that e-mail is a common method of communication and therefore it is more attractive for phishers.

Finally, the show concluded that although researchers try to make everyone aware not to open a message when they are not sure of its source, people do not follow this advice. If they receive a message that says 'I love you', some would feel curious to know this person who loves them. The discussions showed that people are vulnerable to phishing which exploits their interests, beliefs, emotions, generosity, helpfulness, trust, good will, religion and others, which was mentioned by the researcher and agreed by the participants in the programme. Although there are many recommendations presented on how to protect against phishing, these phishers are stronger than those warnings. An evaluation of the programme is discussed in the next chapter.

8.4 Summary

This chapter has presented the development of part of the awareness framework which is the awareness programme and how it has been implemented. It involved seminar sessions, along with e-learning and a television show. The seminar sessions and e-learning used attractive and motivating educational tools, including a presentation, posters, quizzes and cartoons to educate people on the risk e-mail phishing. Interactive quizzes were used to assess people's vulnerability to phishing according to knowledge of phishing, behaviours and reactions and ability to recognise phishing attempts. The interactive quiz game made the learning into an enjoyable, interesting and interactive awareness tool which measured vulnerability to phishing. Although e-learning was developed to support the learning session it was actually useful as a training method on its own.

The television programme concluded that there are people in Qatar who are hackers/phishers and as they seemed to find their task easy and enjoyable would do it many times with little motivation. They were not troubled by any conscience and did not recognise the severity of the crime, so they will continue to hack/phish regardless of the consequences. In addition, it was found that there is clearly a lack of awareness of the phishing threat in young Qatar citizens and they were vulnerable to phishing which exploits their interests, beliefs, trust, good will and religion.

The next chapter presents the evaluation of the proposed e-mail phishing awareness framework and how the framework is put together and tested. The framework is a collection of methods that could be used to make people aware of the risk of e-mail phishing. The learning programme described in this chapter is a set of methods taken from the framework that was used on one specific occasion.

Chapter 9 Evaluation of the Educational Framework

This chapter evaluates the effectiveness of an educational framework on e-mail phishing in enhancing Qatari citizens' level of awareness of the e-mail phishing threat and, consequently, in reducing the risk of e-mail phishing in Qatar. The proposed educational framework involves different training methods, such as embedded training, contextual training and a learning programme which involves a media programme and an educational session with e-learning (see Chapter 8). Each is evaluated to identify its effectiveness in improving user awareness of phishing in Qatar.

9.1 Development of the Educational Framework

The review of available literature led to the conclusion that awareness is an important solution to reduce the effect of phishing and there is a need for a comprehensive e-mail phishing educational framework which involves different training methods including embedded training and contextual training, learning programmes and e-learning. Table 9.1 describes the implementation of each training method in the awareness framework.

Table 9.1: Research implementation of each training approach

Training type	Training implementation details
Embedded training	Phishing penetration test where 3 phishing e-mails were sent: Request account verification, Request to download attachment and Request for private information by e-mail or SMS. Failing participants automatically alerted with a message about phishing providing conceptual and procedural knowledge on how to defend against phishing (see section 6.1.1).
Contextual	Laboratory experiment where 10 e-mails were asked to be inspected, 6 phishing and 4 legitimate e-mails. At the end of the test, participants were given a booklet containing conceptual and procedural knowledge on how to defend against phishing (see section 6.2).
E-learning	A flexible learning, anti-phishing educational website provided with presentation slides, posters, cartoons, games and quizzes (see Section 8.1.6). Results are stored in a database for analysis.

Learning programme	A programmes involving learning sessions/e-learning and media programme was created (see Chapter 8 for more details). Learning session involved presentation slides, posters, cartoons, games and quizzes to educate users on e-mail phishing. E-learning was used to facilitate analysis of users' activity as the results were stored in a database for subsequent analysis. A television programme was conducted with Al-Jazeera Children's Channel to enhance public awareness
--------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

The development of the educational framework applied the learning principles discussed in the literature review in Section 2.5.2.2 (see Table 9.2).

Table 9.2: Learning principles applied in framework

Principles of Learning	Where applied in this research
Learning-by-doing	Applied in embedded training where training is presented after the user has been tricked by phishing e-mail. Embedded training is applied within the reality test designed not only to assess users' vulnerability to phishing but also includes embedded training material where users who fail in the phishing test will be educated immediately about phishing.
Immediate feedback	Provided when users fall for the phishing e-mail in the embedded training. Also given in the learning programme after playing the anti-phishing game and quizzes so that the learners have an indication of their vulnerability level and what they should do to reduce their susceptibility and improve their defence level.
Contiguity	Considered in the design of the educational framework where pictures and relevant text are placed with instructions alongside. This is seen in the presentation slides, games and posters.
Personalisation	The educational material such as the story-board poster, the cartoons, the anti-phishing game and the TV show incorporates a conversational style.
Story-based agent	Applied in posters, presentation slides and the game by using common local and international relevant cartoon characters such as Freej, Naseh and Finding Nemo.
Reflection	Considered in development of proposed educational programme where learners have chance to review new knowledge gained. In particular, presentation slides at the end summarise knowledge on how to avoid phishing and in the game and quizzes where at the end users are provided with their scores and answers, showing them the correct answers so that they learn from their mistakes.
Conceptual and procedural knowledge	Both conceptual and procedural knowledge are involved in the different training methods. In the teaching materials, users are taught conceptual knowledge about phishing and its techniques along with procedural knowledge on how to avoid it and react through a couple of understandable and straightforward best practices.
Motivation	Incorporated in the learning programme where learners are motivated by interactive learning materials (the games and quizzes).

9.2 Evaluation of the anti-phishing educational framework

To evaluate the effect of the educational framework on participants, a quasi-experimental method was used. This method is frequently used for the evaluation of educational programmes when random assignment is not possible (Mark and Cook, 1984). It provides a comparison of participants according to some measures (Shadish et al., 2002; Mark and Cook, 1984; Campbell and Stanley, 1971). Therefore, it was used in this research to compare the outcomes for individuals before and after being involved in educational training either in penetration test, laboratory test or learning programme to measure participant's improvement in phishing knowledge. Four months after the initial training, the penetration test, laboratory test and quizzes developed for the learning programme were held again using a selection of the same participants to measure their knowledge retention. However, to provide reliable results, different participants were involved for each of the different educational training methods. Table 9.3 shows the evaluation process used for each training method of the framework.

Table 9.3: Evaluation process used for each training method

Educational training	Participants	Training evaluation
Embedded training	Qatari employees who use e-mail in their daily work activity (Required authorisation from organisation). Participants=129 from the AAB company	Quantitative analysis of % of people who fall prey to phishing
Contextual	Convenience sample of Qatari e-mail users aged above 17. Participants=30 (friends and colleagues of researcher)	Quantitative analysis according to number of false positive and false negative identifications of phishing emails.
Sessions/ E-learning	Sample of teenagers (between 15-17 years old) who are e-mail users (Required authentication from school). Two schools involved in test. Participants= 50 students.	Quantitative and qualitative analysis of participant's vulnerability to phishing, calculated from quiz scores and questionnaire results after the seminar and online questionnaire.
Media	Television show targeting children since held on Al-Jazeera children's channel. Participants= 35 children in the studio	Qualitative analysis from interviews with 20 experts and Qatari e-mail users with different backgrounds who had watched the show.

For each training method, the results were measured before, immediately after training and after four months to measure the learners' knowledge retention for each approach. The evaluation showed the value of all education methods in enhancing the students' knowledge of the phishing threat and, hence, in reducing the risk of phishing through an awareness programme. All post-test measures show a clear reduction in the number of phishing failures, false positive and false negative identifications. The retention is quite high even after four months of training and this implies that the awareness sessions were understandable and memorable for most participants.

9.3 Outcomes for Embedded and Contextual Training

Embedded training shows a reduction of 35% in the number of people who fall prey to phishing. Even after four months, the increase in the number of failures from 9 to 11% show very little drop in knowledge. Contextual training shows a reduction of about 6% in both false positive and negatives, but after the four months there was an increase of about 5%. This shows that embedded training gives better knowledge retention and will improve users' knowledge more effectively than contextual learning and that people will learn more once they have faced the problem themselves. This confirms the findings of the literature review (see section 2.5.2.2). The results for each training method of the framework are shown in Table 9.4.

Table 9.4: Outcomes for the embedded and contextual training methods

Training method	Pre-test	Post-test	After 4 months of training
Em-bedded training	% of people who fall prey to phishing = 44% (see penetration test 1, Chapter6)	% of people who fall prey to phishing = 9%	% of people who fall prey to phishing = 11%
Contextual Training	False positive rate= 55/4=14 False negative rate= 65/6= 11 (see laboratory experiment, Chapter6)	False positive rate= 30/4= 7.5 False negative rate= 25/6= 4	False positive rate= 50/4= 12.5 False negative rate= 48/6= 8

9.4 Outcomes for Learning Sessions and E-Learning

In the learning sessions, the results of the quizzes show a clear reduction in participants' vulnerability level but this increases a little after four months when they have forgotten some of the information they have learnt.

Since Quiz 1 contained open-ended questions, it was hard to include scoring, but it could still give an overview of how aware students are of phishing. The results show clearly that the level of knowledge and awareness of phishing had obviously improved after the awareness session since responses to the quiz were more precise and clear, whereas before they were short, not very clear and some were completely incorrect (e.g. there were some who did not understand the term phishing and thought it was fishing or a virus). Students were able to remember some of the educational material four months after the session, especially Naseh's tips on how to avoid phishing since it was linked with traffic sign images which students are familiar with.

The results for Quiz 2 and Quiz 3 are given in Figures 9.1 and 9.2 which show the percentage of participants in each category of vulnerability to phishing.

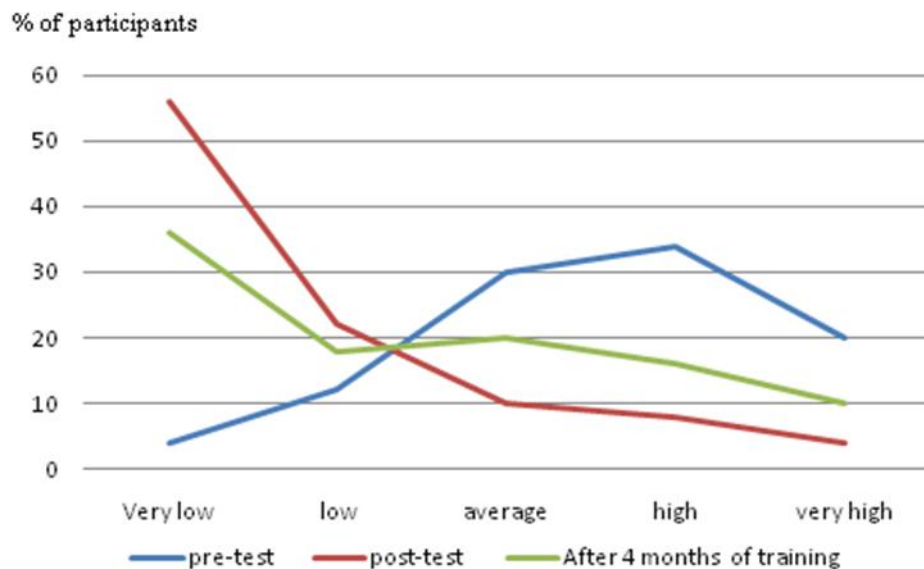


Figure 9.1: Quiz 2 results



Figure 9.2: Quiz 3 results

The majority (74%) of participants in the awareness session stated that the methods used have enhanced their knowledge and awareness of e-mail phishing and only a few (8%) disagreed. Most (66%) described the awareness session as excellent, 23% very good and less than 10% as good and average. The majority (74%) found the information provided by the educational material to be good and believed it to be important to know, but there were some (23%) who did not feel they knew enough to be able to judge the information provided. The participants found all the educational materials were effective in enhancing awareness and publicising the message. The educational method thought to be most effective was the use of quizzes, then posters, cartoons and, finally, the presentation slides, though the difference in popularity of all these methods was small (see Figures 9.3- 9.6 giving response percentages).

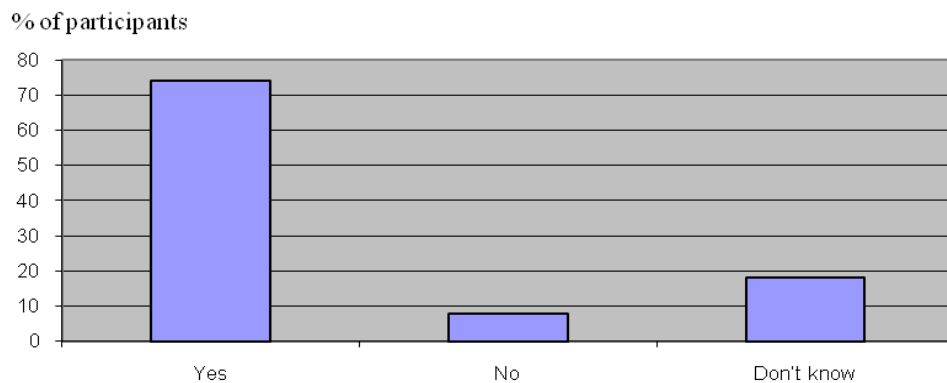


Figure 9.3: Does it enhance the users' level of defence?

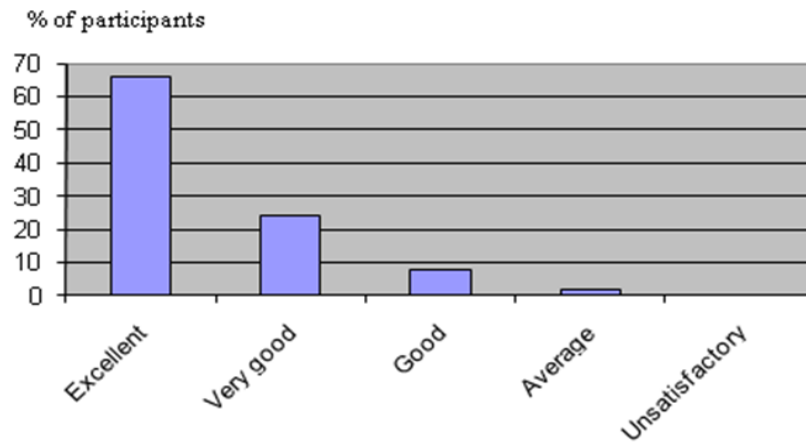


Figure 9.4: How it can be best described?

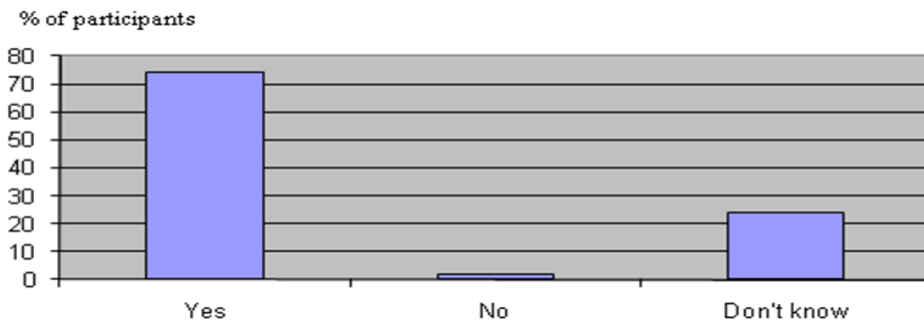


Figure 9.5: Is the information provided important to know?

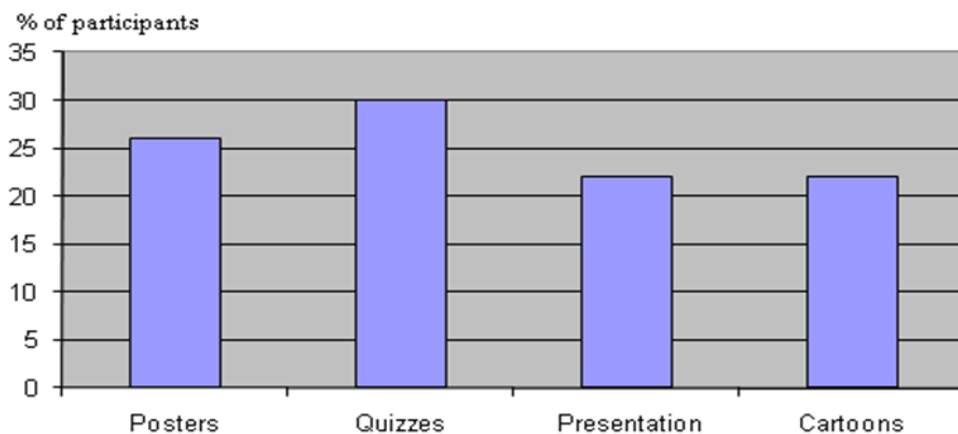


Figure 9.6: Which educational material was more effective?

Before the awareness session, more than half of the respondents (56%) had high to very high vulnerability to phishing. About 42% had low and average vulnerability and it was a shock to find that less than 5% had a very low vulnerability and were well defended

against phishing. However, no matter how high a score was achieved in this test, there might still be a chance of falling victim to phishing attacks. This is because the limitation of the questions proposed in the quiz does not cover all aspects of this type of attack and provides only a sample of behaviours that could make people vulnerable to phishing.

Overall, the majority (98%) showed they were not aware of the phishing threat through their incorrect behaviour as most of them do not inspect URLs and security certificates, they use the same password for more than one application, they disclose their personal information in pop-up windows, they do not report phishing incidents, they trust hyperlinks supplied in the e-mail or they ignore security warnings.

In conclusion, the results based on student behaviours and reactions to quiz 2 show an alarming vulnerability to phishing. However, this improved dramatically after the awareness session when only 12% had high to very high vulnerability to phishing, a much greater percentage (56%) had very low vulnerabilities to phishing and the remainder varied from low to average. The responses clearly show an improvement of 52% in user awareness where it reaches very low vulnerability level (see Figure 9.1).

The results for the quiz 3 game show that the participants' ability to detect phishing attempts was clearly low before the awareness session, where few (less than 10%) achieved a score of 100 in the games but later, after the session, a quarter of the participants reached this score. About 60% had high to very high vulnerability to phishing before the session but this percentage decreased to 21% after the session (see Figure 9.2). Generally, more participants were less vulnerable to phishing e-mails using phishing sites with a fake security certificate than they were to sites with fake URLs and phishing messages. The average improvement reached about 8% (see Figure 10.2), with the highest for game 3 (ability to detect phishing messages) then game 2 (ability to detect security certificate). The participants stated that although it is easy to detect security indicators, some people do not know about them or how to view them, and it is especially difficult when the victim is in hurry or when phishers use icons that are very similar to legitimate security indicators. Some participants suggested extending the

session to more sessions and giving the students the chance to contribute in the session by exchanging their knowledge and experience.

9.5 Evaluation of the Television Programme

It was hard to evaluate the television programme while recording but the researcher had the chance to meet the two phisher boys, the two girls and a sample of the audience before the programme to introduce herself and discuss with them the phishing problem and to see whether they were aware of phishing or not. The phishers certainly showed an interest in phishing and awareness of it but the rest were unaware of phishing, although some were more aware of the terms 'hacking' and 'viruses'. Later, after the programme ended, the researcher asked them again about how they had found the programme and all stated that it was very helpful and enjoyable and that it had definitely enhanced their knowledge and awareness of phishing. They found the information to be illustrated clearly and in a logical sequence, starting with the importance of the Internet in everyday life then moving on to its disadvantages with a focus on phishing as a potential threat. However, this short session was not enough for the researcher to have a solid evaluation of the programme. Another evaluation was therefore made after it was broadcast when the researcher asked a sample of 20 Qatari citizens from different backgrounds (age, education, occupation, e-mail phishing knowledge) and five experts in e-crime and awareness in Qatar, two from the Ministry of Interior and three from Q-CERT, to evaluate the programme. This was done by holding face-to-face, semi-structured interviews with the evaluators separately. Each interviewee was asked the following questions after watching the television show:

- Q1: Was the show useful in enhancing your knowledge and your level of defence against e-mail phishing? What have you gained from this show?
- Q2: How can you best describe the show? Give me your point of view about the show.
- Q3: Do you think that the information provided by the TV show is good and important to know?
- Q4: Are you going to be more concerned from now on about the phishing threat?

Q5. Do you have any comments or suggestions for improvements to the television show?

All the evaluators agreed that the television show was very useful in enhancing people's knowledge and awareness of the Internet threat and, in particular, e-mail phishing. They liked the way the show was presented as it did not intimidate the audience by moving directly into hacking but started gradually by talking about the importance of Internet technology in our lives and its advantages, before demonstrating the disadvantages of hacking as one of the threats associated with the Internet. They found the information was understandable, especially since the compère used the term 'hacking', which is more commonly recognised by the audience, rather than 'phishing' which is a specialised type of hacking. The information presented was simple, understandable and easy to follow. Also, it attracted the interest of the audience as it depended not only on conversation but also on reports and involved interaction with the audience in the studio. They found it useful as well that the compère summarised the points discussed from time to time to keep the attention of the audience on the important issues. Most had no doubt in describing the show as excellent. Most found the information provided was very useful and important to know, especially when discussing how to protect against the phishing threat and when explaining its huge consequences. All of the evaluators were concerned about the phishing threat after watching the TV show and they said that they would follow the recommendations proposed in the programme to protect themselves against the phishing threat in the future.

The expert evaluators were also impressed by the programme presentation and how carefully it was planned. They were surprised by how the phishers freely admitted that they commit phishing attacks and how their parents were not able to control them before reaching this stage. They pointed out that the advantages of this programme, not only for children but also for adults and parents, were that it demonstrated some recommendations for the latter to control children's activity by using available parental control programs. Generally, most commented that the show was "fantastic" and shed light on a subject which was not covered enough before, especially for children. They suggest opening discussion with outside audience.

The enthusiasm about the show led some interviewees to suggest taking it further. Some suggested having more similar programmes talking about hacking and different hacking methods such as social engineering, viruses, Trojan programs and so on. They argued that there was a lot of information to discuss and one show was not enough. Some suggested opening the interaction in the show to an outside audience to enable the public to ask questions and talk about the subject. However, these ideas are not under the control of the researcher. She had hoped to demonstrate some of the developed educational materials in the show but this was not possible. Finally, some interviewees suggested using the phishing awareness session developed in this research in public education (e.g. in schools, universities) to enhance people's awareness of e-mail phishing. It was also suggested that research is needed on the intentions and motivation of phishers and why it has attracted a number of young and teenage Qataris, as was demonstrated from the television show.

The main lessons learned from the television programme were:

1. There are some clever child hackers operating in Qatar who are not being watched or restricted in their actions. Clearly more control over the actions of these children is necessary.
2. There is a clear lack of awareness of phishing amongst most young people in Qatar. This echos the findings from earlier chapters.
3. Using the media as a channel for public awareness is very effective in passing the message on to a large number of people.

Some quotes from the interviewees after the show are *'It was an interesting TV show'*; *'I was amazed how phishers could deceive people to disclose their confidential information'*, *'I have become more aware and cautious after the show'* and *'I learned a lot of tips and clues on how to avoid phishing'*. Overall, the television experience showed the power and effectiveness of television as an education medium.

The advantages and disadvantages of each method in the framework is provided in Table 9.5 so that the user can decide when and where to use each method in the

framework according to the requirements and available resources. This analysis was based on available literature, views of experts in the field and the public, along with the researcher's experience from running each part of the framework.

Table 9.5: Advantages and disadvantages of each method in the framework

Training methods	Advantages	Disadvantages	Where applicable
Contextual training	<p>Measures the ability to distinguish phishing attempts from legitimate ones in a laboratory experiment. Allows trainers to measure false positive and false negative rates.</p> <p>Enables assessment of vulnerability to different phishing techniques</p> <p>Enables the study of behaviour while training to identify factors which make participants vulnerable to phishing.</p> <p>Full interaction between learners and trainers.</p>	<p>Requires users' motivation to involve them in such training</p> <p>May not give reliable results since users may be more cautious regarding phishing because they are in a training session (Herzberg, 2008).</p> <p>Requires special set up and careful selection of training questions on both legitimate and phishing e-mails, trying to cover different phishing techniques and tricks</p>	<p>In organisations needing to enhance their employees' awareness of the phishing threat or for academic research</p>
Embedded training	<p>A well designed penetration test will assess peoples' ability to recognise phishing attempts during their daily activity.</p> <p>Provides effective training since it is related to real world testing (Anderson and Simon, 1996)</p> <p>Gives a better understanding of users' behaviour during day-to-day online activities (Herzberg, 2008)</p> <p>Only people not able to recognise phishing attempts will receive automatic training materials.</p> <p>Less expensive to run for large number of people.</p> <p>Requires less teacher effort.</p> <p>Helps to overcome users' overconfidence in their own ability</p> <p>More motivating than regular learning messages (Kumaraguru et al., 2007)</p> <p>High knowledge retention compared to regular phishing alert messages (Alnajim and Munro, 2009; Kumaraguru et al., 2007).</p>	<p>Requires some form of approval to be carried out</p> <p>Ethical and privacy issues should be considered</p> <p>Might create distrust amongst people who have been tested</p> <p>Such penetration tests might be ignored in the future if used too frequently</p> <p>Requires user recognition to gain acceptance such as awarding a certificate, and giving promotions and praise for those who have not fallen in training.</p> <p>No full interaction between learner and trainers - trainers must base results on the number of people who fail the test</p> <p>Can only test a limited number of different phishing techniques due to sensitivity of such training</p>	<p>In organisations needing to enhance their employees' awareness</p>
E-learning	<p>Provides flexible and accessible learning (Zenger and Uehlein, 2001; Web-based Training Cookbook, 1997: 108).</p> <p>Applies new learning technology and reduces learning time requirements (Miller, 1990).</p> <p>Less expensive than traditional learning because does not require teachers or classrooms.</p> <p>Raises learning knowledge and retention</p>	<p>Missing personal learning experience</p> <p>Users require a computer and Internet access</p> <p>Requires some programming and designing knowledge to set up</p> <p>Users may not understand fully the training material and they can not get help immediately, unless there is an effective live support service (Kumaraguru et al., 2007)</p>	<p>Suitable for global public awareness</p>

Chapter 9: Evaluation of the Educational Framework

	(Fletcher, 1991: 33-42; Fletcher, 1990) Will reach potential victims worldwide more quickly	Requires consideration of many issues in the design, such as security, privacy and usability.	
Media programme	Will reach large numbers of people locally and internationally. Engages people in discussions and can involve other people's experience through vox pop and other techniques. Very passive and entertaining way of learning Enhances awareness effectively and make it easy to remember because of its visual nature People tend to trust national and respectable television channels	Requires a contact and cooperation with media channels Some argue that media might not affect user behaviour (Wilson and Wilson, 2001; Spitzer, 1993; Windahl et al., 1992: 102; Wimmer and Dominick, 1991) Expensive to set up, requires special expertise in filming, using a camera, presenting, etc. Requires being more aware of what you are saying (i.e. not to be offensive or biased).	Suitable for public awareness locally and internationally
Session			
Poster	Portable High resolution image Relatively cheap compared to media Issue presented in simple form and focuses on passing a specific message in a simple way Pleasant to view, attractive	Easy to get damaged May not have high educational value or function because issues are not covered in detail Requires placement in a proper place or an organisation to support its distribution Not all people will be attracted by all posters, most posters would need to target a specific group Needs careful design to reach the maximum number of people and to pass the message clearly Hard to get people's feedback	Suitable for public awareness, particularly suitable for people who regularly visit certain places, for example children visiting schools
Quizzes and Games	Exciting, interactive and will effectively raise knowledge and retention for users (Zhang et al., 2007; Quinn, 2005; Repenning and Lewis, 2005; Gee, 2003). Understandable and easy to remember (Mayer, 2001; Klein, 1999). Uses fun in applying learning	Requires expertise in programming and animation Can require special software to run the game Tends to be of interest to young people more than adults and older people.	Suitable for organisations and the academic sector, especially for young people
Seminar	Good for large groups Can be accompanied by oral or recorded presentations Can use a variety of different media and methods in the seminar Can get lot of information across in short time It can work on enhancing knowledge through interaction and discussions Gives an opportunity to get users' qualitative feedback.	Somewhat expensive as labour intensive Some could find it relatively uninteresting Teachers require communication skills and learners require listening skills Requires good material Needs a means to get people together and venue Everybody needs to be available at the same time	Suitable for organisations and the academic sector
Cartoon	Passes message in an informal, funny way. Requires imagination to create the drawings Inexpensive to produce Quite fun and interesting Can contain a conversational form and	Requires drawing and special skills Tends to link to previous knowledge a user is presumed to have which may not be the case Expensive to distribute in widely read media The message is limited in length in a	Suitable for public awareness

	story board Humour is a powerful rememberable message.	cartoon	
Booklet	Gives information about something in brief in a handy form. Cheap to produce Can contain more information Particularly useful as reference material Effective to make people aware of subject if information is understandable and brief.	People may treat it as junk mail and therefore may not pay attention to the message. Can be time consuming to design and distribute Information can become outdated since it is hard to make changes once printed. Hard to get people's feedback on it Too much information would lead people to forget	Suitable for public awareness

9.6 Summary

This chapter has discussed the awareness framework which consists of multiple training methods. The framework was developed with the assistance of experts in the field of e-crimes and awareness. These experts stressed the importance of making people aware of phishing without intimidating them, creating a framework associated with Qatar and taking into account people's background and the factors which make Qataris vulnerable to phishing. The different educational materials developed in the previous chapters were all used as part of the framework.

In conclusion, the qualitative and quantitative evaluation shows the obvious effectiveness of the awareness educational framework in enhancing people's awareness level on the e-mail phishing problem and their vulnerability to such attack and even in increasing the users' ability to retain the knowledge learned even after a period of four months. These findings support the outcomes of Kumaraguru et al. (2007), Merrienboer et al. (1997) and Sheng et al. (2007) show that those users who were taught how to recognise phishing attempts were better able to remember and distinguish phishing after the training.

The learning session was able to draw on most of the different components of the framework, showing the value of such a multi-channel approach. This suggests that the framework should not be used simply to select the best method of awareness education for a given situation but that it would be better to use a selection of educational

methods. The advantages and disadvantages of each framework component are listed to help guide users when and where to use each educational method in the framework depending on their individual circumstances and resources.

Embedded training, sessions and e-learning were found to be more effective than contextual training due to the direct interaction between learners and tutor and the fact that people learn and remember better when they face the real attack than when reading a piece of information. This agrees with other research (see literature review, Section 2.5.2.2). Similarly, using the media to enhance public awareness was found by a number of evaluators to be very valuable in reducing the risk of phishing in Qatar, despite the obvious cost.

The next chapter presents conclusions and suggests future work.

Chapter 10 Conclusions and Future work

This concluding chapter presents the research contributions and implications, achievements and limitations and, finally, a summary of findings and suggestions for future work.

10.1 Research contributions and implications

The research provides a significant contribution to knowledge by shedding light on the e-mail phishing problem in a particular area of the world which has not been covered before in the literature, which is the State of Qatar. The research contributes by establishing the existence of the problem, its extent, addressing the factors which make Qatari citizens vulnerable to e-mail phishing threat, including the cultural and country-specific factors, and defining an e-mail phishing awareness and educational framework to help in reducing the danger of such threat in Qatar. The framework will help the Qatari government and organisations in enhancing people's awareness of the e-mail phishing threat through a set of useful recommendations and effective educational methods. The research is beneficial for the target groups (Qatari Government, citizens and organisations responsible for ensuring information security) to enable them to help preserve the security and privacy of Qatar and its inhabitants and reduce the level of e-crime, in particular phishing, in the state. Many of the ideas would be helpful for e-mail users, e-mail research scholars, and researchers on e-mail phishing and awareness, especially in those countries with a culture similar to Qatar's such as the Gulf Co-operation Council (GCC) and Arab countries.

On a personal level, the research was challenging and intellectually stimulating. It has also made a major contribution in improving the researcher's knowledge professionally, academically and personally in many aspects, including researching, problem solving, communication skills, oral and writing skills and gaining further expertise in the field of information security, in particular, phishing. Furthermore, the researcher has had an

enjoyable experience in being in a television show and holding some real-life experiments and carrying out an awareness programme with young Qataris, not without surprises, on meeting face-to-face with some current practising and committed teenage phishers. In addition, the researcher was led to empirical investigation of the implication of Qatar culture for people's responses to phishing threat, which was a challenging and exciting field, not discussed before in the literature. This research will make a valuable input in the researcher's forthcoming professional work of being responsible for ensuring network security in an organisation where phishers will inevitably try to breach by targeting people since they are considered to be the weakest link of the security of their organisation. Therefore, making people aware of phishing would enhance their trust decisions when the technological defences fail as often users tend to over trust technology.

10.2 Research Achievements

The research aim and objectives (see Section 1.6) were achieved in this thesis through empirical and non-empirical research in Qatar by a case study of the e-mail phishing problem and also, for comparison, in the UK, as an example of a developed country. The research followed a carefully planned progression through the intended objectives which built on each other, coming finally to fulfilling them by proving the existence, extent and danger of the e-mail phishing problem in Qatar, a fertile ground for phishers. It also, addressed the factors which make Qataris vulnerable to e-mail phishing where awareness was found to be weak and therefore proposed for target groups some effective recommendations and an awareness framework to help reduce the problem in the State of Qatar.

10.3 Research Limitations

Due to the limitation of resources, the researcher was not able to implement the proposed recommendations in reality. However, the recommendations were tested by using the opinion of experts from a range of private and government organisations in the field of e-crime, Qatar culture and law, awareness and education.

The researcher was unable to extend the educational programme to a large number of Qatari citizens, due to difficulties in obtaining authority for access and enough funds and support from responsible organisations.

There were also major difficulties in getting authority from organisations for holding a penetration test for phishing for ethical, security and privacy reasons. Even when authority was granted, the collaborating organisation still required full control over the test to ensure its privacy. However, giving the authority to do such a test was a significant concession on the part of the organisation.

Furthermore, respondents' reluctance to contribute to the research by participating in interviews, surveys and experiments was a further constraint. However, the researcher tried to take positive steps to encourage people to participate, for instance by motivating them by using successfully the previously mentioned tried and tested 'chocolate method' and taking advantage of personal contacts with families and friends.

Also, the research was limited in comparing the survey outcomes for Qatar and the UK which shows a clear difference in the awareness level of the people, the UK being more aware. However, it would have been useful to take the comparison further between both countries in the other research methods, including the experiments, but due to the lack of resources and access to organisations as well as the time constraint, the researcher was unable to provide a complete cross-cultural comparison on phishing and people's vulnerability to it.

10.4 Conclusion

This thesis shows the existence and extent of the e-mail phishing problem in Qatar. Also, it shows that there are many factors which make Qatar an attractive place for phishers since there is availability of money and victims, with no obvious e-law to

protect them. This view was supported by experts as well, which shows that the phishing problem exists in the region and has become significant. There is a readiness by the government and responsible organisations to solve this problem in spite of some difficulties encountered, for instance in tracing phishers and persuading victims to report incidents. Most experts stated that Qatari citizens are susceptible to phishing due to multiple factors but mainly the lack of awareness of it.

The surveys of Qatari and UK e-mail users provided a profile of their awareness of e-mail phishing and their views on the best method of defence against this attack. The questionnaire addressed the knowledge of e-mail phishing, the vulnerability of participants, the extent of e-mail phishing and the defences used against it. Responses in Qatar illustrate that a phishing problem exists, is increasing and that phishing is very successful because citizens are commonly vulnerable to e-mail phishing attack. There are many reasons for this, mainly resulting from the lack of awareness of the phishing threat. The research found that the questionnaire responses regarding the e-mail phishing level of knowledge, the use of anti-phishing software and the reasons for being tricked were similar in both Qatar and the UK. However, other responses were significantly different, indicating a much higher vulnerability to phishing in Qatar than in the UK.

The penetration tests confirmed that Qataris are indeed vulnerable to e-mail phishing. It is of particular concern that about half of the people tested were incapable of distinguishing phishing attacks, indicating a need to enhance the state of awareness of e-mail phishing for Qataris. The tests have demonstrated that Qataris are particularly susceptible to e-mail phishing when it exploits their interest, emotions, beliefs and religion, especially when deployed in religious seasons. Discussions with the participants indicate that Qataris tend to trust phishing e-mails in their native language rather than in English, they have overconfidence in e-mails that appear to come from official and trustworthy institutes in Qatar and they believe that phishing will be limited to certain topics and especially do not expect e-mail phishing to be connected with religion.

Qataris live in a conservative society committed to its culture and, as a result, their response to e-mail phishing has been found to be affected by the culture of Qatar which is influenced by the customs, traditions and religion which play a big role in people's life. In conclusion, Qataris were found to be vulnerable to e-mail phishing attacks because of multiple factors: the culture, country-specific factors, religion, interest, beliefs, as well as personal characteristics.

The research shows a clear lack of awareness on how to detect, react and protect against phishing. For example, some Qataris have overconfidence in the reliability of anti-virus software to detect all phishing attempts, some do not install spam filters and some open e-mails from unknown senders and junk mail. The overconfidence and trustfulness of the Qatari people is likely to be a result of the new found oil wealth in the State of Qatar which, in turn, has led to a rapid growth in the use of technology and the Internet. While education levels are also rapidly increasing in the country, there is clearly a lack of maturity in the knowledge of phishing crime that is a threat to the security of systems in Qatar and the privacy of its people.

Recommendations then emerged from grounded theory based on the findings from the research carried out in the field. Recommendations were defined for the Qatar government, citizens and organisation officials responsible for providing information security to diminish the e-mail phishing threat in Qatar. According to a sample of Qatari citizens and experts from Qatar and the UK in the field of e-crime and Qatar law and culture, the recommendations were considered to be effective in reducing the risk of e-mail phishing in the State of Qatar. Although some of the recommendations are on the way to realisation, such as the establishment of an efficient e-law, some difficulties were identified which might be faced in the enforcement of the law and in getting cooperation from citizens, national and international institutes and other governments, especially from unstable countries such as Nigeria. Some obstacles, which might be faced in implementing the recommendations, are the requirement for resources, the need for support from government and other institutes, and the preference of Qatari citizens

to react to incidents rather than reporting and documenting them, which has led to difficulties in building a record of phishing incidents within organisations.

The evaluators agreed on the need for applying an effective awareness and educational framework to enhance public awareness of the phishing threat in Qatar, especially through the media. This then led to the development an e-mail phishing educational framework which involved different training methods, including embedded training, contextual training and a learning programme incorporating a television programme and an educational session with e-learning. The use of this framework was found to be effective in raising awareness of and defence against the phishing threat in Qatar since an average improvement was detected in people's knowledge of and vulnerability to phishing threat and this was mostly retained even four months afterwards.

The success of the framework raises the question of whether it might also be valuable to other citizens of a similar culture, e.g. in the GCC countries, and in developed countries such as the USA and the UK, where there might be cross-cultural considerations. Some of the factors are likely to be common to other countries, such as the value of the penetration test, but some aspects are particular to Qatar, such as its rapid development and country-specific factors. Other countries need to consider each point of the proposed framework in their own environment.

10.5 Suggestions for Future work

Although this research has had some significant success, there is considerable scope for further work. Suggestions are as follows:

1. Verifying the findings

Although the number of participants in the surveys undertaken is large, it would still be useful to increase the sample size to obtain more reliable results and reduce the margin of error. It would also be useful to verify the findings of the various tests as, in many

cases, the number of participants was small and often a convenience sample. Carrying out penetration tests and laboratory tests on more people would give greater confidence in the results, though this would be difficult because of the authorisation and permissions needed and the ethical constraints on such tests.

2. A long term study of the applicability of the research

The recommendations in this thesis and the awareness framework developed have been tested as far as it is possible within the time constraints of a PhD project. Ideally, the research needs to continue over a long period to see the effects of the recommendations and framework being put into practice in the State of Qatar. This research would require the cooperation of the government and other institutions to apply the recommendations and awareness framework so the effects can be studied. This is clearly well beyond the scope of a PhD research project.

3. Further investigation of cultural and country specific factors

This research has revealed that cultural and country-specific considerations are important factors affecting the Qatari's vulnerability to phishing. Factors identified included the trusting nature of the Qatari people particularly in the religious seasons and the rapid adoption of technology which has left most Qataris unaware of the dangers involved. The discovered factors which make Qatari citizens vulnerable to phishing give only a general guide and other factors or influences may be found, particularly where the influences overlap in the areas mentioned in the previous section. It would be interesting to find if there are other cultural and country-specific factors and whether these affected some parts of Qatari society more than others. More sociological investigation and studies of human behaviour may reveal other characteristics not covered in this research.

4. A business plan for the implementation of the recommendations and framework

A more thorough evaluation of the viability of the proposed recommendations and awareness framework is suggested as future work to motivate the government and responsible and targeted bodies to bring them into reality. This would require estimates of the costs of implementing each recommendation and framework component, and estimates of the cost savings these would bring over the short and long term. All

stakeholders who would benefit would need to be identified and the costs and benefits for each one would need to be estimated. This would take considerable investigation that would not be possible to achieve within the scope of a PhD project, yet it would be exceedingly useful to motivate the government and other bodies to implement the recommendations and awareness framework proposed in this research.

5. Further examples of each component of the framework

Each component of the framework developed in this research was tested by examples. However, there was only one example of many of the components. For example, there was only one booklet produced and only one television show broadcast. While these were both successful, further research would be necessary with different variations of each aspect of the framework to discover what type of booklet is best, what format of television programme is most effective, etc. Such an analysis would be very extensive and would require far more than a PhD project to fully investigate.

6. Extending the framework

The ideas for the framework were derived from the literature and from the survey findings. However, the framework is unlikely to contain all possible awareness methods. For example, some “pop” stars have sometimes sought to include a message in their songs (e.g. John Lennon’s song “Give Peace a Chance”). This is just one possible way in which an awareness message can be spread. This research has investigated and tested some of the more common ways of educating people, but further research could extend the framework to the many other ways in which awareness could be promoted. Investigating the possible extensions to the framework and testing each one would require considerable research and would require many PhD projects to do so.

7. Comparison with other countries

In this research, some comparison has been made with the UK as an example of a developed country. However, it would be useful to know what factors affect other countries and whether the many cultural and country-specific factors can be found elsewhere. Similar surveys in other countries are suggested to measure people’s level of awareness of the phishing threat and discovering the factors which make people susceptible to such attack. It would be helpful to compare Qatar with other countries in

the region such as the Gulf and Arab countries, and with countries in completely different regions to get a better understanding of the influences of the cultural and country-specific factors.

8. Investigating the applicability of the framework in other countries

The recommendations and awareness framework developed has been specifically designed for Qatar. However, it is likely that many of the recommendations and parts of the framework would be applicable in other countries. It is likely that the Gulf States would have similar conditions that would make most of this research applicable but it is uncertain how much would be applicable in other parts of the world. The various different components of the framework could be tested in a number of different countries to discover what parts of the framework work well in different countries and this would also help identify the conditions that would make each component and recommendation applicable. This further research would then help other countries decide how to apply the recommendations and framework themselves.

9. Incorporating m-learning into the framework

The developed educational materials could be presented not just as e-learning but also as m-learning, or ‘mobile learning’ which provides more accessibility for learners by taking advantage of the learning opportunities offered by mobile technologies. There are many researchers of m-learning who have claimed its effectiveness and the need to move towards such technology with the small screen size of the mobile phone (Moore, 2009; Maniar et al., 2008; Masters and Ng'ambi, 2007; McConnetha, 2007 ; Savill-Smith et al., 2006; Naismith et al., 2005; Sharples, 2000). Further work is suggested to test and evaluate awareness methods through m-learning in Qatar and elsewhere to see whether it could be an appropriate part of the awareness framework. Furthermore, as other technologies develop, it will be necessary to carry out research on each new development to find the best way to apply the new technology.

10. New tool development

Since it was discovered that people’s awareness might decay with time after attending an awareness programme, it is suggested that a tool should be developed for enhancing people’s phishing awareness instantly on interacting with an e-mail system. The tool

could be embedded into the email system so it could detect the wrongful action of a user, such as sending an email with their password in the text, and then display some education material to make the user aware of the danger. Such a tool would take a significant development and research would be needed to determine how to detect an incorrect user action and the most appropriate educational material to display.

10.6 The Success of this PhD Research

Although this research is a first step in uncovering e-mail phishing problems in the State of Qatar, there is still scope for future work in extending investigations. However, the research was very successful since the aims and objectives were achieved. Although there were some limitations, they were not serious and some were tackled.

The research has been shown to be original and to make a valuable contribution to knowledge, particularly in relation to Qatar. Perhaps the greatest test of the success of the research is whether the results will be used. In this research, several of the ministries of the Qatar government have shown interest in its results and are planning to take it forward into implementation.

Appendix A: Questionnaire

A1 First version of questionnaire in English

Phishing Survey

Aim: This survey will gauge people's awareness of e-mail phishing and the best way to defend against such attacks. You are now going to be asked 20 simple questions particularly about phishing e-mails

Q1: General information

A. Your country

B. Gender

- Male Female

C. Age

- Under 18 18-29 30-49 Over 50

D. Education level

- School Further Education Higher Education
 Postgraduate Others, please specify

E. Occupation

- Student Business man Unemployed
 Employee, please specify your job title

Q2 Do you have an e-mail address?

- Yes No

If your answer is Yes, then please answer Q3

Q3. How often do you open your e-mail?

- More than once a day Once a day More than once a Week
 Weekly Monthly Very rarely Not at all Others, Please Specify

Q4: How well do you know about phishing?

- None Poor Average Good Expert

Note: Phishing is a criminal fraudulent process. It attempts to gain sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy party in an electronic communication. Phishing is usually carried out by e-mail and often directs users to enter details at a fake website which looks and feels almost identical to a real one.

If you answer to Q4 is None, then please skip Q5

Q5: From where do you know about phishing?

- Internet Media (e.g. TV, newspapers, magazines) Employer
- Friend Others, please specify

If your answer is Employer, then please answer Q6.

Q6: How do you learn from your employer about phishing?

- Set of guidelines
- Awareness and training program
- Others, please specify

Q7: Which of the following is generally NOT a sign that an e-mail may be fraudulent?

- It asks you to click a link in the e-mail message to enter information about your account.
- It conveys a sense of urgency and surprise
- It addresses you by first and last name.
- Security certificate for site matches name of site.
- It asks you to verify some personal information.
- Website's URL starts with https

Q8: You receive an e-mail from your bank asking you to phone a number given in it, Do you.....?

- Phone the number
- Check to ensure it is your bank's real number
- Delete the e-mail

Q9: Do you worry about phishing?

- Yes No

Q10: Do you think e-mail phishing incidents in Qatar or UK have?

- Increased Decreased Same Don't know

Q11: How often do you receive phishing e-mails?

- Very often Sometimes Very rarely Don't know

Q12: How many times have you been tricked by phishing e-mails?

- 1-5 5-10 More than 10 None Don't know

If you answer Q12 None, then please skip Q13, Q14.

Q13: If you have been tricked with phishing e-mail, what was the reason? Please select from the following list:.

- Didn't install anti-phishing or anti-virus software to detect phishing e-mails
- Phishers are coming up with smarter and smarter tricks that make identifying phishing e-mails difficult.
- They came up with sense of urgency, surprise and morality
- I trusted it
- I didn't know about phishing before
- Lack of awareness and training about phishing (e.g. What does it look like? What's its threat? How do you resist it?)
- It directed me to enter details at a fake website whose look and feel were almost identical to the legitimate one
- I didn't believe I would be tricked
- Others, please specify

Q14: If you have been attacked with phishing e-mail, what was the impact of loss from the attack?

- Financial loss, please state roughly how much
- Amount lost Currency (Note: please use US\$ or QR)
- Confidential information, please specify what type
- Others, please specify
- Don't know

Q15: Which of the following actions should you take if you think you've been tricked by a phishing scam?

- Report it to the company whose e-mail address or Web site was forged
- Report it to the police
- Change the passwords on all your accounts
- Check your financial statements immediately
- Cut up your credit and debit cards
- Do nothing
- Others, please specify

Q16: Do you use a product or tool to detect or protect against e-mail phishing, e.g. antivirus and anti-phishing software?

- Yes, please specify the product or the tool you use
- No

Q17: What is the most important feature you would like the anti-phishing product or tool to have in order to prevent phishing e-mails?

- Detect phishing e-mails by just pointing on the link (without having to go to the actual site).
- Give positive confirmation that you are at the right site
- Block phishing e-mails
- Protect your password from being captured by keyboard Trojans
- Others, please specify

Q18: What do you think is the best way to defend against e-mail phishing?

- Have an effective anti-phishing product or tool to detect and prevent phishing e-mails
- Define clear and reasonable guidelines addressing phishing (e.g. Don't give your password through the e-mail, check the sender e-mail address, etc.)
- Provide an educational program consisting of awareness and training to alert people to the phishing threat and teach them how to resist it.
- Carry out penetration testing, because I will learn more when I encounter or am affected by a phishing e-mail (i.e. A fake phishing e-mail will be sent to your e-mail, the e-mail will not harm you as it is only to measure your response to phishing e-mails and to educate you)
- Others, please specify

Q19: Regarding the educational programme, which tool or method do you think is effective to deploy awareness and training against e-mail phishing?

- Newsletters and documents
- Pub-up screens and Screen savers
- Presentation slides
- Posters
- Cartoons
- Videos
- Interactive anti-phishing games (e.g. Computer-based game)
- Penetration testing, because I will learn more when I encounter or am affected by a phishing e-mail
- Others, please specify

Q20: By what means do you prefer the education tools to be embedded?

- Traditional education, paper-based
- Regular seminars with speakers
- Stand alone application (e.g. educational program embedded in your desktop with screen saver and pop-up screens to regularly remind you of how to resist phishing attacks)
- E-mails (i.e. regularly send educational programs to your e-mail)
- False phishing e-mails, designed to test your response to phishing attacks and educate you against phishing (e.g. A fake phishing e-mail will be sent to you. Once you have been tricked and you have clicked on the URL to enter your private information, it will immediately point you to the educational site to teach you about phishing)
- Media (e.g. TV, newspapers)
- Web-based e-learning (i.e. Having an online educational program containing all of the educational tools and materials)
- Others, please specify

A2 Questionnaire after first review

E-mail Phishing Awareness Survey

Note: The following shapes mean: Choose **one answer only** Can choose **more than one answer**

Q1: What is your level of knowledge about e-mail phishing, also called scam, spam, spoofing or fraud e-mails?

- None Poor Average Good Expert

If you answer Q1-None, then please skip Q2

Q2: How do you know about phishing?

- Internet Media (e.g. TV, newspapers) Employer School or university
 Others

Q3: Do you think e-mail phishing incidents are?

- Increasing Decreasing Staying the same Don't know

Q4: Do you worry about e-mail phishing?

- Yes No

Q5: Which of the following is generally a sign that an e-mail may be phishing or fraudulent? You receive an e-mail from your bank which....

- Asks you to enter information about your account (e.g. Your username and password)
- Addresses you by your first and last name (e.g. Dear Ms. Mariam K Al-Hamar).
- Directs you to a website containing a security certificate that matches the name of the website.
- Conveys a sense of urgency and surprise (e.g. You have won \$1million in the raffle, enter your account details now)
- Has been classified as junk or spam mails by your e-mail system.
- Contains an attachment notifying you that it might contain viruses that could harm your computer.
- Points you to a website with a URL that starts with https.
- Asks you to phone a number given in the e-mail.
- Don't know

Q6: Which of the following actions should you take if you think you've been tricked by a phishing e-mail?

- | | |
|--------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| <input type="checkbox"/> Report the incident to the company whose e-mail address or Web site was faked. | <input type="checkbox"/> Change the account details that you have revealed |
| <input type="checkbox"/> Report the incident to the police or an institute that specialises in dealing with these cases. | <input type="checkbox"/> Check your financial statements immediately |
| <input type="checkbox"/> Report the incident to your bank or other organisation for which you have revealed details. | <input type="checkbox"/> Cut up your credit and debit cards |
| | <input type="checkbox"/> Do nothing |
| | <input type="checkbox"/> Others <input type="text"/> |

Q7: How often do you receive phishing E-mails?

- I don't have an E-mail Daily Weekly Monthly Never Others

If you answer Q7: I don't have an E-mail or Never, then please skip Q8 and Q9.

Q8: How many times have you been tricked with phishing E-mails?

- Never Once Twice 3 times More than 3 times Don't know

If you answer Q8: Never, then please skip Q9.

Q9: If you have been tricked with a phishing e-mail, what was the reason you were tricked?

- | | |
|---------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| <input type="checkbox"/> I didn't install a software to prevent phishing e-mails and websites(e.g. anti-virus, anti-phishing, spam filters) | <input type="checkbox"/> The e-mail came up with a sense of urgency and surprise |
| <input type="checkbox"/> The phishers are coming up with smarter tricks which make it difficult to identify phishing | <input type="checkbox"/> Lack of awareness and training about phishing |
| <input type="checkbox"/> The fake website looks almost identical to the legitimate one | <input type="checkbox"/> I trusted the e-mail because I didn't know about phishing |
| <input type="checkbox"/> I didn't believe I would be tricked | <input type="checkbox"/> I was not aware of the importance of the information that I revealed |
| | <input type="checkbox"/> Other <input type="text"/> |

Q10: Do you use software to protect you from phishing e-mails and websites (e.g. anti-virus, anti-phishing software or spam filters)?

- Yes No

Q11: Do you think using anti-virus, anti-phishing software or spam filter is enough to prevent all types of phishing e-mails?

- Yes No, please specify why
- Don't know

Q12: What do you think is the best way to defend yourself against phishing E-mails?

- Be aware and be educated about phishing
 Follow clear guidelines addressing phishing (e.g. Check the web address, Don't give your private information through the e-mail.etc)
 Install effective anti-virus, spam filter or anti-phishing software
 Get affected by phishing e-mails, because I will learn more
 Others

Q13: How do you prefer to be educated about phishing, Is it by....?

- Interactive tutorials and quizzes
 Videos
 Cartoons
 Posters
 Web-based e-learning
 Media
 Seminars
 Newsletters and documents
 Screen savers
 Others

Q14: About yourself**A. Gender**

- Male
 Female

B. Age group

- Under 18
 18-29
 30-49
 Over 50

C. Education level

- School
 Further or Higher Education
 Post Graduate
 Others

D. Occupation

- Student
 Businessman
 Employee, please specify your job
 Others

E. Country

F- Your e-mail address (If you would like to receive educational material about Phishing)

A3 Questionnaire final version (after pilot-test)

Covering letter

Dear Fellow Citizen,

I am a PhD student at Loughborough University in the UK and I am doing my research on “e-mail Phishing” That is a criminal fraudulent process that attempts to gain sensitive information such as usernames, passwords and credit card details by pretending to be a trustworthy party in an electronic communication such as an e-mail. It has become increasingly important as all of us are threatened financially and personally by the menace of e-phishing.

I have designed a questionnaire to see how aware people are about e-mail phishing and how to defend against it. This questionnaire is intended only for Qatari or British citizens who have an e-mail. Therefore, if you are one of them, please help us by completing the questionnaire, otherwise just ignore it. It is important that participants answer the questionnaire honestly.

The questionnaire will take no more than 5 minutes of your time to complete. I hope you will contribute. It is intended to use the results in developing training materials so people can become aware of the crime of e-phishing and learn to protect themselves against e-phishing attacks

Please bear in mind that participants should be only Qatari or British citizens who use e-mail. I assure you that all responses will be confidential and kept private.

Thank you in anticipation of your involvement.

Yours sincerely,

Mariam Al-Hamar

For any questions about the research topic please do not hesitate to contact me by e-mail: m.k.j.al-hamar@lboro.ac.uk.

E-mail Phishing Awareness Survey

Note: The following shapes means: Choose **one answer only** Can choose **more than one answer**

Q1- Gender

Male Female

Q2- What age group are you in?

Under 18 18-29 30-49 Over 50

Q3- Education level

School Further or Higher Education Post Graduate Others

Q4- Occupation

Student Business man/ woman Employee, please specify your job title

Others

Q5- Nationality

Q6-Do you have an E-mail?

Yes No

Q7- Your E-mail (If you would like to receive an educational material about "Phishing")

Q8: How well do you know about E-mail Phishing, it is also called (Scam or Fraud E-mails)?

None: Don't know anything about e-mail phishing.
 Poor: Have heard of e-mail phishing.
 Average: Knows the term e-mail phishing and understand its simple techniques
 Good: Knows the term e-mail phishing, understand more about its techniques and how to protect against it.
 Expert: Knows the term e-mail phishing; understand more about its complex

None Poor Average Good Expert

If you answer Q8-None, then please skip Q9

Q9: From where do you know about phishing?

Internet Media (e.g. TV, newspapers) Employer School or university

Others

Q10: How frequent do you think e-mail phishing incidents are?

- Increasing Decreasing Staying the same Don't know

Q11: Do you worry about e-mail phishing?

- Yes No

Q12: Do you use software to protect you from phishing e-mails and websites (e.g. anti-virus, anti-phishing software or spam filters)?

- Yes No

Q13: Do you think using anti-virus, anti-phishing software or spam filter is enough to prevent all types of phishing e-mails?

- Yes No, please specify why
- Don't know

Q14: Which of the following is generally a sign that an e-mail may be phishing or fraudulent? You receive an e-mail from your bank which....

- Asks you to enter information about your account (e.g. your username and password)
- Addresses you by your first and last name (e.g. Dear Ms. Mariam K Al-Hamar).
- Directs you to a website containing a security certificate matching the name of the website.
- Conveys a sense of urgency and surprise
- Has been classified as junk or spam mail by your e-mail system.
- Contains an attachment notifying you that it might contain viruses that could harm your computer.
- Points you to a website with a URL starting with https.
- Asks you to phone a number given in the e-mail.
- Don't know

Q15: Which of the following actions should you take if you think you've been tricked by a phishing e-mail?

- | | |
|----------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| <input type="checkbox"/> Report the incident to the company whose e-mail address or Web site was faked. | <input type="checkbox"/> Change the account details you have revealed |
| <input type="checkbox"/> Report the incident to the police or an institute specialising in dealing with these cases. | <input type="checkbox"/> Check your financial statements immediately |
| <input type="checkbox"/> Report the incident to your bank or other organisation for which you have revealed details. | <input type="checkbox"/> Cut up your credit and debit cards |
| | <input type="checkbox"/> Do nothing |
| | <input type="checkbox"/> Others <input type="text"/> |

Q16: How often do you receive phishing E-mails?

- Daily Weekly Monthly Never Others

Q17: How many times have you been tricked by phishing e-mails?

- Never Once Twice 3 times More than 3 times Don't know

If you answer Q17 Never, then please skip Q18.

Q18: If you have been tricked by a phishing e-mail, which of the following was the reason you were tricked?

- | | |
|----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| <input type="checkbox"/> I didn't install a software to prevent phishing E-mails and websites (e.g. anti-virus, anti-phishing, spam filters) | <input type="checkbox"/> The e-mail appears with a sense of urgency and surprise |
| <input type="checkbox"/> Phishers are coming up with smarter tricks which make it difficult to identify phishing | <input type="checkbox"/> Lack of awareness and training about phishing |
| <input type="checkbox"/> The fake website looks almost identical to the legitimate one | <input type="checkbox"/> I trusted the e-mail because I didn't know about phishing |
| <input type="checkbox"/> I didn't believe I would be tricked | <input type="checkbox"/> I was not aware of the importance of the information that I revealed |
| | <input type="checkbox"/> Other <input type="text"/> |

Q19: What do you think is the best way to defend yourself against phishing E-mails?

- | | |
|------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| <input type="checkbox"/> Be aware and be educated about phishing | <input type="checkbox"/> Install effective anti-virus, spam filter or anti-phishing software |
| <input type="checkbox"/> Follow clear guidelines addressing phishing (e.g. check web address, don't give your private information in an e-mail.etc.) | <input type="checkbox"/> Get affected by phishing e-mails, because you will learn more |
| | <input type="checkbox"/> Others <input type="text"/> |

Q20: How do you prefer to be educated about phishing, Is it through.....?

- Interactive tutorials and quizzes Videos Cartoons Posters Web-based e-learning Media Seminars Newsletters and documents Screen savers
- Others

A4 Electronic version of questionnaire in Arabic and English

Dear Sir/Madam

I'm PHD student in Loughborough University, UK. I'm doing my research on "E-mail Phishing", I have designed a survey to see how people are aware about E-mail Phishing and how to defend against it.

The survey won't take more than 2 minutes of your time. Click on the URL below to participate in the survey.

<http://co-project.lboro.ac.uk/users/comkja/Survey-Eng.html>

I hope you would contribute and send it to your contact list to gather more people.

Note: If the link doesn't work, please copy the link into your explorer and you will see the survey

Thanks a lot

Mariam AL-Hamar

PHD student

السلام عليكم ورحمة الله وبركاته
أحيتي في الله

أن الله في عون العبد ما دام العبد في عون أخيه

. أنا طالبة دكتوراه في جامعة لفيريا في المملكة المتحدة. موضوع رسالتي عن تصيد المعلومات بالبريد الإلكتروني

. حالياً أقوم بمسح استبياني لمعرفة مدى وعي الناس عن تصيد المعلومات بالبريد الإلكتروني وكيفية التصدي لها

. الاستبيان لن يأخذ أكثر من دقيقتين من وقتك. اضغط على الرابط بالاسفل إذا كنت ترغب في المشاركة.

<http://FreeOnlineSurveys.com/rendersurvey.asp?sid=02vg2iwopywxgfd578765>

ارجو المشاركة والتكرم بنشر الاستبيان الى قائمة بريدك ولكم جزيل الشكر

ملاحظة: إذا الرابط لايعمل انسخ الرابط في المتصفح واضغط انتر وسيظهر لك الاستبيان

E-mail Phishing Awareness Survey

Free Online
Surveys.com

* **Q1: How well do you know about E-mail Phishing, it is also called (Scam, Spam, Spoofing or Fraud E-mails)?**

None Poor Average Good Expert

If you answer Q1-None, then please skip Q2

Q2: From where do you know about E-mail Phishing?
You can choose more than one answer

Internet Media (e.g. TV, newspapers) Employer School or university
 Others please specify

* **Q3: Do you think E-mail phishing incidents are?**

Increasing Decreasing Staying the same Don't know

استبيان عن سرقة المعلومات بالبريد الإلكتروني

Free Online
Surveys.com

* **س1: ما مدى معرفتك عن سرقة المعلومات بالبريد الإلكتروني وهو ما يعرف "Phishing, Scam, Spam or Fraud E-mails"؟**

ممتازة جيدة متوسطة ضعيفة معدومة

إذا أجبت بين 1-معدومة ، يرجى تخطي س2

س2: كيف عرفت عن سرقة المعلومات بالبريد الإلكتروني ؟
يمكنك اختيار أكثر من إجابة

أخرى المدرسة أو الجامعة العمل وسائل الإعلام الانترنت

يرجى التحديد

* **س3: هل تعتقد أن حوادث التصيد بالبريد الإلكتروني في ؟**

لا أعرف بنفس النسبة نقصان زيادة

A5 Questionnaire participants

In Qatar, 1000 Qatari e-mail users over 12 participated in the questionnaire survey, as follows:

- Al-Shaima secondary school
- Carnegie Mellon University
- Commercial Bank of Qatar
- Doha Bank
- Friends and relatives
- Georgetown University
- ICT Qatar

- International Bank of Qatar (IBQ)
- Ministry of Defence
- Ministry of Economy & Commerce
- Ministry of Foreign Affairs
- Ministry of Higher Education
- Ministry of Interior
- Ministry of Municipal and Agriculture Affairs
- Qatar Foundation
- Qatar Petroleum (QP)
- Qatar Telecommunication (Qtel)
- Ras Gas
- Sidra Medical and Research Centre
- University of North Atlantic (CAN)
- University of Qatar

On the other hand, 1000 British e-mail users over 12 were participated in the questionnaire survey as follows:

- Birmingham University
- Bradford College
- Friends and neighbours
- Grange School, Bradford
- Human Relief, Bradford
- In public areas, e.g. Cyprus restaurant, mosque in Bradford and city centre
- Leeds Metropolitan University
- Leicester University
- Loughborough College
- Qatar Embassy
- Qatar Medical and Cultural Attaché
- Qatari students in the UK through Qatar Embassy
- Tong High School, Bradford
- University of Bradford
- University of Loughborough

FRIENDSHIP THROUGH TRADE

التجارة طريق الصداقة

TECHNICAL TRANSLATION UNIT
TRANSLATION INTO ENGLISH
DATE: 25/02/2009



Logo of
State of Qatar

Ministry of Foreign Affairs

State of Qatar
Date: 23/02/1430
18/2/2009

Ref: 5/00067/03/2009 و خ

**His Excellency / Director of human resources and administration the distinguished
Supreme Council for Communications and Information Technology
Doha**

After Greetings

With reference to your letter No.323/ 2009 dated on 10/2/ 2009 regarding the training request submitted by Kiossirt department from Eng. / Mariam Khalid Al-Homer who is an employee in the ministry of foreign affairs

We inform you the approval on the engineer's request while appreciating your cooperation

Yours sincerely
Khamis Ibrahim Al-Mhandi

Director of Information Management and Research, in acting

Technology section

P.O.Box: 250 – DOHA – QATAR Tel.: (+974) 4334334 – Fax: (+974) 4353592

TRUE TRANSLATION INTO ENGLISH OF THE ORIGINAL LETTER IN ARABIC



Arab-British Chamber of Commerce
43 Upper Grosvenor Street, London W1K 2NJ

T: +44 (0) 20 7235 4363 F: +44 (0) 20 7245 6688 E: info@abcc.org.uk W: www.abcc.org.uk

Registered in London No. 1109402. The Joint Arab British Chamber of Commerce. A company limited by guarantee. Registered office as above.

▶ Subject: Re: could you please contribute in my survey	From: Maya Primorac	01-04-2009 14:31
----------------------------------------------------------------	----------------------------	------------------

Dear Ms. Mariam,

All the deans who have a say in this approved your request to hand out the surveys. Would you like to hand out hard copies or have people go online? We have a total of 140 faculty and staff and 140 students.

Best wishes,
Maya

M.K.J.Al-Hamar@lboro.ac.uk wrote:

Dear Ms. Maya Primorac

It was nice to speak with you today.I hope you would help me by conducting my survey to all staffs and students in the university by forwarding the below message.

Thanks a lot and waiting forward for your reply

*Best regards
Mariam AL-Hamar
PHD student
Loughborough university*

Mariam Al-Hamar, Loughborough PhD student

From: **Ray Dawson** (R.J.Dawson@lboro.ac.uk)
Sent: Wednesday, March 04, 2009 3:13:43 PM
To: H.S.Rajamani@bradford.ac.uk
Cc: mariam alhamar (arab_eyes@hotmail.com)

Dear Dr. Rajamani,

I am writing to you on the request of my PhD student, Mariam Al-Hamar, who I believe has been in contact with you already.

I can confirm that Mariam is a full-time PhD student in the Department of Computer Science at Loughborough University. She is researching into phishing and people's awareness of phishing in the State of Qatar, but she needs data from the UK for comparison purposes as part of her research. We would, therefore, be very appreciative if you could allow her to access your students to carry out a survey.

Thank you for your cooperation in this,

Ray Dawson
Professor of Knowledge Management
Department of Computer Science
Loughborough University
LE11 3TU

A7 Samples of completed questionnaire

E-mail Phishing Awareness Survey

Note: The following shapes means: Choose one answer only Can choose more than one answer

Q1- Gender
 Male Female

Q2- What age group are you in?
 Under 18 18-29 30-49 Over 50

Q3- Education level
 School Further or Higher Education Post Graduate Others

Q4- Occupation
 Student Business man/ woman Employee, please specify your job title Others

Q5- Nationality

Q6- Do you have an E-mail?
 Yes No

Q7- Your E-mail (If you would like to receive an educational material about "Phishing")

Q8: How well do you know about E-mail Phishing, it is also called (Scam or Fraud E-mails)?

None: Don't know anything about e-mail phishing.
 Poor: Have heard of e-mail phishing.
 Average: Knows the term e-mail phishing and understand its simple techniques
 Good: Knows the term e-mail phishing, understand more about its techniques and how to protect against it.
 Expert: Knows the term e-mail phishing; understand more about its complex techniques, how to protect against it, how to detect it and how to react to it.

None Poor Average Good Expert

If you answer Q8-None, then please skip Q9
Q9: From where do you know about Phishing?
 Internet Media (e.g. TV, newspapers) Employer School or university Others

Q10: Do you think E-mail Phishing incidents are?
 Increasing Decreasing Staying the same Don't know

Q11: Do you worry about E-mail Phishing?
 Yes No

Q12: Do you use softwares to prevent you from phishing E-mails and websites (e.g. Anti-virus, Anti-phishing software or spam filters)?
 Yes No

Q13: Do you think using anti-virus, anti-phishing software or spam filter is enough to prevent all types of phishing E-mails?
 Yes No, please specify why Don't know

Q14: Which of the following is generally a sign that an E-mail may be Phishing or fraudulent? You receive an E-mail from your bank which....

- Asks you to enter information about your account (e.g. your username and password)
- Addresses you by your first and last name (e.g. Dear Ms. Mariam K Al-Hamar).
- Directs you to a website containing a security certificate that matches the name of the website.
- Conveys a sense of urgency and surprise
- Has been classified as Junk or spam mails by your E-mail system.
- Contain an attachment, notifying you that it might contain viruses that could harm your computer.
- Points you to a website with a URL that starts with https.
- Asks you to phone a number supplied in the email.
- Don't know

Q15: Which of the following actions should you take if you think you've been tricked by a phishing E-mail?

- Report the incident to the company whose e-mail address or Web site was faked.
- Report the incident to the police or an institute that specialises in dealing with these cases.
- Report the incident to your bank or other organization for which you have given out details.
- Change the account details that you have been given out
- Check your financial statements immediately
- Cut up your credit and debit cards
- Do nothing
- Others

Q16: How often do you receive phishing E-mails?

- Daily Weekly Monthly Never Others

Q17: How many times have you been tricked with phishing E-mails?

- Never Once twice 3 times More than 3 times Don't know

If you answer Q17- Never, then please skip Q18.

Q18: If you have been tricked with a phishing E-mail, which of the following was the reason you were tricked?

- I don't install a software to prevent phishing E-mails and websites (e.g. Anti-virus, Anti-phishing, spam filters)
- The Phishers are coming up with smarter tricks which make it difficult to identify phishing
- The fake website looks almost identical to the legitimate one
- I didn't believe I will be tricked
- The E-mail comes up with sense of urgency and surprise
- Lack of awareness and training about phishing
- I trust the E-mail because I don't know about phishing
- I was not aware of the importance of the information that I have given out
- Other

Q19: What do you think is the best way to defend yourself against phishing E-mails?

- Be aware and be educated about phishing
- Follow clear guidelines addressing phishing (e.g. Check the web address, don't give your private information through the E-mail.etc)
- Install effective Anti-virus, spam filter or anti-phishing software
- Get affected by Phishing E-mails, because I will learn more
- Others

Q20: How do you prefer to be educated about Phishing, Is it though.....?

- Interactive tutorials and quizzes Videos Cartoons Posters Web based e-learning Media
- Seminars Newsletters and documents Screen savers Others

E-mail Phishing Awareness Survey

Note: The following shapes means: Choose **one answer only** Can choose **more than one answer**

Q1- Gender

Male Female

Q2- What age group are you in?

Under 18 18-29 30-49 Over 50

Q3- Education level

School Further or Higher Education Post Graduate Others

Q4- Occupation

Student Business man/ woman Employee, please specify your job title Others

Q5- Nationality

Q6- Do you have an E-mail?

Yes No

Q7- Your E-mail (If you would like to receive an educational material about "Phishing")

Q8: How well do you know about E-mail Phishing, it is also called (Scam or Fraud E-mails)?

None: Don't know anything about e-mail phishing.

Poor: Have heard of e-mail phishing.

Average: Knows the term e-mail phishing and understand its simple techniques

Good: Knows the term e-mail phishing, understand more about its techniques and how to protect against it.

Expert: Knows the term e-mail phishing; understand more about its complex techniques, how to protect against it, how to detect it and how to react to it.

None Poor Average Good Expert

If you answer Q8-None, then please skip Q9

Q9: From where do you know about Phishing?

Internet Media (e.g. TV, newspapers) Employer School or university Others

Q10: Do you think E-mail Phishing incidents are?

Increasing Decreasing Staying the same Don't know

Q11: Do you worry about E-mail Phishing?

Yes No

Q12: Do you use softwares to prevent you from phishing E-mails and websites (e.g. Anti-virus, Anti-phishing software or spam filters)?

Yes No

Q13: Do you think using anti-virus, anti-phishing software or spam filter is enough to prevent all types of phishing E-mails?

Yes No, please specify why Don't know

Q14: Which of the following is generally a sign that an E-mail may be Phishing or fraudulent? You receive an E-mail from your bank which....

- Asks you to enter information about your account (e.g. your username and password)
- Addresses you by your first and last name (e.g. Dear Ms. Mariam K Al-Hamar).
- Directs you to a website containing a security certificate that matches the name of the website.
- Conveys a sense of urgency and surprise
- Has been classified as Junk or spam mails by your E-mail system.
- Contain an attachment, notifying you that it might contain viruses that could harm your computer.
- Points you to a website with a URL that starts with https.
- Asks you to phone a number supplied in the email.
- Don't know

Q15: Which of the following actions should you take if you think you've been tricked by a phishing E-mail?

- Report the incident to the company whose e-mail address or Web site was faked.
- Report the incident to the police or an institute that specialises in dealing with these cases.
- Report the incident to your bank or other organization for which you have given out details.
- Change the account details that you have been given out
- Check your financial statements immediately
- Cut up your credit and debit cards
- Do nothing
- Others

Q16: How often do you receive phishing E-mails?

- Daily Weekly Monthly Never Others

Q17: How many times have you been tricked with phishing E-mails?

- Never Once twice 3 times More than 3 times Don't know

If you answer Q17- Never, then please skip Q18.

Q18: If you have been tricked with a phishing E-mail, which of the following was the reason you were tricked?

- I don't install a software to prevent phishing E-mails and websites (e.g. Anti-virus, Anti-phishing, spam filters)
- The Phishers are coming up with smarter tricks which make it difficult to identify phishing
- The fake website looks almost identical to the legitimate one
- I didn't believe I will be tricked
- The E-mail comes up with sense of urgency and surprise
- Lack of awareness and training about phishing
- I trust the E-mail because I don't know about phishing
- I was not aware of the importance of the information that I have given out
- Other

Q19: What do you think is the best way to defend yourself against phishing E-mails?

- Be aware and be educated about phishing
- Follow clear guidelines addressing phishing (e.g. Check the web address, don't give your private information through the E-mail.etc)
- Install effective Anti-virus, spam filter or anti-phishing software
- Get affected by Phishing E-mails, because I will learn more
- Others

Q20: How do you prefer to be educated about Phishing, Is it though.....?

- Interactive tutorials and quizzes Videos Cartoons Posters Web based e-learning Media
- Seminars Newsletters and documents Screen savers Others

استبيان عن سرقة المعلومات بالبريد الإلكتروني

ملاحظة: الأشكال التالية تعني: اختر إجابة واحدة فقط يمكنك اختيار أكثر من إجابة

س1: الجنس

ذكر أنثى

س2: السن

تحت 18 18-29 30-49 أكثر من 50

س3: مستوى التعليم

ثانوية فما دون دبلوم أو بكالوريوس دراسات عليا أخرى

س4: المهنة

طالب رجل أعمال موظف ، يرجى تحديد طبيعة عملك أخرى

س5: بلدك

س6: هل لديك بريد إلكتروني؟

نعم لا

س7: بريدك الإلكتروني (إذا كنت تريد أن نرسل لك معلومات عن سرقة المعلومات)

س8: ما مدى معرفتك عن سرقة المعلومات عن طريق البريد الإلكتروني وهو ما يعرف "Phishing, Scam, or Fraud E-mails"؟

معدومة: لا يعرف شيئاً عن التصيد الإلكتروني .
ضعيفة: سمعت عن التصيد الإلكتروني .
متوسطة: أعرف ما هو التصيد بالبريد الإلكتروني و أعرف عن التقنيات التي يستخدمها المتصيدون لخداع الناس
جيدة: أعرف ما هو التصيد بالبريد الإلكتروني ، وأعرف المزيد عن تقنياتهم وكيفية حماية منه .
ممتازة: جيدة: أعرف ما هو التصيد بالبريد الإلكتروني ، أعرف المزيد عن تقنياته المتطورة ، وكيفية حماية منه ، كيفية الكشف عليها وكيفية الرد عليها .

معدومة ضعيفة متوسطة جيدة ممتازة

إذا أجبت س8-معدومة ، يرجى تخطي س9

س9: كيف عرفت عن سرقة المعلومات بالبريد الإلكتروني؟

الإنترنت وسائل الإعلام (التلفاز، الصحف....) العمل المدرسة أو الجامعة أخرى

س10: هل تعتقد أن حوادث السرقة بالبريد الإلكتروني في؟

زيادة نقصان بنفس النسبة لا أعرف

س11: هل أنت قلق بشأن سرقة المعلومات عن طريق البريد الإلكتروني؟

نعم لا

س12: هل تستخدم منتج أو برنامج لمكافحة سرقة المعلومات كبرنامج مكافحة الفيروسات والسرقة "Anti-virus, Anti-phishing or Spam filters"؟

نعم لا

س13: هل تعتقد استخدام برامج مكافحة الفيروسات وسرقة المعلومات كافي لكشف ومكافحة جميع أنواع رسائل ومواقع سرقة المعلومات؟

نعم لا، يرجى التحديد لماذا لا أعرف

س14: أي مما يلي يمكن أن يعتبر سرقة للمعلومات عن طريق البريد الإلكتروني؟ وصلتك رسالة من البنك الى بريدك الإلكتروني.....

- تطلب منك إدخال معلومات عن حسابك مثل رقم الحساب والرقم السري .
- صيغة الرسالة ملحة أو مفاجئة (مثل: لقد فزت في السحب الشهري بمبلغ مليون دولار ويجب عليك إدخال معلومات عن حسابك فوراً)
- الرسالة موجهة باسمك الثلاثي.
- توجهك الرسالة للدخول الى موقع الكتروني يحتوي على شهادة أمنية "Security Certificate" مطابقة لاسم الموقع وصحيحة.
- الرسالة ترشدك للذهاب الى موقع الإلكتروني يبدأ عنوانه ب https
- الرسالة صنفت في خانة البريد الغير المرغوب فيه أو المزجج "Junk mail, Spam mail"
- الرسالة مرفقة بملفات كملفات أو برامج صنفت على أنها قد تحتوي على فيروسات ضارة بجهازك
- تطلب منك الاتصال برقم موجود في الرسالة
- لا أعرف

س15: أي من الإجراءات التالية ينبغي أن تتخذها إذا كنت تعتقد أنك قد خدعت برسائل سرقة المعلومات بالبريد الإلكتروني؟

- لا أفعل شيئاً
- أغير معلومات حسابي
- أبلغ الشركة التي تم تزور عنوان بريدها أو موقعها الإلكتروني لخداعي
- أراجع بياناتي المالية على الفور
- أبلغ الهيئة المختصة في التعامل مع هذه الحوادث كالجهاز الأمنية
- أوقف بطاقة السحب الآلي
- أبلغ البنك أو الهيئة التي أبحث بمعلوماتها
- أخرى

س16: ما معدل رسائل سرقة المعلومات التي تصلك بالبريد الإلكتروني؟

- يوماً
- اسبوعياً
- شهرياً
- ولا مرة
- أخرى نادراً

إذا أجبت س16- ليس لدى بريد الكتروني أو ولا مرة ، يرجى تخطي س17 و س18

س17: كم مرة تعرضت للخداع من رسائل سرقة المعلومات بالبريد الإلكتروني؟

- ولا مرة
- مرة
- مرتين
- 3 مرات
- أكثر من 3 مرات
- لا أعرف

إذا أجبت س17- ولا مرة ، يرجى تخطي س18

س18: إذا كنت قد خدعت من قبل برسائل سرقة المعلومات بالبريد الإلكتروني، أي مما يلي كان سبب خداعك؟

- لأنني لم أحمل برامج لمكافحة الفيروسات أو سرقة المعلومات
- لأنني وثقت بالرسالة لعدم معرفتي من قبل عن سرقة المعلومات
- لأن الموقع الكتروني الوهمي يكاد يكون مماثل للموقع الحقيقي
- لأنني لم اعتقد بانني سأخدع
- لأن صيغة الرسالة ملحة أو مفاجئة
- لقلّة التوعية والمعرفة بخطورة رسائل سرقة المعلومات
- لعدم ادراكي بأهمية المعلومات التي طلبتها الرسالة
- أخرى

س19: في رأيك ما هي أفضل وسيلة لمكافحة رسائل سرقة المعلومات بالبريد الإلكتروني؟

- التوعية والتثقيف بخطر سرقة المعلومات وكيفية مكافحتها .
- أتبع مبادئ توجيهية واضحة (كالتحقق من عنوان الموقع الإلكتروني)
- التحرض لرسائل السرقة لأنني أتعلم حينما أخدع
- أحمل برامج فعالة لمكافحة سرقة المعلومات
- أخرى

س20: أي من الوسائل التعليمية التالية تفضل لتثقيفك بسرقة المعلومات بالبريد الإلكتروني؟ من خلال.....

- لعبه إلكترونية
- مقاطع فيديو
- كريكثير
- مواقع الكترونية تعليمية
- الاعلام
- محاضرات
- ملصقات "Posters"
- نشرات ورقية
- شاشة عرض الكمبيوتر "screen savers"
- أخرى

A8 Questionnaire results

In total, 2000 people have participated in the survey as shown below:



The screenshot shows the FreeOnlineSurveys.com website interface. At the top, there is a navigation bar with links for 'Your Surveys', 'Address Book', 'FAQ', and 'UPGRADE'. On the right side, there are icons for 'Account details', 'Members logout', and 'Contact us'. Below the navigation bar is a table listing several surveys.

Status	Title	Date Created	Responses	Options
Survey Active	قطر -استبيان عن تصيد المعلومات بالبريد الإلكتروني	4/14/2009	845	Results
Survey Active	E-mail Phishing Awareness Survey- Qatar	4/14/2009	155	Results
Survey Active	E-mail Phishing Awareness Survey	3/7/2009	400	Results
Survey Active	استبيان عن تصيد المعلومات بالبريد الإلكتروني	3/7/2009	600	Results

A9 In-depth analysis of Qatar questionnaire

Level of knowledge /Age	None	Poor	Average	Good	Expert
Under 18	61	60	64	56	36
Between 18-29	46	82	139	87	16
Between 30-50	51	58	101	71	29
Over 50	7	10	11	15	0

To find whether there is a relation between participants' level of knowledge on e-mail phishing and age, the author applies Chi-squared test as follows:

Contingency table

	A	B	C	D	E	
1	61	60	64	56	36	277
2	46	82	139	87	16	370
3	51	58	101	71	29	310
4	7	10	11	15	0	43
	165	210	315	229	81	1000

	A	B	C	D	E
1	45.7	58.2	87.3	63.4	22.4
2	61.0	77.7	117.	84.7	30.0
3	51.1	65.1	97.7	71.0	25.1
4	7.09	9.03	13.5	9.85	3.48

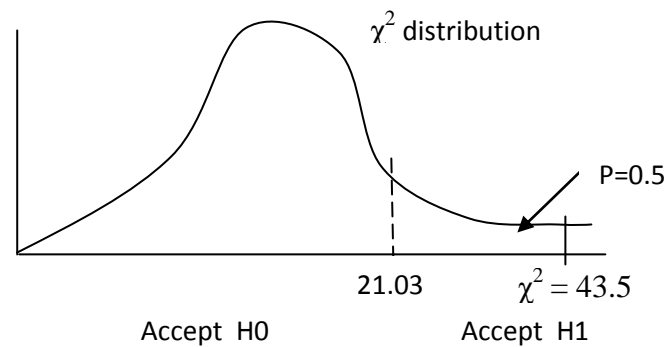
χ^2 was calculated using the following formula:

$$\chi^2 = \sum 2 n_i \ln \frac{n_i}{e_i}$$

Chi-squared $\chi^2 = 43.5$

degrees of freedom = $(4-1) * (5-1) = 12$

Critical value of $x = 21.03$ for $p=5\%$



where:

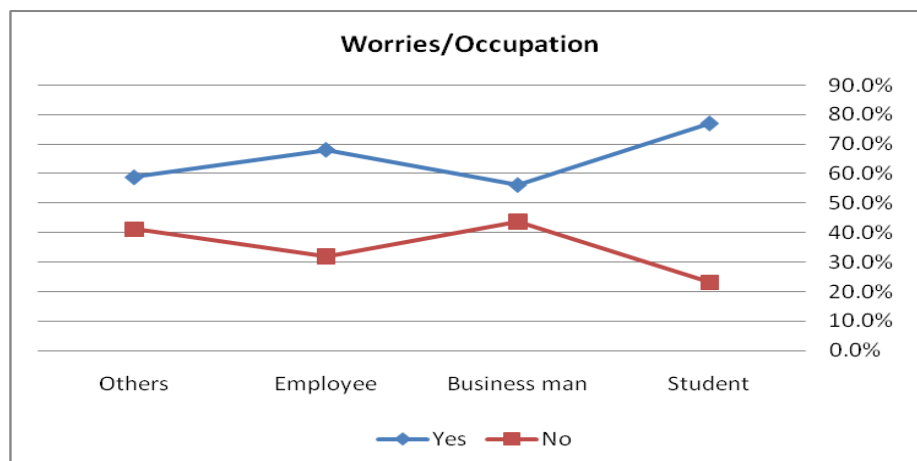
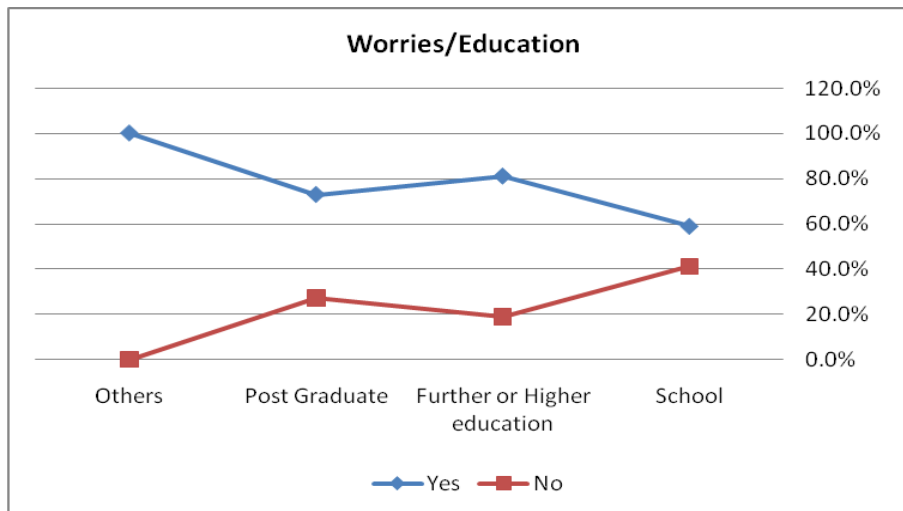
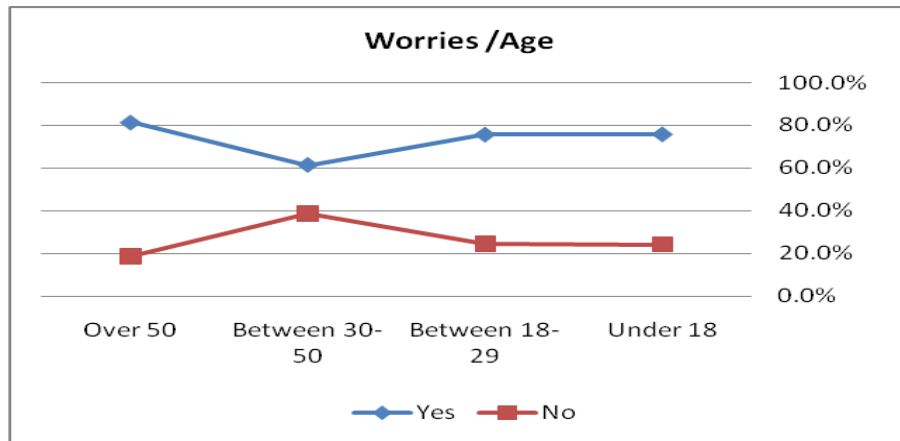
H0= There is no relation between the two responses

H1= There is relation between the two responses

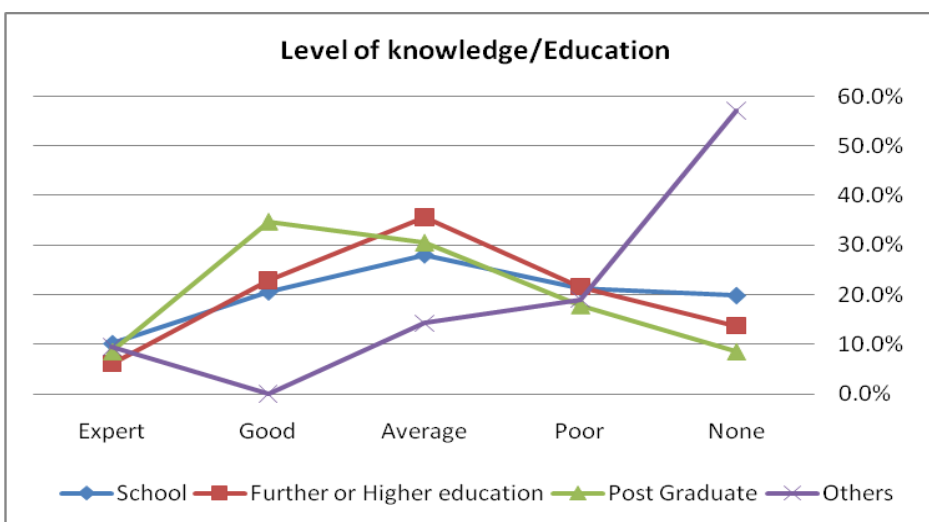
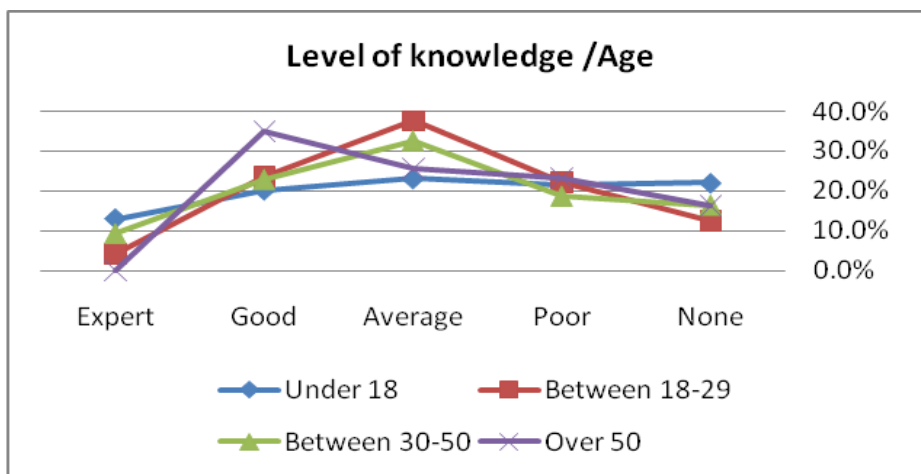
The author concludes that definitely participants' level of knowledge on e-mail phishing and age are related.

Related variable are illustrated with the value of chi-square in tables below:

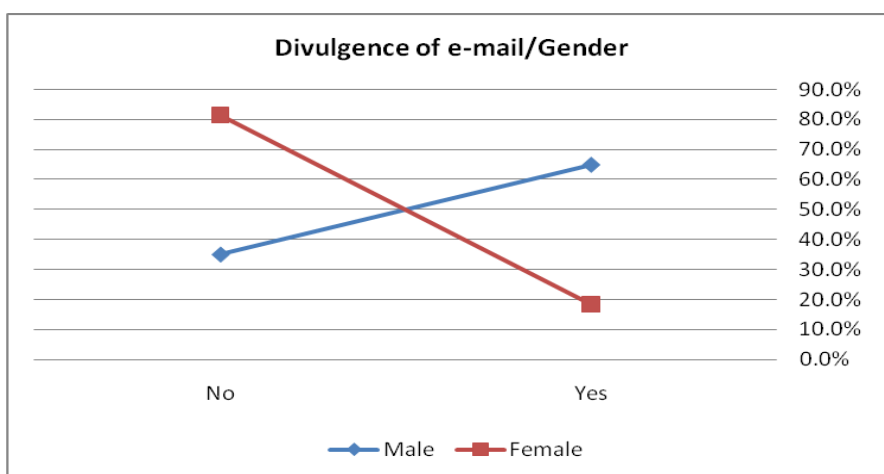
	Worries of e-mail phishing
Age	$X = 7.815, \chi^2 = 23.6$
Education	$X = 7.815, \chi^2 = 60.6$
Occupation	$X = 7.815, \chi^2 = 14.3$

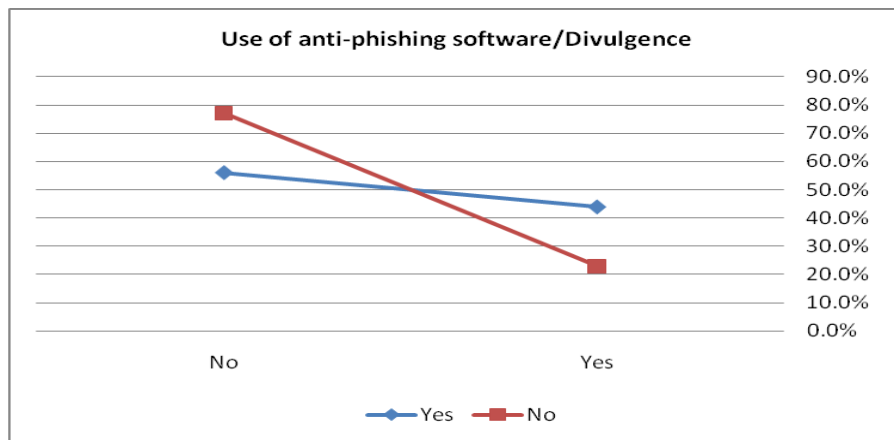
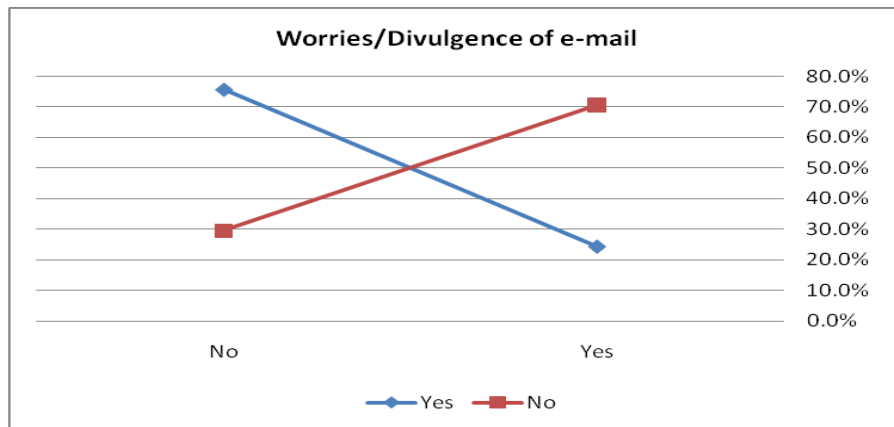
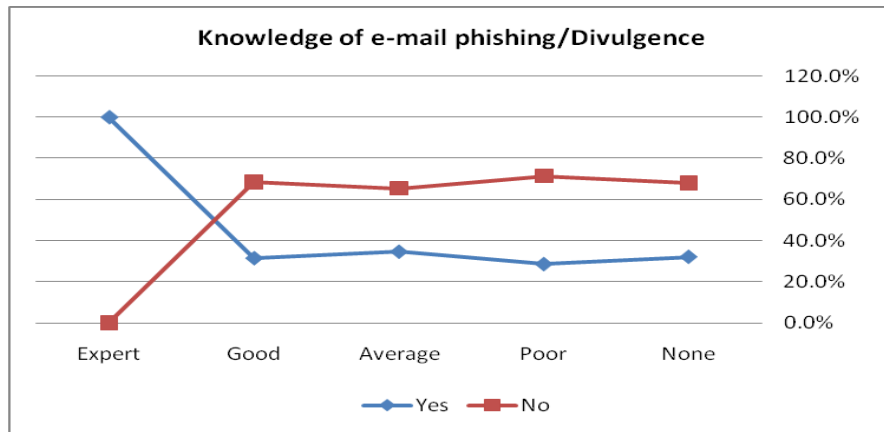


	Level of knowledge
Age	$X = 21.03, \chi^2 = 43.5$
Education	$X = 21.03, \chi^2 = 54.6$



	Divulgence of e-mail addresses
Gender	X= 3.841, $\chi^2=222$
Level of knowledge of e-mail phishing	X= 9.488, $\chi^2= 149$
Worries of e-mail phishing	X= 3.841, $\chi^2= 186$
Use of anti-phishing software	X= 3.841, $\chi^2= 40.2$





	Efficiency of anti-phishing software
Use of anti-phishing software	X= 5.991, $\chi^2= 12$

A10 Comparison between Qatar and UK

χ^2 were calculated using the following formula:

$$\chi^2 = \sum 2 n_i \ln \frac{n_i}{e_i} \quad \text{Where } p \text{ (level of significance)} = 5\%$$

Questionnaire variables	χ^2	Significance between Qatar and UK
Knowledge of e-mail phishing		
E-mail phishing level of knowledge	8.62	Not significance
Source of knowledge	19.6	Significance
Predicted e-mail phishing trend	8.23	Significance
Vulnerability to e-mail phishing		
Participants' worries about e-mail phishing	3.96	Significance
Use of anti-phishing software	2.35	Not significance
Participants' ability to detect e-mail phishing	79.8	Significance
Participants' procedure once attacked by e-mail phishing	46.9	Significance
Participants' divulgence of their e-mail address	21.3	Significance
Extent of e-mail phishing		
Amount of phishing e-mails received by participants	63.5	Significance
Number of times participants have been tricked with e-mail phishing	136	Significance
Reason for being tricked	5.84	Not significance
Defence against e-mail phishing		
Participant's view on efficiency of existing anti-phishing software	25.6	Significance
Participant's view on best way to defend against e-mail phishing	15.7	Significance
Participants' preferred method for awareness and education against e-mail phishing	26.2	Significance

A11 Interviews during questionnaire phase

20 participants in the survey from Qatar and UK were interviewed face-to-face by semi-structured interview containing the following questions:

Q1: According to Q14, if participants got the detection of phishing e-mails wrong, what is the reason?

Q2: According to Q15, if participants have not reacted once they have been tricked, what is the reason?

Q3: If you revealed your e-mail address, why did you?

The following questions were put only to Qataris:

Q3: Why do you think Qatari people could be vulnerable to falling prey to e-mail phishing attacks?

Q4: How do you think Qatari culture affects people's responses to phishing attacks?

Q5: Do you believe country-specific factors such as (1) the vast development experience in Qatar in all sectors especially the economy and ICT, and (2) the absence of an e-law, have assisted development of phishing in Qatar?

Q6: Do you think the establishment of an e-law will help in reducing e-crimes in particular, phishing?

Q7: Do you think Qatari people need more time to cope with the rapid developments in ICT and technology in Qatar in recent years in order to understand not only their advantages but also to be aware of the threats associated with them?

A12 Conclusions from interviews

1. Most of the participants interviewed after completing the questionnaire said that they were not familiar with the terms for security indicators such as https and security certificate and most of their decisions were just guesses.

2. The majority of interviewed participants stated that not all e-mails classified as junk or spam mails or which contain viruses are fraudulent and some do check their junk

mails and sometimes download attachments with viruses, even if the sender is unknown. Also, some participants think that communicating off-line by telephone or post is more trustworthy and safer than online communication, since most thought that online methods are more commonly used in a fraudulent attack.

3. Some of the interviewed participants commented that reporting to the police would make the case bigger and some people said *the law does not protect the dupe* (a common saying in Qatar). Also, it was believed that reporting the case to the company whose e-mail address or website was faked will not make any difference to what happens, as most think that it will not take the matter seriously. Furthermore, some stated they did not know that there is a specialised body to deal with such cases, the Q-CERT (Qatar Computer Emergency Response Team), which handles Internet crimes in Qatar.

4. In the interview, participants revealed that they did not believe they were being tricked, because they lacked awareness of the phishing threat, and because of the smart and varied techniques used by phishers against their victims, these participants frequently fall prey to such attacks.

5. Those who failed in this test stated in the interview that this question was trusted because it was within a survey for a research purposes and some said they did not think their e-mail addresses were confidential information that should not be disclosed.

6. The majority of those Qatari citizens interviewed thought that they had expert knowledge of e-mail phishing since they know how to use the computer and Internet very well in chatting and accessing information or they have heard about the term phishing.

7. The majority stated that Qatari people are vulnerable to e-mail phishing attacks because they are generous, trustful and helpful. A lot of them did not understand properly how to protect themselves against such attack, how to spot threats and how to react once they have been tricked. And a lot do not install anti-viruses or spam filters.

8. All of the interviewed participants have noted that Qatari culture has an effect on people's responses to phishing attacks. Since Qataris are living in a conservative society with a collection of tradition, customs and religious beliefs which have become tracking

on part of their culture. Furthermore, most Qataris are religious and follow Islamic beliefs in being moral, doing good, treating people nicely, trusting them and helping them when required, therefore when phishers use these factors which touch their emotions and religion then they would believe it. Also, Qataris in general are generous, trustful and helpful and this would be used by phishers to fool them.

9. A lot believe that the society needs time to absorb such huge changes which have happened in the country and by that time people will get used to such changes and will be more aware since the government and institutions in Qatar are trying to defend against such attacks by awareness of people and enhancing the security measures.

10. Almost all of the interviewed participants believe that the evolution in the economy and ICT has assisted in the existence and the development of the phishing problem in Qatar and has made it attractive for phishers with the availability of a lot of money and online users who are novices to the Internet and most likely do not know the risks associated it with it. However, some commented that this does not mean the country has to stop developing. Furthermore, some state that phishers are taking advantage of the lack of e-law in Qatar and therefore the establishment of e-law would be essential in helping to reduce e-crimes in Qatar and, in particular, phishing.

A13 Examples of interviews

The following are two examples of interviews with Qatari participants

Example 1

Q1: According to Q14, if participants got the detection of phishing e-mails wrong, what was the reason?

Most of my decisions were just guessed since I'm not familiar with the terms https and security certificate.

With regard to the 'E-mail asks you to phone a given number', I did not think that offline communication by telephone or post is fraudulent, because it is usually done through online communication.

Q2: According to Q15, if participants have not reacted once they have been tricked, what is the reason?

If I have been tricked, I will just report to my bank and they will react and cut up my credit card.

I don't prefer to report to the police, I think I would look stupid and *the law does not protect the dupe*. I also did not know that there is a specialised body to deal with such cases, the Q-CERT (Qatar Computer Emergency Response Team), which handles Internet crimes in Qatar.

Q3: If you revealed your e-mail address, why did you?

Because I trusted it because it was within a survey for a research purpose and I did not think it was phishing me.

Q4: Why do you think Qatari people could be vulnerable to falling prey to e-mail phishing attacks?

The majority of Qataris are vulnerable to e-mail phishing attacks, although some might have heard the term phishing but a lot of them do not understand properly how to protect themselves against such attack, how to spot threats and how to react once have been tricked.

Q5: How do you think Qatari culture affects people's responses to phishing attacks?

It does affect them, since Qataris are living in a conservative society with a collection of traditions, customs and religious beliefs which have become part of their culture. Qataris in general are generous, trustful and helpful and this would be used by phishers to fool them.

Q6: How have country-specific factors such as (1) the vast development experience in Qatar in all sectors, especially the economy and ICT, and (2) the absence of an e-law, assisted development of phishing in Qatar?

Yes, I do believe that the evolution in the economy and ICT has make Qatar attractive for phishers with the availability of a lot of money and online users who are novice to

the Internet and most likely do not know the risks associated it with it. Also phishers take advantage of the lack of e-law in Qatar.

Q7: How much time do Qatari people need to cope with the rapid developments in ICT and technology in Qatar in recent years in order to understand not only their advantages but also to be aware of the threats associated with them?

Yes, I think the society needs time to absorb such changes which have happened and by then people will get used to such changes and will be more aware.

Example 2

Q1: According to Q14, if participants have made a wrong detection of phishing e-mails, what is the reason ?

I did not detect that e-mails in junk mails are harmful because I do not think all of them are or contain viruses. However, I don't think it is an accurate measure and I always check my junk mails even if the sender is unknown.

Q2: According to Q15, if participants do not react once have been tricked, why is that?

I will do nothing if I have been tricked, I believe reporting would not make any difference to what happens, it would only waste paper. If I have already been tricked neither can anyone bring back what has been stolen from me. I have to bear the consequences of my mistakes. What I would do to make others aware is by sharing my experience in the well-known blogs and forums such as Qatar University forum and Qatar Share Market forum.

Q3: If you revealed your e-mail address, why did you ?

I did not think that my e-mail address is confidential information that should not be disclosed.

Q4: Why do you think Qatari people could be vulnerable to falling prey to e-mail phishing attacks?

Because phishers are getting smart and use various techniques to trick their victims and some of these are over confident and believe they are smart enough but would be tricked one day.

Q5: How do you think Qatari culture affects people's responses to phishing attacks?

I think it has a major affect, since most Qataris are religious which implies goodness, treating people nicely, trusting them, helping them when required, therefore when phishing uses these factors which touch their emotions, religion and beliefs, then they would believe it.

Q6: How have country-specific factors such as (1) the vast development experience in Qatar in all sectors, especially the economy and ICT, and (2) the absence of an e-law, assisted development of phishing in Qatar?

I do think all of these have assisted in the existence and the development of the phishing problem in Qatar. However, this does not mean we have to stop developing. However, I think the establishment of an e-law will help in reducing e-crimes in Qatar and, in particular, phishing.

Q7: How much time do Qatari people need to cope with the rapid developments in ICT and technology in Qatar in recent years in order to understand not only their advantages but also to be aware of the threats associated with them?

I think that after two years people will be more aware because the government is trying to find a solution to defend against such attacks by making people aware and enhancing the security measures.

Appendix B: Interviews

This section provides a full breakdown of face-to-face, semi-structured interviews held with experts in Qatar in relation to e-mail phishing and enhancing people's awareness on such attack. Also, there was a structured interview by e-mail with one of the leading companies in the UK in providing information security and testing services since 1989.

B1 Draft Letter to Interview Participants

5 August, 2009

Dear Sir/Madam,

E-mail Phishing

You may have already heard or read about or have even been affected by e-mail phishing. This is a fraudulent process used by criminals. What they do is try to acquire sensitive information such as usernames, passwords and credit card details by pretending to be an honest and trustworthy person in an electronic communication such as an e-mail. This can have very serious financial and social consequences for their victims. As a PhD student at Loughborough University in the UK, I am doing research on 'e-mail phishing' as a contribution to foiling those criminal schemes.

The research aims to reduce the e-mail phishing hazard in the State of Qatar by developing an effective e-mail phishing awareness framework and to point to possibilities of wider application. In order to achieve the desired goals, I need to interview officials and citizens such as you, who are in a position to provide valuable information on attitudes in Qatar culture, e-mail phishing, awareness and related data. We would like to invite you to be part of this study, which will help the researcher to review the extent of e-mail phishing, the cultural effect associated with people's responses to phishing, organisational strategy, views on protecting themselves and/or their customers from e-mail phishing attacks and in particular the methods they use for creating awareness among their employees and customers and for educating them about such threats.

I assure you all responses will be confidential and kept strictly private.

Thank you in anticipation of your involvement

Yours faithfully,

Mariam Al-Hamar

For any queries about the research topic, please don't hesitate to contact me through my e-mail: m.k.j.al-hamar@lboro.ac.uk.

B2 Consent Form for Interview Participants

CERTIFICATION BY PARTICIPANT

I, certify that I am voluntarily giving my consent to provide information for the above described project entitled: **Reducing the Risk of E-mail Phishing through Awareness and Education: An Empirical study of the State of Qatar Considering Cultural Differences**, being conducted at Loughborough University, UK by: Ms. Mariam AL-Hamar.

I certify that I have agreed to be interviewed in the subject of as previously explained by Ms. Mariam AL-Hamar and that that I freely consent to participate in this project. I have had the opportunity to have any questions answered, I have been fully explained the procedures of interview and that information gathered will be only used for the benefit of the entitled research and will be confidential and kept strictly private.

Signed:

Witness other than the interviewee: Date:

.....

For any queries about the research topic please don't hesitate to contact the researcher (Name: Ms. Mariam AL-Hamar, ph. +974 5553493, E-mail: m.k.j.al-hamar@lboro.ac.uk).

B3 Interview questions for domain experts

1. IT professionals in the private and government sectors interviewed face-to-face:

Officer of the Computer Crimes Unit, Economic Crimes Prevention Division, General Admin. Public Security Criminal Investigation Dept., Ministry of Interior.

Manager of Public Relations Dept., Ministry of Interior.

Manager Operational Risk, Doha Bank

Manager of ISP, Qtel

Network engineer, ISP Department, Qtel

Senior Incident Specialist, Incident Management, Q-CERT

Analyst, Critical Infrastructure Protection, Q-CERT

Public Awareness Manager, Q-CERT

2. General framework for questions asked during interviews

2.1 Extent of e-mail phishing

Is e-mail phishing the most frequent phishing attack you have experienced?

How often do your organisation and its clients receive phishing e-mails? Is the frequency increasing?

Are e-mail phishing incidents increasing in your organisation?

What is the number of successful phishing attacks? Is it increasing?

2.2 Review of organisational strategy of defence against phishing

What is your strategy to protect your organisation and its clients from e-mail phishing attacks? Do you make a phishing penetration test to examine your employees' vulnerability to phishing?

What actions does your organisation take once phishing frauds are encountered? And what actions do you take once attacked by phishing frauds?

Do you cooperate with other organisations to take the case further (e.g. ICT)?

How do your employees and clients react to phishing attacks before and once they have been tricked?

2.3 Processes deployed for phishing awareness

Does your organisation consider awareness of phishing important to defend itself from such attack?

If yes, then what process do you deploy to enhance your employees' and customers' awareness on phishing? How is it carried out? And what methods of enhancing awareness do you deploy (e.g. e-learning, posters, seminars, newsletter, leaflets, etc.)?

Do you believe your employees and clients are well aware of the phishing threat? And of how to protect themselves? Do they know how to spot cases and how to react?

2.4 Interviewee opinions

What do you think is the best method for creating awareness and educating people about e-mail phishing?

Why do you think Qatari employees and clients could be vulnerable to falling prey to e-mail phishing attacks?

How do you think Qatari culture affects people's responses to phishing attacks?

How aware do you think Qatari employees and clients are aware of e-mail phishing threat?

Do you believe country-specific factors have helped development of phishing in Qatar? Like, first, the vast development experience in Qatar in all sectors especially the economy and ICT? Second, the absence of an e-law?

Do you think the establishment of an e-law will help in reducing e-crimes, in particular phishing?

Do you think Qatari people need more time to cope with the rapid development in ICT and technology in Qatar in recent years ? First to be able to understand their advantages? Second, to be aware of the threats associated with them?

Do you believe Qatari people are well aware of the phishing threat? How to protect themselves? How to spot threats and how to react?

Since two organisations, the Ministry of Interior and ICT Qatar, are dealing with e-crimes in Qatar and in particular, phishing, additional questions were added to the above in the section ‘Review organisational strategy of defence against phishing’.

Since you are dealing with e-crimes in Qatar, what is the procedure you are currently following when you receive a phishing incident? What actions do you take once attacked by phishing frauds? And which organisations/institutes are you cooperating with to deal with such crimes?

Are you in the process of developing an e-law in Qatar to protect online users? What does the law involve? Which organisations are involved in the development of the e-law? And when is it going to be established?

Does your organisation play a role in enhancing the awareness of Qatari society about the phishing threat? Similarly, since Qtel is the main telecommunication service provider in Qatar, further questions were added to the section ‘Review organisational strategy of defence against phishing’.

Since you are the main telecommunication service provider in Qatar, do Qatari organisations and people refer to you to deal with phishing incidents?

If yes, what action do you take once you receive such a request?

B4 Interview with Head of Prosecution, Ministry of Public Prosecution.

After looking at interviewees’ backgrounds and expertise, the questions were designed to discuss the topic of phishing in general without going in depth into the technical aspects.

1. Extent of phishing

Is phishing is the most frequent attack you have experienced?

What is the number of successful phishing attacks? Is it increasing?

2. Review of organisational approach to phishing attacks

What is your strategy to protect the society from phishing attacks?

What actions do you take once you receive a case of phishing?

What problems do you face in e-crimes and in particular phishing crimes?

Does your organisation consider awareness of phishing as an important method of defence?

What do you think is the best method for creating awareness and educating people about phishing?

3. Interviewee opinions

How do you think Qatari culture affects people's responses to phishing attacks?

Do you think organisations are allowed to make phishing penetration tests to examine their employees' vulnerability to phishing?

Do you think Qataris are vulnerable to falling prey to e-mail phishing attacks? and why?

Do you believe country-specific factors such as (1) the vast development experience in Qatar in all sectors, especially the economy and ICT, and (2) the absence of an e-law, have assisted development of phishing in Qatar?

Do you think the establishment of an e-law will help in reducing e-crimes, in particular phishing?

Do you think Qatari people need more time to cope with the rapid development in ICT and technology in Qatar in recent years in order to understand not only their advantages but also to be aware of the threats associated with them?

How aware do you think Qatari people are of the phishing threat? How to protect themselves? How to spot threats and how to react?

B5 Interview with expert in Islamic studies, voluntary administrator, Ministry of Endowments and Islamic Affairs

1. Use by phishers of religious, emotional and moral issues

Phishers exploit victims' emotions, morals and religion to commit their crimes. Why do you think this is successful in Qatar?

Should your Ministry make people aware of such a threat? What effect would this have on people (e.g. they may not trust others, become unhelpful)?

Are there some people who refer to you once they have been tricked with phishing? And what do you advise them?

Have you experienced such cases of attack happening in Qatar?

B6 Interview with experts in education and training

Director of one of the high schools in Qatar, Ministry of Education and Higher Education

Computer Lecturer, Institute of Administrative Development. The institute is responsible for enhancing administrative development for organisations in Qatar by developing employees' skills.

1. Best process for education and awareness

What do you think is the best method for awareness and educating people?

Does people's background play a big role in awareness?

What are the best conditions for increasing awareness ? How to get people interested, especially in such topics?

How to assess the awareness programme? What is the preparation required ?

How to get people to remember what they learned?

How to get people interested in training again?

2. Processes deployed for phishing awareness

Does your organisation play a role in educating people about cyber threats, in particular e-mail phishing? If no, do you want to?

3. Interviewee opinions

If no, do you think it is important to have some material about such threats in academic institutions to make students aware?

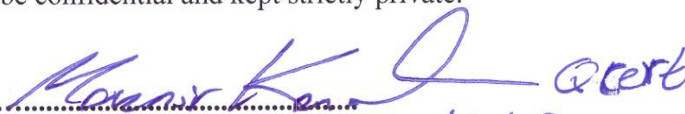
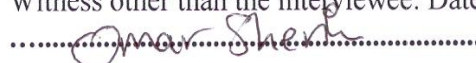
Do you think Qatari people need more time to cope with the rapid development in ICT and technology in Qatar in recent years in order to understand not only their advantages but also to be aware of the threats associated with such technology?

B7 Examples of signed Consent Forms

CERTIFICATION BY PARTICIPANT

I, certify that I am voluntarily giving my consent to provide information for the above described project entitled: *Reducing the Risk of E-mail Phishing through Awareness and Education: An Empirical study of the State of Qatar Considering Cultural Differences*, being conducted at Loughborough University, UK by: Ms. Mariam AL-Hamar.

I certify that I have agreed to be interviewed in the subject of as previously explained by Ms. Mariam AL-Hamar and that that I freely consent to participate in this project. I have had the opportunity to have any questions answered, I have been fully explained the procedures of interview and that information gathered will be only used for the benefit of the entitled research and will be confidential and kept strictly private.


Signed: 
 Witness other than the interviewee: Date: 19/8/09


For any queries about the research topic please don't hesitate to contact the researcher
 (Name: Ms. Mariam AL-Hamar, ph. +974 5553493, E-mail: m.k.j.al-hamar@lboro.ac.uk).

CERTIFICATION BY PARTICIPANT

I, certify that I am voluntarily giving my consent to provide information for the above described project entitled: *Reducing the Risk of E-mail Phishing through Awareness and Education: An Empirical study of the State of Qatar Considering Cultural Differences*, being conducted at Loughborough University, UK by: Ms. Mariam AL-Hamar.

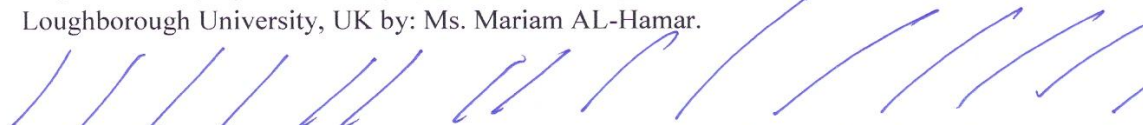
I certify that I have agreed to be interviewed in the subject of as previously explained by Ms. Mariam AL-Hamar and that that I freely consent to participate in this project. I have had the opportunity to have any questions answered, I have been fully explained the procedures of interview and that information gathered will be only used for the benefit of the entitled research and will be confidential and kept strictly private.

Signed:  FIRAZ · m · A, Qatari
Witness other than the interviewee: Date: 18/8/2009

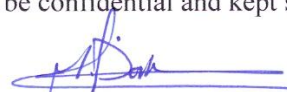
For any queries about the research topic please don't hesitate to contact the researcher (Name: Ms. Mariam AL-Hamar, ph. +974 5553493, E-mail: m..k.j.al-hamar@lboro.ac.uk).

CERTIFICATION BY PARTICIPANT

I, certify that I am voluntarily giving my consent to provide information for the above described project entitled: *Reducing the Risk of E-mail Phishing through Awareness and Education: An Empirical study of the State of Qatar Considering Cultural Differences*, being conducted at Loughborough University, UK by: Ms. Mariam AL-Hamar.



I certify that I have agreed to be interviewed in the subject of as previously explained by Ms. Mariam AL-Hamar and that that I freely consent to participate in this project. I have had the opportunity to have any questions answered, I have been fully explained the procedures of interview and that information gathered will be only used for the benefit of the entitled research and will be confidential and kept strictly private.

Signed:  Deha Bank
Witness other than the interviewee: Date: 13/8/2009

For any queries about the research topic please don't hesitate to contact the researcher (Name: Ms. Mariam AL-Hamar, ph. +974 5553493, E-mail: m..k.j.al-hamar@lboro.ac.uk).

B8 Details of interviews

Interview 1

Date of interview: 12th August 2009

Duration: Approximately 1 hour 30 minutes

Interviewees: Two people from the Ministry of Interior were interviewed together:

Mahmoud Salah D. Ibrahim, Officer of the Computer Crimes Unit, Economic Crimes Prevention Division, General Admin. of Public Security Criminal Investigation Dept., Ministry of Interior.

Abdullah Al-Muftah, Manager of Public Relations Dept., Ministry of Interior.

1. Extent of e-mail phishing

Is e-mail phishing the most frequent phishing attack you have experienced?

Yes, it has peaked recently and has become more concern. We receive lots of phishing attacks in the form of SMS, E-mail, websites and phones. Most reported phishing attacks were attacks which target banks. Banks have got a restricted law from the Qatar Central Bank (QCB) in which they have to refer to us in case of any attacks, in particular, phishing attacks which they have encountered otherwise the bank will be fined. Since the case is critical, usually banks will only refer to us for forensic and deal with the case, most don't refer to other institutes such as ICT Qatar or Qtel as they find bank reputation is the top priority. In most cases, we found difficulty to forensic the phishing crimes since, in most cases, phishers do not use their personality, but they take advantage of people in Qatar or sometimes they steal their identity or impersonate them to commit their crimes, usually without their knowledge. However, it is difficult to prove the good faith of the person. Usually, the stolen money is transferred abroad interrelated, for example, from China to Nigeria and Russia, which makes it difficult catch the phisher especially since there is no cooperation between Qatar and other countries in such matters, such as China and Nigeria. Not only financial losses are consequences of such attacks, also loss of information and moral losses such as reputation are confidential and in some cases very critical.

How often do your organisation and clients receive phishing e-mails? Is the frequency increasing?

I'm not sure but I think it is decreasing because we have applied some security measures.

Are e-mail phishing incidents increasing in your organisation?

No, but possibly through personal e-mails

What is the number of successful phishing attacks? Is it increasing?

It is undetermined or null

2. Review of organisational strategy of defence against phishing

What is your strategy to protect your organisation and its clients from e-mail phishing attacks? Do you make a phishing penetration test to examine your employees' vulnerability to phishing?

Anti-phishing filters are effective. One of our strategies to combat phishing is to train people to recognise phishing attempts and to deal with them. Education can be effective, especially where training provides direct feedback. We don't conduct a penetration test for our employees because they are well aware of phishing and therefore there is no need to assess them.

What actions does your organisation take once phishing frauds are encountered? And what actions do you take once attacked by phishing frauds?

We collect all information and data for further investigations and actions.

Do you cooperate with other organisations to take the case further (e.g. ICT)?

We do co-operate with Qtel in some cases to block certain websites or IPs. However, banks have got a strict law to follow from Qatar Central Bank to refer to us once such cases are detected.

How do your employees and clients react to phishing attacks before and once they have been tricked?

Our employees will immediately report the incidents towards dealing with the case

Since you are dealing with e-crimes in Qatar, what is the procedure you are currently following when you receive a phishing incident? What actions do you take once attacked by phishing frauds? And which organisations/institutes are you cooperating with to deal with such crimes?

First we file the case then the cyber crime centre of CID department deals with the crime investigation and collecting data and sometimes it require a cooperation with other organisations such as Qtel.

Are you in the process of developing an e-law in Qatar to protect online users? What does the law involve? Which organisations are involved in the development of the e-law? And when is it going to be established?

ICT Qatar is in the process of developing e-law, I don't know what it involves but it will cover all issues related to online communication.

Does your organisation play a role in enhancing the awareness of Qatari society about the phishing threat?

Yes, through public relation programmes, awareness seminars and classes were done about e-crimes.

3. Processes deployed for phishing awareness

Does your organisation consider awareness of phishing important to defend itself from such attack?

Yes, awareness is very important to protect from phishing attacks since phishers try to trick victims by clever techniques which in most cases are not detected by technological tools such as spam filter or anti-viruses because they are clever, improving and trying to overcome those tools. In the field of awareness, we deal with the matter cautiously to avoid intimidating the society. On the topic of e-crime, we don't want to intimidate people since Qatar society is still safe, conservative and has ethics, principles and religious beliefs.

If yes, then what process do you deploy to enhance your employees' and customers' awareness on phishing? How is it carried out? And what methods of enhancing awareness do you deploy (e.g. e-learning, posters, seminars, newsletter, leaflets, etc.)?

We use to train people through various processes like e-learning, seminars, exhibitions, posters and newsletters, SMS and media (through newspapers and TV programmes) to recognise phishing attempts and to deal with those attacks. We publish monthly a magazine called *The Police is with you*; it is distributed to almost all organisation in Qatar private and government and it is usually published in newspapers. It contains a lot of articles on different topics that matter to Qatar society and some of our publication have articles about e-crimes and cyber crimes.

Public Relations Department in Ministry of Interior is responsible for raising public awareness on topics which many need consciousness such as drugs and recycling; however, they did not yet provide awareness on phishing in particular. Initially, CID provides public relations with the topic of awareness and they develop the awareness tool, usually a poster, leaflet and video. Public relations has coordinated with CID in the past period to give lectures to school students about the dangers of the Internet and the ways to avoid and the procedures that must be taken in case of being fooled. Also there is a plan to develop leaflets and posters on e-crimes.

However, they found media, especially TV, are the best way to enhance public awareness since it is more watched and preferred by Qataris. We did not yet provide any awareness for e-crimes, but there is a plan for that since we found there is a need to make people aware since we found it becomes more noticed. I think the game is an interesting tool for awareness, especially for kids.

Do you believe your employees and clients are well aware of the phishing threat? How to protect themselves? Do they know how to spot cases and how to react?

Our employees are well aware but our client 'public citizens', most of them are not.

4. Interviewee opinions

What do you think is the best method for creating awareness and educating people about e-mail phishing?

I think it is the media, SMS and sending e-mail messages within each organisation, also with cooperation with ISPs to send such information to personal e-mail holders. The public relations have got what is called 'awareness e-mail' which is sent to people who are registered in our awareness programme, and then every while we sent an awareness on specific topics usually according to the occasions (e.g. awareness of safety in Ramadan, traffic safety on Eid).

Why do you think Qatari employees and clients could be vulnerable to falling prey to e-mail phishing attacks?

Yes, I do think that. We have received lots of incidents where victims have been preyed on through their kindness, trust, morals and emotions, especially since Qatari people are still holding on to their culture and Islamic beliefs.

How do you think Qatari culture affects people's responses to phishing attacks?

Yes, of course phishers and criminals in general study the culture and the personality of victims if possible for committing their crimes. For example, since Vodafone was launched in Qatar, we have received a lot of phishing attacks which exploit people by claiming that they are Vodafone official office in Egypt and they can provide cheaper services for them. Basically, attackers use things existing in Qatar.

How aware do you think Qatari employees and clients are of e-mail phishing threat?

No, most are not. I think by the time and by providing an effective awareness, they will be more aware.

Do you believe country-specific factors such as (1) the vast development experience in Qatar in all sectors, especially the economy and ICT, and (2) the absence of an e-law, have assisted development of phishing in Qatar?

Yes, I do believe that the rapid development which Qatar has experienced in the last few years in all fields, economic, politics, telecom and others makes Qatar vulnerable to cyber crimes. With regard to e-law, there is no clear assigned e-law in Qatar. However, in penalties law No.11 of 2004, there is a section about computer crimes on pages 142-147. It is a small section, it does not cover all types of fraud existing nowadays but it covers in general topics such as viruses, misuse of data or computers and unauthorised

access, etc. It does not even criminalise phishing attacks. However, it does criminalise viruses which are distributed through floppy disk and CDs, which means if distribution of viruses is through Internet, e-mail or even USB it is not criminalised. Therefore, when a phishing case went to the court, there was not actually an explicit law under which to punish the phishers, because the law is quite old and was not planned very well. Once we receive e-crimes, we research and investigate, then we perform all actions required such as ask Qtel to block the site and we provide a report of the case to the Prosecution. However, most lawyers and justices do not have knowledge in IT therefore they found difficulty even in understanding most of the terms mentioned in our report and mostly they depend on our report to either to criminalise the accused or not, even though in most cases there is no clear law support decision.

I think the current law will have to be changed and there should be a separate e-law which covers all issues related to electronic communications and crimes. However, Q-CERT is currently developing an electronic law for Qatar, yet it is not approved. There is a plan to establish e-law for all GCC countries to be an umbrella for all countries.

Do you think the establishment of an e-law will help in reducing e-crimes, in particular phishing?

Yes, I think because there is no clear e-law phishers and criminals can commit their crimes freely and escape with no punishment. However, since most phishing attacks originate from outside the country, the law might not be able to be enforced in other countries such as Nigeria and China.

Do you think Qatari people need more time to cope with the rapid development in ICT and technology in Qatar in recent years in order to understand not only their advantages but also to be aware of the threats associated with them?

Yes, I think the development in ICT went very fast. Nowadays, we can see 5 year-old kid with a pc. Most people know how to use the Internet but they do not actually know that the Internet has got lots of negatives like the distribution of destructive ideas such as Al-Qaeda and existence of crimes and black market. We have to know how to deal with the technology, gain the good things only and we have to know how to protect ourself. Most people don't have anti-virus or even don't update it and they download anything from Internet, putting themselves at risk of crimes. I think schools should not only

teach students IT but also how to use the Internet safely and protect themselves from possible criminal attacks.

Do you believe Qatari people are well aware of the phishing threat? How to protect themselves? How to spot threats and how to react?

No, most are not well aware.

Interview 2

Date of interview: 14th August 2009

Duration: Approximately 1hour

Interviewee: Mohamed Darwish, Manager Operational Risk, Doha Bank

1. Extent of e-mail phishing

Is e-mail phishing the most frequent phishing attack you have experienced?

The first phishing attack we faced was recently in March 2008, since then an average of 2 attacks per month was experienced, which means it is most frequent. However, it stopped in November 2008 due to some counter measures the bank has provided. Customers usually phone the call centre in case of any attacks encountered, for example we receive calls from customers claiming that he/she has received an SMS from the bank stating that an amount of money has been transferred from this account to another internally without his/her notice. Usually phishing attacks exploit people's interest and goods, such as an attack stating that you have won a car but we need you to transfer an amount of money for payment of taxes , or we are children at an orphan charity institute and we require your help for orphans or even sometimes they are cleverer than that, as they claim to use their victims as a representative or an intermediary for a foreign institute or person in Doha, where then they transfer an amount of money into the victim's bank account where in turn it is transferred later to another account. In most cases, victims were promised to gain a percentage amount of money or in some cases they exploited people's goodness and emotions, such as claiming that this money is for charity. Phishers in most cases use the victim's identity to commit any crime. Usually, the attacks came from foreign countries such as Russia and Nigeria where attackers cannot be reached or criminalised since there is no law of co-operation between these countries and Qatar to criminalise those kind of attackers, whereas if the case arises for example within the GCC countries the attackers could be criminalised since there is a clear corporation between GCC countries in almost all matters.

How often do your organisation and clients receive phishing e-mails? Is the frequency increasing?

It is a lot but I'm not sure by how many exactly. However, it has been reduced now since the bank has applied restricted technical solutions such as filters, anti-viruses, malicious code scans, along with restriction policies and, in general, employees have become well aware of phishing attack since they have been educated.

Are e-mail phishing incidents increasing in your organisation?

No, as I say, they have been reduced

What is the number of successful phishing attacks? Is it increasing?

He commented that this was private information that he was not allowed to disclose.

2. Review of organisational strategy of defence against phishing

What is your strategy to protect your organisation and clients from e-mail phishing attacks? Do you make a phishing penetration test to examine your employees' vulnerability to phishing?

We have done some things to prevent phishing attacks since November 2008, as follows:

- It takes 24 hours to activate any account added as third-party account to one of our client accounts and, before that, we call back the account owner to ensure that he has taken this action. Also it is not allowed to have a account which adds a third party to more than one account on the same day. This has prevented phishers who gain access illegally to a client bank account and add themselves or others as beneficiary third party account where transactions can be done easily from the account owner to any of the beneficiaries listed. So since then, about 5 such phishing attacks were caught every month.
- The bank has reduced the limited amount for daily transactions from 50,000 to 40,000 QR.

- The bank deals with a foreign company which is a professional on information security, and it protects the bank from possible hackers.
- By default, the bank does not allow transactions over the phone, unless the client asks for this feature and can also activate and deactivate it as necessary avoid phishing attacks which can impersonate the client over the phone. Also, clients are not allowed to make more than one transaction per day.
- The bank provides SMS service for clients for any actions they held within their account (e.g. once open a new account, transactions either debited or credited, access to online banking and adding a beneficiary to your account). Although there is a possibility that hackers could sniff the line between Qtel and us to capture the message content, but this is hard.
- The bank provides flexibility for the delivery channel of the PIN mailer (a sealed card with the password), so it is delivered to the client either by mail or collected from the bank personally or sent via SMS.
- We have increased two levels of security in online banking: username, password and account number, including the added levels, security questions and virtual keyboard to avoid any malicious code which detects keyboard typing. The security questions are decided upon once the client opens an account with us, from then on each time he/she requires to access the account online, one of these questions is selected randomly to be answered, so each time there will be a different question when the client seeks to log in which helps in avoiding phishing attacks.
- We make our clients aware of phishing attacks through SMS and e-mail. Once we experienced an attack which infected a number of people and we notified all clients to avoid it.
- With regard to penetration test, the bank does not perform such auditing, neither for our clients nor employees, since it has some legal issues, and people might complain also that it requires a team working on this action and even if it is applied, phishers can use this by sending the same e-mail and direct victims to a malicious website instead. I think there is no need for such a test; we try to make people as aware as possible without the need to audit and inspect, which people won't like.

What actions does your organisation take once phishing frauds are encountered? And what actions do you take once attacked by phishing frauds?

- If we receive a phishing attack within the organisation, we block it and add it into our database record and inform all of our employees who are also made aware to call the incide andt management for help in such cases.
- With regard to our clients, once we receive a call from a client of a phishing attack they have encountered, we first ensure that the case really exists and then we inform the Qatar Central Bank and the computer crimes' unit in the Ministry of Interior to carry out the investigation and in most cases we ask Qtel to block the phishing site or phone number. Usually, clients refer to us immediately once they encounter or have been tricked, this really facilitates our actions since the case is recent and the money can be blocked and held by the bank.
- According to bank regulation, the bank is not required to pay for the victims who fail prey to phishers because it is the responsibility of the client to keep their information private from anyone. However, the bank usually recovers the infected client since most stolen amounts were relatively small and bank reputation came as first priority.

Do you cooperate with other organisations to take the case further (e.g. ICT)?

No, we don't since the case is critical and confidential for the bank.

How do your employees and clients react to phishing attacks before and once they have been tricked?

The majority of them who receive an attack or even get infected will report immediately to the bank.

3. Processes deployed for phishing awareness

Does your organisation consider awareness of phishing important to defend itself from such attack?

Yes, we do provide awareness for our customers and employees.

If yes, what process do you deploy to enhance your employees' and customers' awareness on phishing? How is it carried out? And what method of enhancing awareness do you deploy (e.g. e-learning, posters, seminars, newsletter, leaflets, etc.)?

We people aware of phishing by sending awareness material through their e-mail addresses, SMS, and we have got some material on our website. Once we experience a frequent attack we send it to our clients to be aware of it.

Do you believe your employees and clients are well aware of the phishing threat? How to protect themselves? Do they know how to spot cases and how to react?

I think people are still not aware enough, we still receive phishing attacks, even in simpler ones people do fail but with the new actions we perform we help to stop phishing attacks but does not mean they do not happen. Some clients won't refer to us even if they have been attacked, especially well known people, since they think this might affect their reputation, some will only change their password immediately. However, most clients react immediately once they fall victims by calling the bank.

4. Interviewee opinions

What do you think is the best method for creating awareness and educating people about e-mail phishing?

Media is the best way of getting people aware, phishing attacks should be shared with media; this is not the case in Qatar, but in other countries, yes.

Why do you think Qatari employees and clients could be vulnerable to falling prey to e-mail phishing attacks?

In general, there are no specific criteria for victims of phishing attacks, nearly all categories of Qataris can fall victim to phishing attacks regardless of their backgrounds, even people with a high level of education and computer literacy and the poor are attacked by phishers. We have experience that the amount stolen in a phishing attack varies from 1000 QR to millions QR.

Some of our infected clients have claimed that they've never disclosed their account details to anyone, but actually they have been infected by spy or malicious software into client PC have stolen their account details without client notice. This becomes more successful since most victims do not install anti-viruses to protect themselves from such attacks.

How do you think Qatari culture affects people's responses to phishing attacks?

Yes, Qataris are more trusted, kindness, emotional and in general it is easy to trick them especially by utilizing their emotion e.g. need help and pay charity. These types of attacks are new to Qatar and still not all people are aware of it therefore they are easily tricked. Also most think phishing attacks will always ask for your account information straight forward which is not always the case they are clever than that. How aware do you think Qatari employees and clients are aware of e-mail phishing threat?

I'm not sure, but with refer to our clients there is a significant amount of them are unaware of phishing.

Do you believe country-specific factors such as (1) the vast development experience in Qatar in all sectors especially the economy and ICT, and (2) the absence of an e-law, have assisted development of phishing in Qatar?

Yes, I do. I think people should understand how to use the technology safely and there should be a clear law to protect them.

Do you think the establishment of an e-law will help in reducing e-crimes in particular, phishing?

Yes, I do.

Do you think Qatari people need more time to cope with the rapid development in ICT and technology in Qatar in recent years in order to understand not only their advantages but also to be aware of the threats associated with them?

Yes, they have to know the danger of using the technology and this might take time.

Do you believe Qatari people are well aware of the phishing threat? How to protect themselves? How to spot threats and how to react?

No, they still need more awareness programmes to get to understand phishing and avoid it.

Interview 3

Date of interview: 18th August 2009

Duration: Approximately 1hour15 minutes

Interviewee: Two people from the Qtel were interviewed together:

Ahmed Rashid Al-Suwaidi, Manager of ISPs, Qtel

Firaz, network engineer, ISP department, Qtel

1. Extent of e-mail phishing

Is e-mail phishing is the most frequent phishing attack you have experienced?

We do not have tangible figures, about 4 cases per month; however, most are not reported. Phishing website and SMS are most common phishing attacks. We have received a couple of incidents where an attacker impersonated some banks in Qatar, and some hack into the website server in Qatar and host their own website and achieve phishing where all transactions are then transferred to the attacker. Phishing can trick people easily, since most victims do not look at the address bar or even check the security certificate.

An example of phishing attack reported by our customers are denial of service attack (DOS), SMS attacks which ask victims to phone or send an SMS to a given number, and usually this number deducts more than expected from your account e.g. 300 QR instead of few rials, If we are then informed about the case we block the number. However, we might face a lot of legal issues, especially if the company is abroad and that is usually the case, and then the company might complain and take legal action since Qtel's action in blocking the number has consequences of financial losses and reduction of customers.

There are two ways of attack, either single which is easy to block or the more complicated one, multiple attacks such as Botnet attacks resulting in DOS and therefore client discomfort. In this attack, multiple systems access a single website, frequently

causing overload to the server, but it appears as genuine action and it is hard to find a solution for such attack.

The main problem we face now is from attackers from foreign countries who cannot be reached because there is no co-operative law with those countries and Qatar. Examples are Nigeria and China. Also from ipark since a lot of people access the Internet and perform their attacks where it is hard to know the identity of the attacker since it is available to the public and as users do not register for accessing the Internet, we cannot even know from the Mac address since it is not registered. Therefore there is no control over it and we suggest providing some kind of ID proof before accessing the Internet such as visa card, ID number, etc. However, the traffic of ipark is low (10%) since the weather is hot and not supporting, most who use the ipark are usually foreigners while most Qataris have got Internet access in their home and prefer not to access Internet in public places where they do not have privacy.

How often does your organisation and clients receive phishing e-mails? Is its frequency increasing? Are e-mail phishing incidents increasing in your organisation?

I do not have specific statistics, but I think it is not increasing much since Qtel has applied a strategy to prevent phishing attacks.

What is the number of successful phishing attacks? Is it increasing?

We do not receive all phishing reports, some people refer to the Ministry of Interior or to their bank once they face such attack and in most cases we then get informed of the action and usually block the site and we can provide required information about the case.

2. Review of organisational strategy of defence against phishing

What is your strategy to protect your organisation and clients from e-mail phishing attacks? Do you make a phishing penetration test to examine your employees' vulnerability to phishing? What actions does your organisation take once phishing frauds are encountered? And what actions do you take once attacked by phishing frauds?

Our strategy to protect Qtel from phishing attacks is based on applying effective hardware and software on the mail server, provide layers of protection and install spam filters and anti-viruses in to the employee's PC. However, some new spams take time to be adapted to spams in the existed software and spam filters are not so intelligent to detect all possible phishing attacks since some appear legitimate, therefore comes the importance to make Qtel employees aware of possible threats and how to react.

With regard to clients, usually we do not take any action until we receive a report of the incident from our client or get notices from Q-CERT or Ministry of Interior. And in that case we inspect the incident and then decide in co-operation with Q-CERT and the ministry whether block it. In general, anti-Islamic, political or sensitive websites are blocked immediately by Qtel according to a decision having been made only by the Ministry of Interior. We then inspect the IP address of the phishing website. If it is inside Qatar, it can be easily blocked from its webhost within hours, but if it outside Qatar we can block our clients from viewing it but we usually cannot block it from its web host. So anyone abroad can view the website unless there is cooperation with the webhost company on blocking the site and in most cases that is hard unless it is affecting their business and reputation. However, Q-CERT has cooperation with CERTs around the world which are responsible for avoiding e-crimes, therefore if the attack comes from abroad it contacts the CERT in that country which will take action and block the site, usually in days, but in some countries where there are no CERTs it is then hard to block the site, unless the web host company is co-operative.

Do you cooperate with other organisations to take the case further (e.g. Q-CERT)?

We cooperate with Q-CERT in a lot of matters, they inform us about any existing virus and we then try to control it at that time to avoid its spreading. Once we observe high traffic from any PC, in cooperation with Q-CERT we investigate the matter in case it might be an attack or denial of service, therefore we phone the person and inform him of the high traffic. Usually, most do not know as they may be controlled by a malicious code or virus which performs that action. We then ask them to follow certain steps to overcome the problem and this involves launching an automated web page portal with easy guidelines to follow, involving running a well known virus scan, spam filter or malware removing software which is usually 30-day trial. Usually people are

cooperative in such cases but if they are not we immediately block them from accessing the Internet or block their SMTP (Simple Mail Transfer Protocol (SMTP) until the problem is resolved.

How do your employees and clients react to phishing attacks before and once they have been tricked?

Yes, according to our organisation policies, employees have to call the incident management in case of such attacks having been encountered where incident management will then take action whether communicating with other parties or blocking,etc, as I mentioned earlier.

Since you are the main telecommunication service provider in Qatar, do Qatari organisations and people refer to you to deal with phishing incidents? If yes, what action do you take once you receive such a request?

Yes, once they refer to use we perform the same action as explained before.

3. Processes deployed for phishing awareness

Does your organisation consider awareness of phishing important to defend itself from such attack?

Yes, we have got a PR department which aims to make customers aware and educate them on how to use the Internet safely. We do that by posting major attacks in the newspaper, sending SMS to all clients and we have some materials on our website that cover Internet usage policy.

So then what process do you deploy to enhance your employees' and customers' awareness on phishing? How is it done? And what method of enhancing awareness do you deploy (e.g. e-learning, posters, seminars, newsletter, leaflets, etc.)?

We provide awareness on phishing by newspaper and usually by sending SMS to all of our customers since it is a common channel to reach people and make them aware. We provide awareness when required, that is, when we experience an attack becoming more frequent and a lot of people fall in it, then we decide to make them aware. However, Q-

CERT focuses on enhancing public awareness on matters associated with technology.

Do you believe your employees and clients are well aware of the phishing threat? How to protect themselves? Do they know how to spot cases and how to react?

No, more effort have to be made to enhance people's awareness. Some people become doubtful about SMS messages and e-mails, even legitimate ones from Qtel. We still receive calls asking for verification whether it is true or fake.

4. Interviewee opinions

What do you think is the best method for creating awareness and educating people about e-mail phishing?

SMS and media are the best method of awareness where you can reach people. Nowadays nearly all adults have got a mobile, sometimes even children, therefore it is better to use the technology to spread awareness.

Why do you think Qatari employees and clients could be vulnerable to falling prey to e-mail phishing attacks?

In general, I think people with different backgrounds are vulnerable to phishing attacks.

How do you think Qatari culture affects people's responses to phishing attacks?

Yes, I do. Since phishers utilise Qatari's goodness and emotion by mentioning moral and emotional topics in the religion, there is need for help. In general, Qataris trust a phishing e-mail in Arabic more than in English since they understand it better, it presents its meaning perfectly and they might believe it since it is their native language. Still, we have not experienced an attack done inside Qatar, most of the time attackers come from abroad as it is part of Qatar culture where Qataris do not favour committing attacks and getting people harmed whereas this is common in some neighbouring countries such as Saudi Arabia.

How aware do you think Qatari employees and clients are of the e-mail phishing threat?

Once we discover an attack that becomes common, such as the recent phishing SMS messages about winning a Hammer car, we then do make our clients aware of such a threat, usually through SMS, e-mails.

Do you believe country-specific factors such as (1) the vast development experience in Qatar in all sectors, especially the economy and ICT, and (2) the absence of an e-law, have assisted development of phishing in Qatar?

Qatar is coming to the forefront in economics and ICT. The existence of Vodafone is beneficial for both customers since competition on prices and quality of service existed and for Qtel where it has reduced the load and cost. In general all e-crimes are not supported by the current law. I think there should be one which will support Qtel actions. Till now, we take our action and do blocking without a clear law to support our actions e.g. like blocking, therefore anyone can complain about us.

Do you think the establishment of an e-law will help in reducing e-crimes, in particular phishing?

Yes, there is a strong need for an effective e-law. I have noticed that ICT is working on developing an e-law.

Do you think Qatari people need more time to cope with the rapid development in ICT and technology in Qatar in recent years in order to understand not only their advantages but also to be aware of the threats associated with them?

Since Internet penetration is high in Qatar, therefore attackers are increasing their interest in Qatar. However, we can't stop the development or improvement. As a result, people went to a huge transition in technology without being aware enough of how to use the Internet in the right way and avoid attackers.

Do you believe Qatari people are well aware of the phishing threat? How to protect themselves? How to spot threats and how to react?

From my experience, I think people are still not aware enough of phishing. Most calls we receive from clients ask us to verify whether the e-mail they received is a phishing attack or not and few calls come after they have been phished. Most people do not even read the terms and conditions of website, privacy seals to ensure their protection, the

majority do not update their anti-virus if they have one and some run peer to peer applications where users will open port to attackers to access their computer.

Interview 4

Date of interview: 19th August 2009

Duration: About 2 hours

Interviewees: Three people from Q-CERT together:

Mounir Kamal, Senior Incident Specialist, Incident Management,
Q-CERT

Omar Sherin, Analyst, Critical Infrastructure Protection, Q-CERT

Nora al-Abdulla, Public Awareness Manager, Q-CERT

1. Extent of e-mail phishing

Is e-mail phishing the most frequent phishing attack you have experienced?

Phishers usually study security awareness level of victims, e.g. what they like? (e.g. cars, shopping), what things attract them?. Once this is done, it might even remove any doubt or technical thinking on victims. Phishing has two parts: the technical part of it and the social engineering part where phishers try to study the community and the characteristic of victims, towards tricking them to attain their goal. In general, the majority of phishing is targeting the financial sector, especially banks. Most frequent phishing is by phone, SMS or e-mail which mostly target organisations in Qatar. Usually phishers exploit vulnerability within the website or the victim's PC (e.g. does not update software, does not have anti-virus, spam filter, etc.) for malware infection. We received two incidents last year with websites infected with malware inside Qatar which were then blocked. However, usually phishing attacks are from outside, e.g. Argentina and China. We have experienced a phishing attack stating that you have won a Hammer or that bad magic is being used against you. Although this seems unrealistic, in Qatar culture it is believable and some people have really fallen victim to such attack. It was mentioned in newspapers, being common.

In ipark there are security threats associated, therefore we suggest having an authentication process.

How often do your organisation and clients receive phishing e-mails? Is the frequency increasing?

We do not have statistics, but we receive a lot, most are filtered by our spam filter but there are some that still who bypass it.

Are e-mail phishing incidents increasing in your organisation?

We do not have specific measurement, but I think it is decreasing since we provide adequate security measures.

What is the number of successful phishing attacks? Is it increasing?

As I mentioned, we don't have records of number of victims.

2. Review of organisational strategy of defence against phishing

What is your strategy to protect your organisation and clients from e-mail phishing attacks? Do you make a phishing penetration test to examine your employees' vulnerability to phishing?

We use spam filters, firewalls and anti-viruses. We are also registered with APWG (Anti-Phishing Working Group). They provide a feature which can check for phishing websites identical to your organisation and once this is discovered Q-CERT will try to block the site. If it is local we refer to Qtel and if it is abroad then we refer to the CERT in this country to block the site. However, there are no CERTs in some countries such as Nigeria. In that case the website can't be blocked in the absence of a law to criminalise such attacks. We also use open DNS solutions which will check if any website is infected. We are also carrying out a honey pot project, so we attract attackers to attack us and then we collect the statistics of number of attacks, where they are from, their IPs. We study the attacks and we send Qtel a summary report. In case we discover an attack on targeted Qatar institutes or the public whether made inside or outside Qatar, we immediately contact Qtel to take action.

We can't conduct penetration test, since it is hard to do on a large scale, it requires authorisation, people might complain and there is concern also that phishers could use it to make their attack.

What actions does your organisation take once phishing frauds are encountered? And what actions do you take once attacked by phishing frauds?

We take the following steps:

1. Verify the incident, the incident management team work on investigating the attack to ensure that it is a real crime
- 2 We report it, the incident management team work on investigating the attack.
3. Layers of protection. First we trace the IP address and then decide whether to block it or not and then take blocking action. Usually we block the source of attack (i.e. the site) locally in Qatar in cooperation with Qtel. This is done within hours. If the attack is from abroad, which is always the case, then we speak with CERT in the country where the phishing site is hosted asking them to block the site and if there is no CERT we then contact the organisation hosting the phish site to block the website and in most cases they co-operate but sometimes they do not agree to block it. However, even if the site was blocked the phisher would launch another new site with no problem of DNS name since it is not appropriate business.

Do you cooperate with other organisations to take the case further (e.g. Qtel)?

As I mentioned, we co-operate usually with Qtel and now Vodafone and CERTs around the world. Ministry of Interior and CID might refer to us as we are an information security consultancy. Not all phishing attacks are reported to Q-CERT, most are not, especially in banks, as reputation is an important factor for most organisations.

How do your employees and clients react to phishing attacks before and once they have been tricked?

They report to incident management, then we carry out possible actions.

Since you are dealing with e-crimes in Qatar, what is the procedure you are currently following when you receive a phishing incident? What actions do you take once

attacked by phishing frauds? And which organisations/institutes are you cooperating with to deal with such crimes?

I have mentioned that before.

Are you in the process of developing an e-law in Qatar to protect online users? What does the law involve? Which organisations are involved in the development of the e-law? And when is it going to be established?

Yes, the law has been set up already with co-operation in the development of the law with associated organisations such as Ministry of Interior, Prosecution, CID, Qtel and others. However, the law is not yet approved by higher authorities who might take a year. The new law covers almost all issues associated with Internet usage including topics such as misuse of devices, cyber crime, computer-related fraud and others. Although we are late in establishing e-law, it was beneficial, since we have learned from others' mistakes and experience in e-law.

Does your organisation play a role in enhancing the awareness of Qatari society about the phishing threat?

Yes, we try to develop an aware community with regard to ICT.

4. Processes deployed for phishing awareness

Does your organisation consider awareness of phishing important to defend itself from such attack?

Yes, we do.

If yes, then what process do you deploy to enhance your employees' and customers' awareness on phishing? How is it carried out? And what method of enhancing awareness does you deploys (e.g. e-learning, posters, seminars, newsletter, leaflets, etc.)?

Awareness is important, since people are the weakest link. We have once written a column in the newspaper about Internet crimes. All of our employees are expert in IT and are aware of such threat. However, we send them articles very often on various security topics to make them aware them of the latest protections, attacks around the

world. We provide in our website articles on the topics of security and cyber crimes for the benefit of public awareness.

With regard to the public, ict QATAR is an operative member in the development of Child Online Protection Initiative with International Telecommunications Union (ITU). On Initiative for Telecommunications and Information Society Day, we conducted an awareness workshop to protect Qatar's children against cyber crime. We cooperated with the Supreme Education Council (SEC) and private schools in Qatar to conduct a workshop in Arabic and English. During the workshop children were asked to draw a picture describing cyber crime. We found the drawings varied: some were negative scary picture and others were positive, some even provided some guidelines and others not, but all this has given us a clue of the level of awareness of children on this matter.

Currently, we are developing an awareness campaign called K2-12 Cyber Safety Curriculum for schools in cooperation with SEC, the Council of Family Affairs and ITU. It aims to address the gap between the heavy use of technology in schools and the knowledge of how to use it safely. It covers the topics of Cyber Community Citizenship, Online Personal Safety, Cyber Predator Identification, Cyber Security and Intellectual property.

However, although awareness is our main concern, there is a budget issue and a need for co-operation with other organisations. The K2-12 curriculum is going to be paper-based, with some articles and maybe cartoons since our target is children and we would like to attract them. But posters, leaflets and advertisements are not our consideration, since it would require an effort and enough budget. The idea of the game is interesting but we do not have enough knowledge on how to build such a game. In general, all of the above tools mentioned are nice to have towards achieving an effective and interesting awareness; nevertheless, it might be done in the future when resources are available.

Do you believe your employees and clients are well aware of the phishing threat? How to protect themselves? Do they know how to spot cases and how to react?

Phishing could trick even expert people and we fall victim to such attack, Nora went to an Islamic website containing Holy Quran software but once she downloaded it, her e-mail had been stolen. Omar also faced an attack when a phisher stole his father's e-mail

account and sent him an e-mail pretending to be his father requesting an amount of money. Even expert people do not check the security certificate of the site each time or even the URL since it looks almost identical but there is a difference of a dot or a letter. In security, everything could be faked, even the SSL and the security certificate. Also there is a tool which will remove the address bar in the browser and insert a new bar with the legitimate address, which happens in seconds, where victims can't recognise it, leading the victims to feel that the site is legitimate since the URL is true.

5. Interviewee opinions

What do you think is the best method for creating awareness and educating people about e-mail phishing?

I think it is the media through TV programmes, posters, cartoons and articles published in Qatar newspapers. Media is the common means for reaching a high proportion of people. I might suggest as well the SMS since it becomes more common now for organisations to send advertisements in SMS. However, there might be an issue that Qtel might not provide its clients' mobile numbers to protect customer privacy. I think media are the best. But if you are targeting children then it is better to visit schools and conduct a seminar on security. Your idea of educating and enhancing awareness through a game would also be a good idea to try and see children's reaction. I think they would like it and learn from it better than the seminar, since it is interesting tool of learning which children would prefer.

Why do you think Qatari employees and clients could be vulnerable to falling prey to e-mail phishing attacks?

Yes, as I mentioned, anyone can be vulnerable to such attack, irrespective of their background, even experts in security are vulnerable.

How do you think Qatari culture affects people's responses to phishing attacks?

I think Qatar is a trusted environment, people feel they are safe and therefore this might reflect that they would fall in a phishing attack.

How aware do you think Qatari employees and clients are of e-mail phishing threat?

It is difficult to say how aware people are, it is a conflict to discover since it is hard to measure security awareness.

Do you believe country-specific factors such as (1) the vast development experience in Qatar in all sectors, especially the economy and ICT, and (2) the absence of an e-law, have assisted development of phishing in Qatar?

There is no law in Qatar which prevents phishing attacks which make phishing hard to control.

Do you think the establishment of an e-law will help in reducing e-crimes, in particular phishing?

Yes, of course the law will help to establish a framework and legislation to criminalise attacks and support our actions of blocking and other organisation such as Qtel. I think attackers will be reduced since there will be an e-law to criminalise them.

Do you think Qatari people need more time to cope with the rapid development in ICT and technology in Qatar in recent years in order to understand not only their advantages but also to be aware of the threats associated with them?

Yes, I think there should be work done to enhance the security awareness of the community and this is our role. I think this would take a time where people will absorb the technology and how to use it effectively and safely.

Interview 5

Date of interview: 21st August 2009

Duration: Approximately 45 min

Interviewee: Abdullah Al-Malki, Head of Prosecution, Ministry of Public Prosecution

1. Extent of e-mail phishing

Is phishing the most frequent attack you have experienced?

Yes, this phenomenon began to appear since 2004, since then it has been raised. Criminal intention has extended from stolen victim's money, personal/confidential

information into exploiting victims in their implementation of the crimes and to blackmail or exploiting it for political and terrorist intentions

What is the number of successful phishing attacks? Is it increasing?

I don't have a figure

2. Review of organisational approach to phishing attacks

What is your strategy to protect the society from e-mail phishing attacks?

We are trying to limit them by:

1. Awareness
2. Enactment of laws that criminalize this phenomenon
3. Cooperation with other countries and competent authorities such as ICT and Ministry of Interior.
4. Trying to fight this phenomenon by participate in relevant conferences to find out the latest information and exchange views and experiences
5. Get aid from companies specialised in the Information security to consult in that matter

What actions do you take once you receive a case of e-mail phishing?

When we receive a complaint, we send it to justice after a preliminary investigation with the assistance of the technical department and then we follow the procedure for the issue.

What problems do you face in e-crimes and, in particular, phishing crimes?

Since this type of crime is directed at modern banking and financial centres, in the belief of maintaining their reputation, they don't report these incidents. We require banks to change and increase their security measures and to report any case to the Central Bank and, in turns, they will inform us of the case. Also we sensitise and make them aware that failure to cooperate with us might have negative results on the economy of the country.

Victims prefer to keep private the damage that occurred to them from such attacks to avoid embarrassment and ridicule and most are unaware of the right measures to take or reactions at the crisis time to minimise the possible damage

We face problems in making people aware of such threat, since we found that through enhancing citizen's awareness on such cases, their confidence has begun to decline.

Also we find difficulty in proving the guilt of the offender since it is usually difficult to trace phishers who are most likely to get lost, usually they are from abroad where it is difficult to get hold of them and sometimes they use their victim's devices or names to commit their crimes. Also we find difficulties on understanding the terms associated with e-crimes and on how to deal with them and take the fair decision therefore, we usually rely on the ministry of interior investigation report provided to us.

Does your organisation consider awareness of phishing as an important method of defence?

Yes, because most of the cases are the result of ignorance or willingness to help. Most cases can use religious scruples, moral or humanitarian principles to deceive people. We cooperate with all competent authorities to educate the community towards limiting this phenomenon

What do you think is the best method for creating awareness and educating people about e-mail phishing?

The media

3. Interviewee opinions

How do you think Qatari culture affects people's responses to phishing attacks?

Of course, Qatari societies are religious, tribal and modernisation is new for them. Also they are not practising these new developments, especially in technology, which increases the vulnerability to such threats.

Do you think organisations are allowed to perform a phishing penetration test to examine their employees' vulnerability to phishing?

Yes, it would be legal only if employees have signed in their employment contract that they agreed to have such auditing but there are ethical issues that should be taken into consideration where employees should have their privacy.

Do you think Qataris are vulnerable to falling prey to e-mail phishing attacks? and why?

Yes, as I mentioned, because Qataris are generous and helpful and phishers try to use that to commit their attacks.

Do you believe country-specific factors such as (1) the vast development experience in Qatar in all sectors, especially the economy and ICT, and (2) the absence of an e-law, have assisted development of phishing in Qatar?

Yes, because there is currently an economic turnover, making Qatar an appealing goal to phishers and there is a massive development in communications which led to the increase in the number of Internet users who mostly have novice knowledge and usually use it for entertainment and are therefore unaware of the threats and risks associated.

Do you think the establishment of an e-law will help in reducing e-crimes, in particular phishing?

There is no special law on cyber-crimes to be consulted in such cases; however, the current law included some of these crimes. The law is not up to date; it was not modified since it was released in 2004 to include the recent and emerging issues of cyber-crimes.

Therefore, we created a new law specialist in electronic crimes in collaboration with all relevant bodies seeking access to a comprehensive law that covers all aspects, taking in the experiences of other countries in this area and it is developed to suit with the current and future developments.

I think this law will protect victims and help us to take power, there is a common saying, "When there is no punishment, people get awful ill-mannered".

Do you think Qatari people need more time to cope with the rapid development in ICT and technology in Qatar in recent years in order to understand not only their advantages but also to be aware of the threats associated with them?

Qatar is a rich country, and like other developing countries, it is developing and in a stage of conflict to keep up with modernity and modern technology. Therefore the community needs time to absorb this technology with its advantages and disadvantages

How aware do you think Qatari people are of the phishing threat? How to protect themselves? How to spot threats and how to react?

No, I think people are not sufficiently aware because there must be a comprehensive awareness from banks, financial institutions and the people.

Interview 6

Date of interview: 24th August 2009

Duration: Approximately 20 minutes

Interviewee: Dr.Khalifa Jassim Al-Kuwari, Voluntary Administrator, Ministry of Endowments and Islamic Affairs

1. Use by phishers of religious, emotional and moral issues

Phishers exploit victims' emotions, morals and religion to commit their crimes. Why do you think this is successful in Qatar?

Because it is part of Qatar culture that people are generous and helpful, especially when it touches their emotions, ethic and morals, which phishers could use to get victims.

Should your Ministry make people aware of such a threat? What effect would this have on people (e.g. they may not trust others, become unhelpful)?

We have established a license for some charities and Red Crescent Societies to collect charity and Zakat from individuals and institutions and send to beneficiaries after checking a lot of things such as ensuring their dissociation from terrorist organisations and their non-exploitation against the security of the countries. Also, we have assigned delegates in many countries in the world to verify the arrival of these funds to eligible applicants.

Are there some people who refer to you once they have been tricked by phishing? And what do you advise them?

Yes, we receive a lot of calls saying that they receive messages or calls from a person or an institute requesting funds for charities and they ask us to ensure whether it is legitimate or accredited. We therefore direct them to deposit their charities with us and we will check whether if they are eligible applicants and then we provide them with the money. We also make people aware to donate for accredited institutions and individuals only.

Unfortunately, enhanced awareness on the topic could result in negative impact on those in need, since it will create a kind of lack of confidence in any message received, even if it was correct. Furthermore, people becomes doubtful in urgent humanitarian cases, such as the need for blood donation and disasters donations

Have you experienced such cases of attack in Qatar?

Yes, we have experienced a lot of suspicious charity centres which we then try to close if possible.

Interview 7

Date of interview: 25th August 2009

Duration: Approximately 30 minutes

Interviewee: Director of one of the high schools in Qatar, Ministry of Education and Higher Education

1. Best process for education and awareness

What do you think is the best method for awareness and educating people?

It depends on their age. For example, children prefer games and indirect ways of learning, while adults might prefer media and some do prefer seminars and distant learning (e-learning).

Does people's background play a big role in awareness?

Yes, as I mentioned before.

What are the best conditions for increasing awareness? How to get people interested, especially in such topics?

First, the awareness has to be well planned with a clear aim and objectives. The place should be appropriate and include all of the required tools and it would be preferred if the awareness tools are interactive and interesting to keep people engrossed (e.g. avoid formal interaction, add some fun to the training by having some jokes, related stories and keep everything simple and related to something they are familiar with to help them to remember). Finally, it would be beneficial to provide a certificate of approval to recruit them.

How to assess the awareness programme?

It is not easy to assess, but personal observations, simple test, well designed questionnaires and interviews with participants might help a lot in evaluating the effectiveness of the programme in enhancing their awareness level.

How to get people to remember what they learned?

Either by having a tool to get people to remember the principles or by demonstrating them in a simple diagram presented by pictures. However, some will remember things if they have been encountered or if they are repeated to them on a daily basis such as having them on their screen savers, so it depend on the personality of each participant. However, a lot of research has been done in this area, so it is better to have a look at it.

2 Processes deployed for phishing awareness

Does your organisation play a role in educating people about cyber threats, in particular e-mail phishing? If no, do you want to do so?

No, we actually think awareness of phishing should not be involved in the curriculum, since it is contrary to the values and principles that we try to install in our students such as trust and kindness. Therefore, we are studying this subject and trying to make students aware far from the curriculum by collaborating with organisations with responsibility in this field such as the Ministry of Interior and ICT.

3. Interviewee opinions

If no, do you think it is important to have some material about such threats in academic institutions to make students aware?

Yes, of course. Students have to know the threats of the Internet.

Do you think Qatari people need more time to cope with the rapid development in ICT and technology in Qatar in recent years in order to understand not only their advantages but also to be aware of the threats associated with such technology?

Yes, I do.

Interview 8

Date of interview: 27th August 2009

Duration: approximately 15 minutes

Interviewee: Computer lecturer, Institute of Administrative Development

I went to the Institute of Administrative Development since I thought it is responsible for staff development in Qatar and met one of the computer lecturers who asked me to not mention his name. He explained that the institute aims to develop the capacity of employees in topics such as time management and how to use the computer desktop and things like secretarial skills. When questioned why they do not involve awareness on e-crimes in general, he replied that employers are the ones who have to include such training not the Institute, since its main objective is to develop employees in Qatar with high school education to raise their operation in computer and secretarial work but then it had been circulated to some employees.

Interview 9

The author was interested in interviewing an organisation which does phishing audits for other organisations. However, there was no such organisation in Qatar. Finally, a UK company, First Base Technologies, was discovered which is a leader in providing information security and testing services. It also does social engineering audit for organisations. Mr. Peter Wood, Chief of Operations, First Base Technologies, was interviewed by a structured questionnaire sent by e-mail due to the author's inability to arrange a face-to-face interview. The following are print screens of communications with the company:

▶ Subject: Re: Could you please please fill out my questionnaire....	From: Peter Wood
This message has attached files. Show	

Hello Mariam

I have now completed your questionnaire - I hope this is useful. Please let me know if you have any further questions.

kind regards
Pete

At 16:40 22/03/2009 +0000, M.K.J.Al-Hamar@lboro.ac.uk wrote:

Dear Mr. Peter

*I have attached it again I hope it would be fine now and if not please let me know.
I hope you would contribute in the questionnaire.*

Thanks a lot for your help and support

Best regards

Mariam AL-Hamar

Note: You may choose **one answer only** You may choose **more than one answer**

Q1: What is your level of knowledge about e-mail phishing (also called scams or fraud e-mails)?

None Poor Average Good Expert

Q2: Do you think e-mail phishing incidents are?

Increasing Decreasing Stable Don't know

Q3: Do you worry about e-mail phishing?

Yes No

Q4: Do you think e-mail phishing is still hard to protect against?

Yes, please specify why

No, please specify why

Don't know

Q5: Why do you think people are vulnerable to being deceived by phishing e-mails?

They don't install a software to prevent phishing e-mails and websites (e.g. anti-phishing, spam filters)

The e-mail appears with sense of urgency and surprise

Lack of awareness and training about phishing

Phishers are coming up with smarter tricks which make it difficult to identify phishing

They trust the e-mail because they don't know about phishing

They are not aware of the importance of the information they have disclosed

The fake website looks almost identical to the legitimate one

Other

Some people believe that they won't be tricked

Q6: How do you rank your organisation in identifying phishing e-mails?

Zero Poor Average Good Expert

Q7: How do you find the demand for anti-phishing services by clients has been?

Increasing Decreasing Same Don't know

Q8: Does your organisation keep statistics on detected / intercepted phishing e-mails?

Yes No

Q9: How often does your organisation receive phishing e-mails?

Daily Weekly Monthly Never Others

If you answer Q9 Never, then please skip Q10 and Q11.

Q10: How many times has your organisation been attacked with phishing e-mails?

- Never Once Twice 3 times More than 3 times Don't know

Q11: How does your organisation spot phishing e-mails?

User education on best practice, personal firewalls.

Q12: What is your procedure for client anti-phishing services (i.e. Your methodology to prevent phishing)?

We are purely penetration testers, so we do not provide this service. However, we do offer social engineering services to test for susceptibility to phishing.

Q13: What services does your organisation provide for clients to develop defences against e-mail phishing?

- Install effective spam filter or anti-phishing software
- Define clear and reasonable security policies and guidelines addressing phishing (e.g. Don't give your password through e-mail, check web address, etc.)
- Explain guidelines and policies to employees
- Make clients aware and educate them about phishing.
- Carry out penetration test (i.e. A fake, non-harmful phishing e-mail will be sent to employees, only to educate employees and to measure their response to phishing e-mails). Please specify how it is done.
- Develop incident management process to report phishing incidents and respond to them. Please specify how it is performed
- Develop effective measurement process to measure organisation's vulnerability to phishing attacks. Please specify how it is done
- Others, please specify

Q14: Which of the following methods does your organisation offer your clients to deploy in awareness and training against e-mail phishing?

- Computer-based game Videos Cartoons Posters Web-based e-learning Media
- Seminars Newsletters and documents Screen savers Others

Q15: Which of the following actions does your organisation take when tricked by a phishing e-mail?

- | | |
|-----------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> Do nothing | <input type="checkbox"/> Change account details revealed |
| <input type="checkbox"/> Report incident to company whose e-mail address or Web site was faked. | <input type="checkbox"/> Check financial statements immediately |
| <input type="checkbox"/> Report incident to police or institute specialising in dealing with these cases. | <input type="checkbox"/> Cut up credit and debit cards |
| <input type="checkbox"/> Report incident to our bank | <input checked="" type="checkbox"/> Others <div style="border: 1px solid black; padding: 5px; display: inline-block;">We have never been tricked; however all of the above are good practice</div> |

Q16: What action does your organisation take for clients when they have encountered or have been attacked by phishing frauds?

Provide advice and refer to best practice.

Q17: What is your best practice for phishing that you mention in the survey? Is it standard policies and guidelines or is it defined by your company?

Our best practice is simple:

1. Never click on a link in an e-mail, but instead browse to the site manually
2. If in doubt, check e-mail message headers
3. Turn on anti-phishing function in Firefox (or Internet Explorer if you use it)
4. Always run Firefox with NoScript plug in (we don't permit our people to use IE)

Q18: How do you educate or train your clients on these practices?

Face-to-face seminars and podcasts with presentation slides. We also use articles in their in-house publications and on their intranet (see attached example).

Q19: How long does the training take?

About 1 hour for live session, about 20 minutes for podcast

Q20: Do you set up different training for different departments, e.g. for IT staff, other employees?

So far, we have trained only IT staff

Q21: How do you set up the training? Is it after the penetration testing or before?

This is not connected to penetration testing, but is part of the security awareness training programmes

Q22: Do you carry out auditing after the training to see whether the clients are still aware of phishing or not?

No, that is their responsibility in all projects so far.

Q23: How do you motivate employees to attend the training? Bearing in mind that not all employees are interested to know about phishing?

That is also the client's problem!

Q24: About yourself:

A. Country

UK

B. Occupation

Your employer

First Base Technologies

Your job title

Partner, Chief of Operations

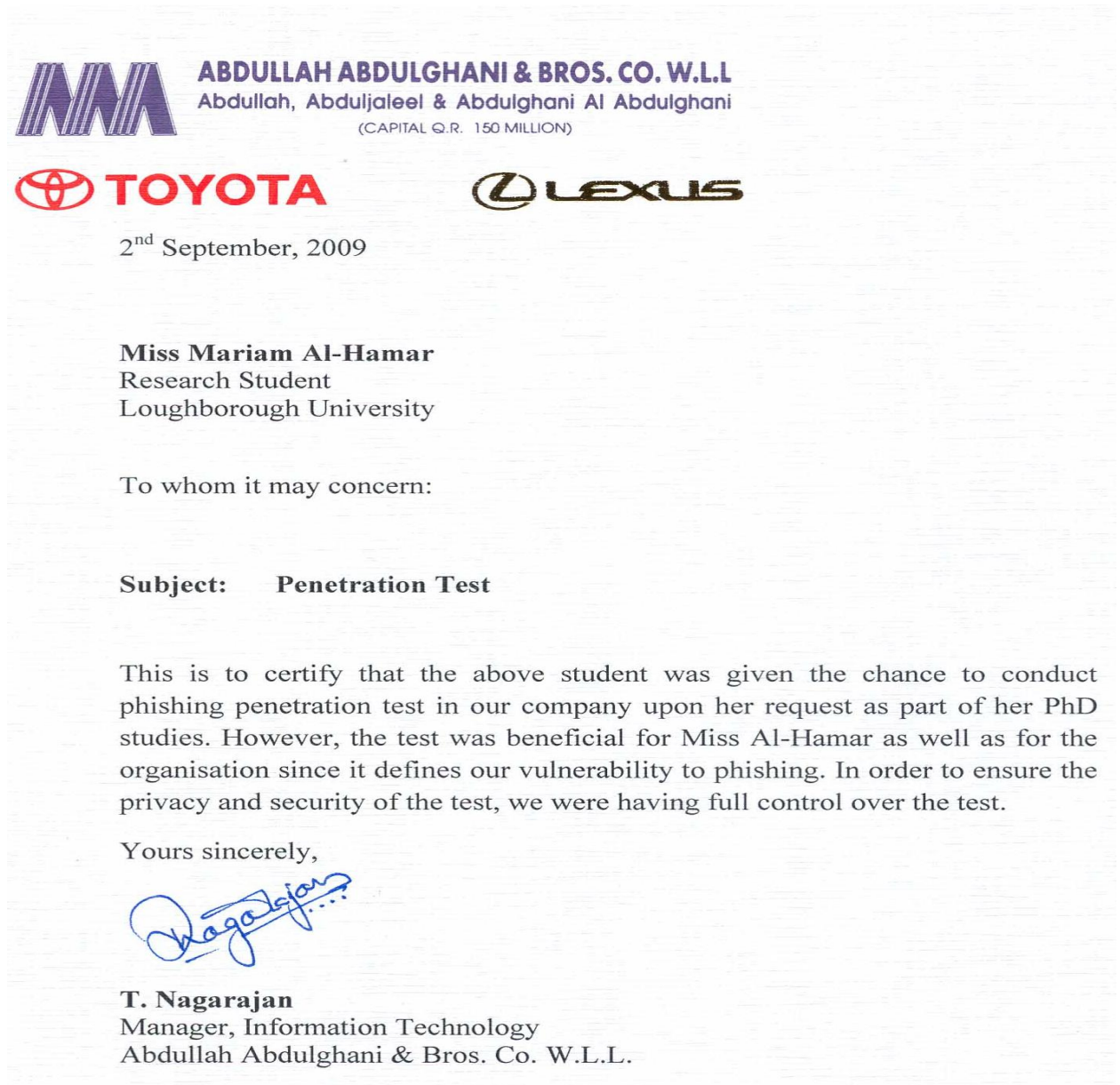
If you would like to find out more about the topic, please do not hesitate to contact me: Mariam Al-Hamar, research student (PhD), Loughborough University, UK. My email: m.k.j.al-hamar@lboro.ac.uk

Appendix C: Penetration Tests and Laboratory Experiment

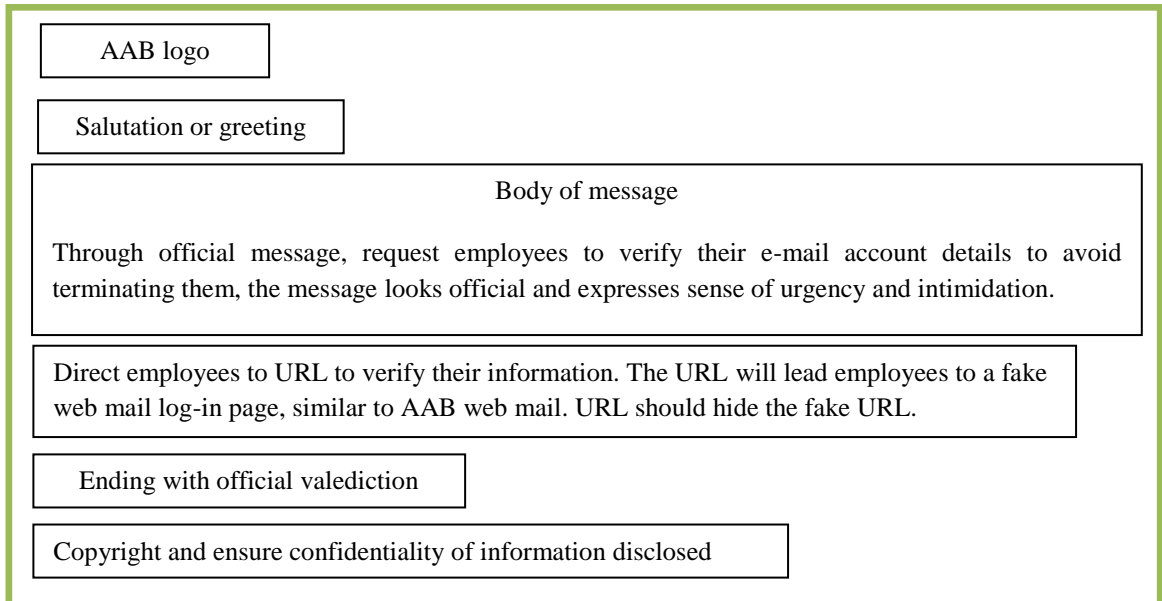
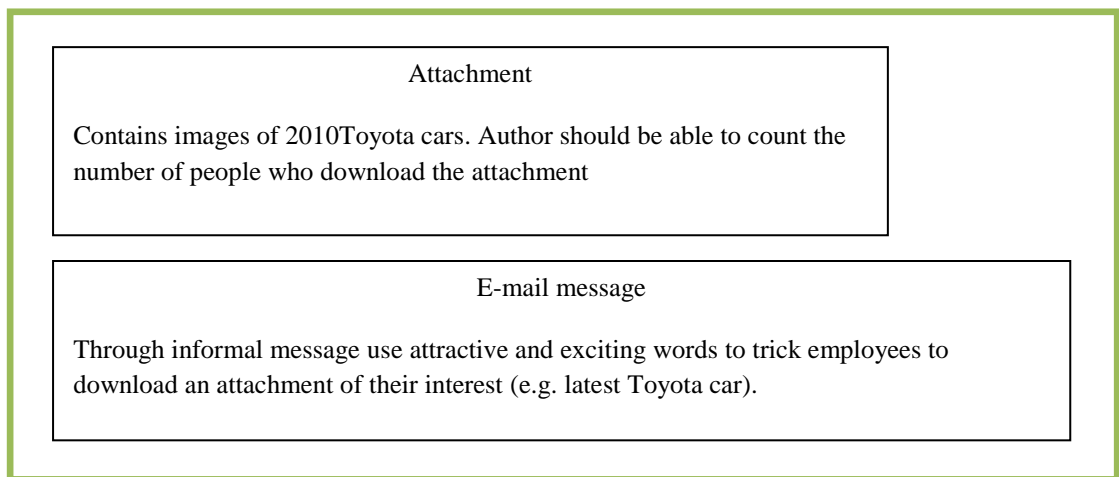
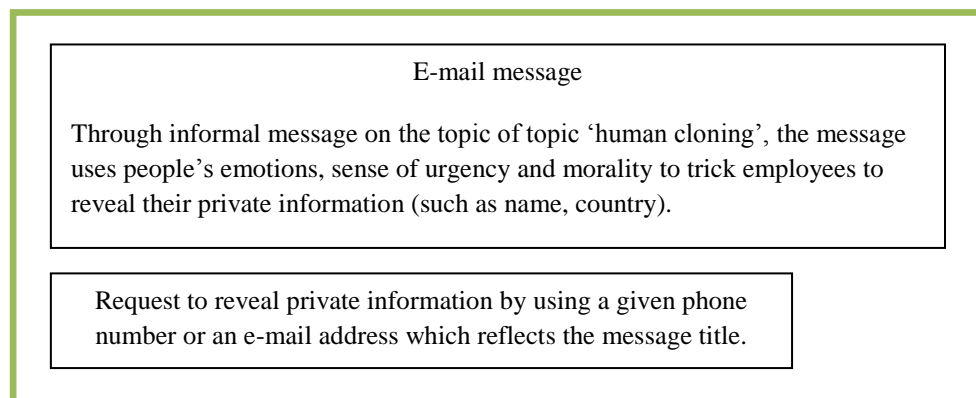
C1 Penetration test 1

- **Planning**

The researcher first obtained approval from AAB for conducting the experiment in their premises but with a condition that it would be run under their control (see letter below).



A team of IT personnel in AAB were then involved in the planning of the three phishing e-mails for the study which were agreed as follows:

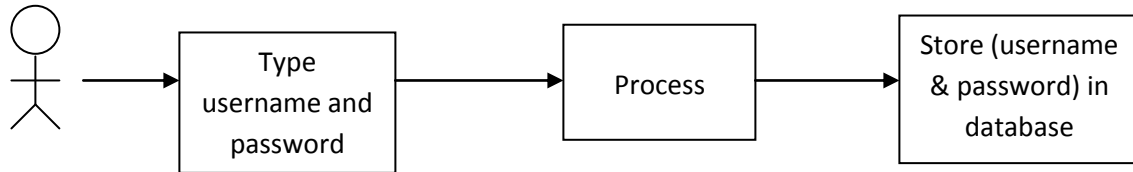
E-mail 1: Request account verification**E-mail 2: Request to download attachment****E-mail 3: Request private information via e-mail or SMS.**

- **Designing**

E-mail 1: Request account verification

Theoretical design of fake webpage:

The following diagram illustrates the process of AAB fake webmail:



The webpage is implemented in Macromedia Dreamweaver 8. MySQL was used to store employees' account details (username and password) and PHP was used as middleware to process these data. The main reason for choosing PHP is that it is open source software and is widely used and supported by internet service providers. MySQL was chosen because it supports multi-user connections, it is open source, compatible with PHP and widely supported by ISPs.

WAMP Server is installed on the administrator PC; it consists of PHP, MySQL and Apache Server. This allows running the developed webpage on one machine without the need to upload files to a remote server for testing purposes.

Database Design

The MySQL database file (login) keeps records of employees' login details, the table below shows the fields contained in the login database table:

ID	int (integer), unique and auto-incremented.
Username	Employee username - a character.
Password	Employee password - a character.
Date/time	Date and the time of swiping the card, in 0000-00-00 00:00:00 format.

Basically, the ID gets increased by a factor of (1) each time any data are entered or recorded, so in this case each entry has its own ID to make it easy to deal with each entry individually as well as allowing the database to distinguish between various entries. Employee username, password and date and time will be recorded automatically when the employee logs in.

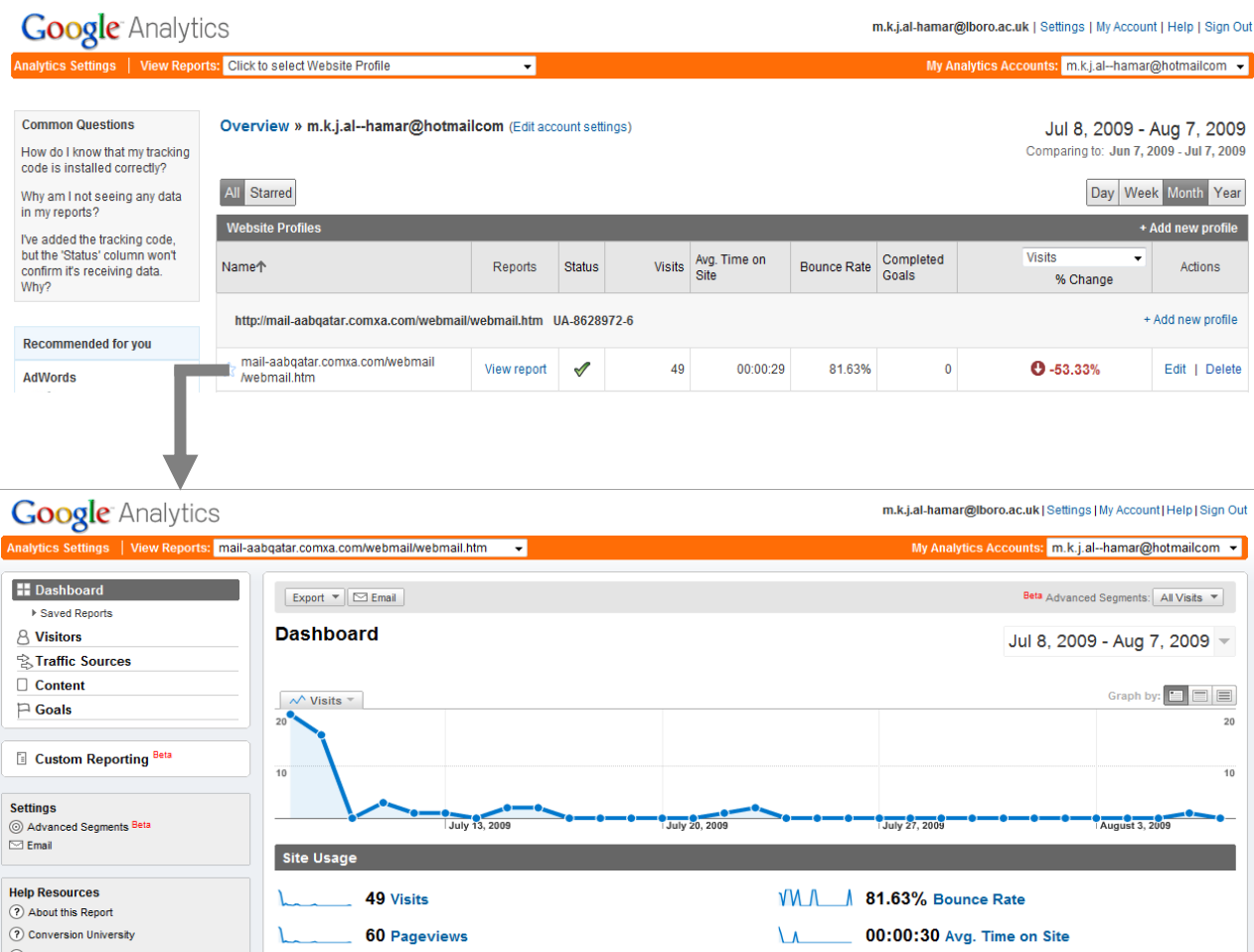
PHP design

After the database was planned and structured, the PHP design was developed. Macromedia Dreamweaver was used as a tool in the designing of the webpage and generating the appropriate PHP codes for different tasks. In the following sections, the folders will be explained with all codes and screen shots that will visualise the project.

Below is the PHP source code for the fake webpage:

```
<?php
$host="mysql9.000webhost.com"; // Host name
$username="a7836896_moi"; // Mysql username
$password="Alhamar6"; // Mysql password
$db_name="a7836896_moi"; // Database name
$tbl_name="guestbook"; // Table name
// Connect to server and select database.
mysql_connect("$host", "$username", "$password")or die("cannot
connect server ");
mysql_select_db("$db_name")or die("cannot select DB");
$datetime=date("y-m-d h:i:s"); //date time
$username=$_POST["login_userid"];
$password=$_POST["login_password"];
$sql="INSERT INTO $tbl_name(name, email,
datetime)VALUES ('$username', '$password','$datetime)";
$result=mysql_query($sql);
//check if query successful
if($result){
echo "Successful";
echo "<BR>";
}
else {
echo "ERROR";
}
mysql_close();
?>
```

The fake webpage will count the number of visitors using Google analytics tool, a free tool which enables the website owners to monitor their website traffic (see Figure below). This was done simply by adding a simple code provided by Google analytic to the end of the HTML body, so that all website visitors will be recorded in Google analytics. This was beneficial since the author can know the number of employees who enter the website but do not verify their account information. The fake website was hosted in the free webhosting website 'http://www.000webhost.com/'. According to Google analytics, 49 employees entered the fake website; however, according to the results provided from the AAB team only 19 of them verified their account information



E-mail 2: Request to download attachment

This e-mail seeks to trick AAB employees to download an attachment of interest which is 'Latest Toyota car', containing images of 210 Toyota cars.

It was important that the author should know the number of employees who failed in the attack and downloaded the attachment; therefore to know the latter number, the author designed a HTML file with a simple code to redirect users automatically to a website containing pictures of Toyota cars and also a counter using Google analytics tool to count the number of visitors to the site. According to the Google analytic tool, in total 33 employees fell prey to the e-mail by downloading the attachment (see figure below).

The redirecting code was the following:


```
<meta HTTP-EQUIV="REFRESH" content="0; www.mail-
aabqatar.comxa.com/webmail/toyota.html">
```

where 0 is the number of seconds' wait before redirecting. Set to 0, it redirects straightaway to the URL www.mail-aabqatar.comxa.com/webmail/toyota.html.


Attachment redirecting to URL below

<http://www.mail-aabqatar.comxa.com/webmail/toyota.html>

2010 Toyota Prius



2010 Toyota Camry Hybrid



Check out the latest Toyota model

From: **mariam alhamar** (arab_eyes@hotmail.com)

Sent: Sunday, May 17, 2009 10:39:47 PM

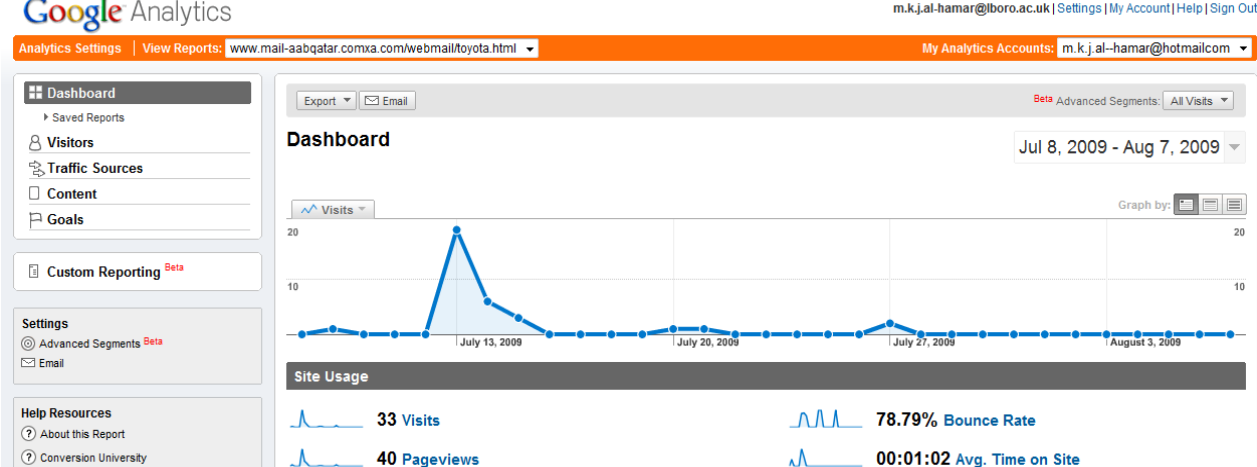
To: itmtoyota@qatar.net.qa; nagaraj@aabqatar.com

1 attachment
LatestToy...htm (0.7 KB)

Check out the latest and the most inventive Toyota car model in the market.

Go on and Download the attachment.

The website contain counter



E-mail 3: Request private information via e-mail or SMS



This e-mail was easy to design and the author wrote a message which tried to trick people to provide their private information (name and country) via e-mail or SMS by playing on people’s morality and emotions. The decision was to write a message about ‘human cloning’, trying to convince people to support a petition against human cloning by providing their private information. It was expected that this would trick people since human cloning is unacceptable on humanitarian, ethical and social grounds and people might thus think that giving their information will save humanity (see Figure below). Note:

the phone number supplied in e-mail 3 was changed by AAB to another mobile number in Qatar where they have more control.

Please don't ignore this e-mail

From: **mariam alhamar** (arab_eyes@hotmail.com)
 Sent: Sunday, May 17, 2009 10:40:43 PM
 To: itmtoyota@qatar.net.qa; nagaraj@aabqatar.com

Currently, a group of scientists in the United States is engaged in cloning children. It is well known that human cloning is unacceptable in terms of the humanitarian, ethical and social grounds. Many religious scholars believe that human cloning undermines the sanctity of human life.

If you are against human cloning please support our petition by sending your name and your country to this e-mail (human_rights@live.co.uk) or by sending an SMS to this number  (00447846622760) 

After 14 days this information will be presented to the Commission on Human Rights towards stopping this project.

You can save humanity, please don't hesitate in supporting our petition.

C2 Penetration test 2

- **Planning and design**

Participants' characteristics and interests

Members of the researcher's family and relatives were chosen to be victims of the spear phishing experiments; they were carefully chosen to represent a sample of Qatari e-mail users. Participants were half male and half female, each with different backgrounds in terms of age, education, occupation and computer knowledge. To ensure participants' privacy, names were identified by their initials (i.e. First and surname).

Age: 6 are below 18, 19 are 18-29, 3 are 30-50 and 2 are over 50

Education: 15 school, 12 higher education, 3 postgraduate education

Occupation: 16 students, 7 employees, 4 are both employees and students, 7 others (e.g. retired or housewife) and 2 businessmen.

Computer knowledge based on author's judgement: 8 poor, 8 average, 7 good and 7 with expert knowledge

No.	Participant initials	Computer knowledge	Age	Education	Occupation
1	A K 1	Poor	15	School	Student
2	Y K	Poor	14	School	Student
3	J A	Poor	14	School	Student
4	F S	Poor	51	School	Housewife
5	S A	Poor	20	School	Housewife
6	K J	Poor	53	Higher education	Retired
7	I A	Poor	14	School	Student
8	H A	Poor	14	School	Student
9	S Y	Average	19	Higher education	Student
10	S O	Average	20	Higher education	Student
11	T A	Average	27	School	Employee
12	A K 2	Average	20	Higher education	Employee/ student
13	M A 1	Average	16	School	Student
14	M H	Average	18	Higher education	Student
15	M A 2	Average	42	Higher education	Retired
16	A J 1	Average	37	Higher education	Employee
17	F M	Good	18	School	Student
18	N J	Good	39	School	Housewife
19	M A 3	Good	19	Higher education	Student
20	N A 1	Good	19	School	Student
21	N M	Good	26	School	Employee
22	M Z	Good	23	School	Housewife
23	A J 2	Good	27	Higher education	Employee/ businessman
24	A K 3	Expert	26	Postgrad	Employee
25	J K	Expert	23	Postgrad	Employee/ student
26	N K	Expert	27	Higher education	Employee
27	H J	Expert	26	Higher education	Employee
28	N A 2	Expert	19	School	Employee/ student
29	A Z	Expert	25	Postgrad	Employee/ student
30	A J 3	Expert	25	Higher education	Retired/ business man

Before designing phishing e-mails, the interests of each victim were identified, this knowledge was gained from the long relationship of the victim with the researcher since they are members of her family and relatives.

No.	Interests
1	Games and downloading Arabic movies and series
2	Mobiles and motor cycles
3	Photography and chatting
4	Cooking recipes and interior design
5	Games and watch TV channels online
6	Reading newspapers and buy/sell in Qatar share market
7	Cars and Motorcycles and looking for friendships online
8	Chatting and watching movies in Youtube
9	Downloading English scary movies and look for makeup and hair styles.
10	Look for strange things such as furniture and dresses and register in forums and read articles on cooking and decorating
11	Photography and buying dresses and things from forums
12	Cars, chatting and horoscopes
13	Downloading Arabic movies and shopping
14	Downloading Arabic movies and listen to music
15	Reading religious articles and paying Zakat online
16	Watch short videos in YouTube and chatting
17	Register in forums, read articles on cooking and decorating and looking for new designs of Jewelleries and accessories
18	Buying brand-name bags (e.g. GUCCI) and looking at new styles of furniture
19	Use the Facebook and look for dressing, make-up and hair styles.
20	Learning English and computer online and reading stories and books
21	Cake decorating Religious articles
22	Handcrafts and cooking
23	Buy and sell shares online and read articles about shares and business in Qatar
24	Looking for affordable hotels and ticket offers and listen to and download music
25	Reading topics on computing and downloading new programs and applications
26	Reading articles on computing and downloading movies
27	Games and follow-up artists' news
28	Drawing and handcrafts
29	Cars and follow-up sports news
30	Read newspapers, political articles and books and follow-up economic news

Phishing e-mails were based on victims' interests. Although it was hard to use each interest for each victim, only one interest was chosen, unique and not common to other victims towards having a broadened experiment study where e-mail phishing was designed for each victim by using just one of their interests to assess their vulnerability to falling prey to phishing attacks. Table shows interest used for each victim along with the subject and the language of the designed phishing e-mail.

Design of Spear phishing attack

No	Interest used	Spear phishing e-mail Language used
1	Downloading Arabic movies and series	Free and fast downloading for Arabic TV series of high quality. (Do you want to watch the latest Arabic TV series? Then register in the website below to enjoy free and fast downloading with high quality. Don't miss out)
2	Motor cycles	Cheap prices of latest Motor cycles to enjoy summer (Do you want to enjoy summer with your friends and family in <i>sealine</i> ? Here are cheap motor cycles to rent long term. For more information contact this number.
3	Photography and visiting Flickr website	The best 10 chosen pictures on flickr (don't miss to see the best 10 chosen pictures on flickr by flicker website, pictured are in the attached file above)
4	Cooking recipes	New food recipes for the family in Ramadan (You want to be different this Ramadan, you want to make something new, visit the following website for new healthy food recipes for your family this Ramadan)
5	Games	Assess your intelligence, play the most intelligent game in the world for free (Aisha has invited you to play this game to assess your intelligence, she have scored 620, can you beat this score, then go on to play this most intelligent game in the world. It's free)
6	Reading news papers	We can deliver for you 'Al-Sharq' news papers to your home daily for only 200 QR per year. Don't miss out this offer it is limited
7	Looking for friendships online	(Sarah has invited you to see her new pictures on her Facebook account)
8	Watching movies in Youtube	Look at the most viewed movies in Youtube
9	Look for makeup and hair styles.	Are you stylish? Do you want to be a beauty expert? You have the chance to be one now by just joining our beauty course for free. It will guide you step by step.
10	Register in forums and read articles on cooking and decorating	You can find a wonderful and unique home decorating just join "Aldecor" forum and you will receive a free magazine
11	Buying dresses and things from forums	There are new collections of fabulous dresses for Eid which will make you special.
12	Cars	You can win a Lexus car for free, you just have to join the big raffle which will be held after Ramadan. To join fill in your details in the attached file and forward it to us.
13	Shopping online for dress and bags	Does it cost you a lot to buy luxury and branded clothes You can get one for cheap prices. Click on this URL.
14	Listen and download	For all those who love the singer Yara, here is her new video clip.

	music	
15	Paying Zakat online	Zakat <i>al-Fitr</i> is a duty which is required of every Muslim at the conclusion of the month of Ramadan as a token of thankfulness to God for having enabled him or her to observe the obligatory fast. You can pay your 'Zakat Al-Fetr' online with few clicks. God bless you all
16	Chatting	Do you want to know the one who blocks you in MSN. It's Easy, Secure and Free! Try it Now, Click Here
17	Looking for new designs of jewellerys and accessories	For every woman who loves Jewellerys and would like to be always special and attractive. 'Damas' offers you new collection of Jewellerys for Eid.
18	Buying brand bags (e.g. GUCCI)	It is amazing, look at the branded bags below, They are actually cakes.
19	Horoscopes	Do you believe in Horoscopes? You can receive your daily Horoscopes for free. Just join into this website.
20	Reading stories and books	Here are 2 English novels to help you learn the language Undercover White Trash The Mars Run Download and see how interesting they are.
21	Religious articles	Every Muslim has wondered how to spend his time in Ramadan? It is actually easy, just read this article 'How to invest your time in Ramadan'
22	Hand crafts	Look at the fantastic collection of wrapping for weddings and births celebrations.
23	Read articles about shares and business in Qatar	Are you a business man and worried about your state in the market after the world financial crises? The article below forecasts the status of Qatar share market after the world financial crises.
24	Looking for affordable hotels and ticket offers	Don't miss out, 35% discount for Intercontinental hotels this month. Don't miss out on this bargain.
25	Downloading new programs and applications	New programs released by Microsoft.
26	Read articles on computing	The latest release of windows. Watch out for hot news on computing on [www.computing.com]. You can join for free.
27	Follow-up on Artists' news	The latest news of artists in this season.
28	Drawing	Sign up for the coming Arabic drawing exhibition.
29	Follow-up sport news	Do you want to be up to date with sport events in the world? Here is an electronic version for the Al-Reyada sport magazine.
30	Follow-up to	Economics are changing in 2010. To read more, visit this website.

	economic news	
--	---------------	--

All were in Arabic except for 4 participants: NA 1, AK 3, JK and NK since their level of English is pretty high and the topic needed to be in English.

- **Evaluation**

Interview questions

Evaluation was done after the experiment by holding semi-structured interviews with participants, according to their responses to the experiment, based on the following questions:

Do you usually open e-mails from unknown senders and in the junk?

Do you think it is a phishing e-mail? If yes or no, explain why?

Do you install anti-viruses or spam filters?

Do you know what phishing is?

If you fell prey to the e-mail:

What made you get tricked by this e-mail?

If he/she did not fall prey to the e-mail:

Did you open the e-mail? If no, why?

Why didn't you get tricked?

Examples of interviews

Example 1

Do you usually open e-mails from unknown senders and in the junk?

Yes, I do

Do you think it is a phishing e-mail? If yes or no, explain why?

Yes, because I have been tricked with phishing before so I have an experience

Do you install anti-viruses or spam filters?

Yes, I install anti-viruses but I don't know anything about spam filters

Do you know what phishing is?

Yes, it will attempt to steal my confidential information such as username and password

Example 2

Do you usually open e-mails from unknown senders and in the junk?

Yes, sometimes

Do you think it is a phishing e-mail? If yes or no, explain why?

No, because I did not know about phishing

Do you install anti-viruses or spam filters?

No, I don't install any of those

Do you know what phishing is?

No

If he/she fell prey to the e-mail:

What made you get tricked by this e-mail?

As I mentioned, I did not know about phishing since I have recently got my e-mail.

• **Summary of experiment findings**

- 17 out of 30 participants have been tricked by phishing e-mails
- 21 out of 30 did not know the term phishing.
- 18 out of 30 open e-mails from unknown senders and from the junk.
- 20 out of 30 have got anti-viruses in their PC, only 10 keep them up to date and only 4 have got spam filters

No.	Failed in experiment	Explanations of responses
1	No	It required registration and because it was in Arabic
2	Yes	It was a good offer I did not expect that I will get phished one day
3	Yes	I'm interested to see the best photos
4	Yes	I did not know about phishing I have recently got my e-mail and I don't know about e-mails
5	Yes	Lack of knowledge about phishing
6	Yes	It was in Arabic, that's why I trust it
7	Yes	I like making friendship online I don't think a lady could phish me
8	Yes	It was excited and I usually visit Youtube
9	Yes	I love to cope with fashion and it was for free I don't think there is phishing in beauty
10	Yes	It touches my interest
11	Yes	The timing for the test was appropriate where there are usually offers for fabulous dresses. Therefore I was not in doubt
12	No	Because I have heard of this kind of phishing before from friend
13	Yes	Offers are really cheap and I get used to buying from forums
14	No	Because I didn't want to hear music in Ramadan
15	Yes	Because <i>Zakhat al-Fitris</i> is required of every Muslim and I never thought there will be a cheat on that
16	No	I have heard about this program
17	No	I prefer to buy jewelleryes from shops
18	No	I prefer to buy bags from shops
19	No	I haven't checked my e-mail
20	No	I have opened the e-mail, but I downloaded the attachments because I didn't prefer to read from e-books.
21	Yes	I like to know how to get God's blessing in Ramadan
22	No	I have not got the chance to look at it
23	No	I don't open it because it is from unknown sender
24	Yes	It was a good offer and I always look at hotels offers
25	No	Because it was from unknown sender, and because I have knowledge on phishing
26	No	Because it was from unknown sender and I have been tricked before with phishing
27	No	Did not check his e-mail and because I have knowledge on phishing
28	Yes	I love being in a drawing exhibition
29	Yes	I like to read sport news
30	Yes	I have not faced phishing before

Chi-squared test

Level of computer knowledge / Phishing detections	Poor	Average	Good	Expert
Correct	1	3	6	3
False	7	5	1	4

Data: contingency table

	A	B	C	D	
1	1	3	6	3	13
2	7	5	1	4	17
	8	8	7	7	30

Expected: contingency table

	A	B	C	D
1	3.47	3.47	3.03	3.03
2	4.53	4.53	3.97	3.97

Chi-square (χ^2) = 8.33

Degrees of freedom = 3

Critical chi-squared = 7.82

They are quite relationship between participant's level of knowledge and their ability to detect phishing attempts

C3 Experimental study

- **Planning and design**

Participants' characteristics

30 people participated in the experimental study, each with different backgrounds in terms of e-mail phishing level of knowledge, age, education and occupation. Below shows the demography of participants, participants were asked to fill out the below table:

E-mail phishing level of knowledge: 10 poor, 8 average, 7 good and 5 with expert knowledge

Age: 15 are 18-29, 11 are 30-50 and only 4 are over 50


Education: 8 school, 19 higher education, 3 with post graduate education



Occupation: 13 students, 14 employees, 2 are both employees and students and 3 others (e.g. retired or housewife or unemployed)

No.	Participant	E-mail phishing knowledge	Age	Education	Occupation
1	D K	Poor	28	School	Employee
2	F L 1	Poor	31	Higher education	Student
3	W M	Poor	51	Higher education	Employee
4	S N	Poor	18	School	Student
5	A S	Poor	30	School	Employee
6	T O	Poor	25	School	Student
7	A A	Poor	33	Higher education	Student
8	S M 1	Poor	18	Higher education	Employee
9	M S 1	Poor	53	Higher education	Employee
10	N S 1	Poor	19	Higher education	Student
11	A K	Average	32	Higher education	Employee
12	W J	Average	38	Higher education	Others
13	N S 2	Average	51	School	Student
14	M M	Average	22	Higher education	Others
15	A M	Average	20	Higher education	Employee
16	F O	Average	52	Higher education	Employee
17	F J	Average	28	School	Student
18	R M	Average	22	Higher education	Student
19	M S 2	Good	34	Higher education	Employee
20	F L 2	Good	24	Postgraduate	Student
21	K M	Good	34	Postgraduate	Employee
22	Y N	Good	24	Higher education	Student
23	J T	Good	36	Higher education	Student
24	H K	Good	26	Higher education	Employee
25	B M	Good	22	Higher education	Others
26	N K	Expert	41	School	Student
27	S M 2	Expert	30	School	Employee
28	J J	Expert	27	Higher education	Employee
29	H S	Expert	44	Postgraduate	Student
30	R D	Expert	29	Higher education	Employee

E-mail design

E-mail subject and language	Description
6 Phishing e-mails	
Fulfil your Zakat online (Arabic)	<p>Zakat is one of the 5 Pillars of Islam, in which as a Muslim it is our duty to contribute a portion of our earnings. All the contributions will then be used for a good cause and given to the right people. We are getting to Ramadan soon; it is a reminder to pay your Zakat before the blessing month.</p> <p>All you need to do is pay your Zakat online today! www.qzf.org.qa/zakat</p> <p>If you have already paid your Zakat, don't miss to pay Sadaka for people who need it, follow this URL: www.qzf.org.qa/sadaka forget to pay</p> <p>Help us in reminding other Muslims; don't let this message stop with you. Send it to your mail list and you will gain the blessing.</p> <p>Original site: http://www.zf.org.qa/</p>
You can know the person you loves who loves you (Arabic)	<p>Do you want to know the person who loves you in secret???</p> <p>Send this message to 15 people and then you can see an image of the person who loves you by clicking on this page http://your-love.c.la will</p> <p>You will be amazed when you know ... Image that will show you the secret to resemble the beloved 50%</p> <p style="text-align: center;">You haven't send the message to 15 people If you have sent it please re-visit after a while</p>
Q-tel downloads mozaic (Arabic)	<p>Dear Qtel customer,</p> <p>You have received Mozaic settings for free. Kindly SAVE/INSTALL and start enjoying the coolest Music, latest movies, plus more! www.mozaic.qa</p> <p>Original site: www.mozaic.qa</p>
Buy/sell your shares online (Arabic)	<p>The old website for Doha Securities Market (DSMC) has been changed. Now you can perform online securities trading in the new site of Qatar Eexchange (QE) in the following URL: http://www.dsm.com.qa/pps/dsm/portal/Pages/DSM_Home</p> <p>If you a businessman and you're tired of going to the Share market every day, the site offers you a secure online securities trading</p> <p>Original site: http://www2.dsm.com.qa/pps/dsm/portal/Pages/DSM_Home</p>
Help to enhance e-	Dear Qatari citizens

<p>services in Qatar (Arabic)</p>	<p>The Ministry of Interior would like to encourage people to use e-government services. You can check and pay your bills online such as traffic offences on http://www.mol.gov.qa/site/arabic/eServices/index.html</p> <p>Be aware that any delay in payment will consequently increase your payment</p> <p>Original site: http://www.moi.gov.qa/site/arabic/eServices/index.html</p>
<p>Carrefour promotions Poster (Arabic/eng)</p>	 <p>The button directs to this fake site: http://72.32.124.138/carefour.com</p> <p>Original site: http://www.carrefourqatar.com/</p>
<p>4 Legitimate e-mails</p>	
<p>Doha Bank Travel Insurance (English)</p>	<p>Dear Doha Bank Account Owner,</p> <p>Buy Travel Insurance from Doha Bank and ensure peace of mind while on vacation. YOU will gain 50% discount, this offer is valid until 15/9/09. For details, call Doha Bank customer service 4257517 or e-mail: bancacpu@dohabank.com.</p>

<p>Protect from viruses and phishing (English)</p>	<p>Microsoft Phishing Filter Add-on for MSN Search Toolbar to protect yourself from viruses and phishing, download this software to your pc for free from Microsoft site.</p> <p>http://www.microsoft.com/mscorp/safety/technologies/antiphishing/at_glance.msp</p>
<p>You can win fabulous prizes in Dohasooq Poster (English)</p>	
<p>Invitation from Facebook</p>	 <p>Sign up button goes to the Original site: http://www.facebook.com</p>

Answer sheet for participants

Name:-----

Date:-----

Time spent:

100

Decide whether the e-mail is phishing, legitimate or don't know, and then tick in the appropriate field in the table below.

List of e-mails	Phishing	Legitimate
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

- **Evaluate participants' responses to study**

Results

Participants' level of detection was ranked from poor to excellent according to their responses to the study. Final results were as follows:

Participants' detection level	Scores	Number of participants	% of participants
Excellent	100	3	10
Very good	70-90	9	30
Good	50-60	11	36.7
Poor	Below 50	7	23.3

120 detections were wrong and the remaining 180 were correct. The amount of wrong detections varies for each e-mail in the study, as shown below:

No.	E-mail topics	Number of Wrong detections	% of Wrong detections
1	Fulfil your Zakat online	22	18.3%
2	You can know the person who loves you	11	9.2%
3	Q-tel downloads mosaic	8	6.7%
4	Buy/sell your shares online	15	12.5%
5	Help to enhance e-services in Qatar	5	4.2%
6	Carrefour promotions	4	3.3%
7	Doha Bank Travel Insurance	20	16.7%
8	Protect from viruses and phishing	19	15.8%
9	You can win fabulous prizes in Dohasooq	11	9.2%
10	Invitation from Facebook	5	4.2%
Total		120	100%

Grid matrices of participants' scores and wrong detections are shown in Table below:

Participants	Scores	Wrong detections
1	30	1, 2, 3, 4, 7, 8 and 5
2	60	1, 2, 4 and 7
3	50	1, 4, 8, 9 and 10
4	60	1, 2, 3 and 4
5	80	7 and 8
6	50	1, 2, 7, 8 and 9
7	80	1 and 9
8	20	1, 2, 3, 4, 7, 8, 9 and 10
9	70	1, 8 and 9
10	50	1, 2, 3, 7 and 9
11	60	6, 7, 8 and 9
12	80	1 and 5
13	60	1, 2, 7 and 8
14	30	1, 2, 3, 4, 7, 8 and 5
15	20	1, 2, 3, 4, 7, 8, 10 and 5
16	60	1, 7, 8 and 9
17	60	1, 6, 8 and 9
18	40	1, 2, 4, 7, 8 and 9
19	30	1, 2, 3, 4, 7, 8 and 9
20	50	1, 4, 6, 7 and 8
21	80	7 and 8
22	30	1, 3, 4, 6, 7, 8 and 10
23	50	1, 4, 7, 8 and 10
24	70	1, 7 and 8
25	100	None

26	70	1, 4 and 7
27	100	None
28	90	4
29	70	4, 7 and 5
30	100	None

- **Semi-structured discussion points**

In-depth discussions took place with participants after the study according to the observation grid matrix referred to above and the following semi-structured discussion points:

1. Were you aware of the phishing threat before?
2. For participants who took more time than allocated to complete. What was the reason for your taking more time than allocated?
3. Which of the given e-mails did you spend more time on to detect whether it was phishing or legitimate? And why?
4. For participants with scores less than 100. Look at the wrong detections, ask for the reason for such an answer and then explain the right detection.
5. Which was the most tempting phishing e-mail?
6. Which of the given e-mails was difficult/tricky to detect whether phishing or legitimate? And why?
7. Why do you think Qatari people could be vulnerable to falling prey to e-mail phishing attacks (e.g. effect of native language, kindness, etc.)?
8. How do you think Qatari culture affects people's responses to phishing attacks? Why is that? What are the possible cultural factors?
9. What do you think is the most successful trick that phishers could use on Qataris? Why?

10. What have you learnt from the study? Have you achieved new knowledge about phishing?

11. Did you find it useful? And what did you like and dislike about it?

12. Do you have any comments or suggestions on how to improve the study?

Summary of discussion outcomes

1. Were you aware of the phishing threat before?

Most participants stated that they were unaware of the phishing threat and few really noticed it.

2. Reason for taking more time than allocated

Most participants completed the study before the time allocated because a lot did not take enough time to recognise phishing attempts by inspecting security indicators and some were even guessing. Only a few participants spent more than the time allocated for the experiment and they explained that this was due to their confusion on making the right detection, especially for the e-mail which provided a free tool to protect from viruses and phishing since some phishers use this trick to get their victims to fall to phishing.

3. Which of the given e-mails did you spend more time onto detect whether phishing or legitimate? And why?

The following e-mails: Q-tel downloads mosaic, buy/sell your shares online, help to enhance e-services in Qatar and invitation from Facebook were more confusing phishing e-mails since the URL given was a fake but with only slight difference that was hard to notice. Some participants were confused by the legitimate Facebook invitation because of recent exploitation of Facebook by phishers.

4. For participants with scores less than 100. Wrong detections looked at, participant asked for the reason for such answer and then right detection was explained.

No.	E-mail topics	Reason for wrong detections
1	Fulfil your Zakat online	<ul style="list-style-type: none"> - I trust Zakat fund institute - It used people's emotion, beliefs and religion - The fake website was similar to the official site - I trusted it because it was written in my native language (Arabic)
2	You can know the person who loves you	<ul style="list-style-type: none"> - It was exciting and interesting to me - Utilising my emotion - I love adventure - Usually phishing written in English - It required distributing the e-mail to my contact list which was strange
3	Q-tel downloads mosaic	<ul style="list-style-type: none"> - The fake website looks similar to Q-tel official site - It is trusted Q-tel institute - The e-mail uses common kind of e-mail send by Q-tel - I was in my native language (Arabic)
4	Buy/sell your shares online	<ul style="list-style-type: none"> - It used the event of changing the website for online securities trading from Doha Securities Market Company into Qatar Exchange website. - I used to buy and sell my shares online since it is secure and trustful. - A very minor difference in the fake URL - It attracted my interest - It was in my native language (Arabic)
5	Help to enhance e-services in Qatar	<ul style="list-style-type: none"> - Uses official communication - The Ministry of Interior is a trusted governmental institute - I've been using e-governments services before with no problems - I get intimidated with the urgency and penalty payment - It was written in Arabic
6	Carrefour promotions	<ul style="list-style-type: none"> - It is frequent e-mail sent by Carrefour supermarket - It used a poster which is hard to be faked - I did not recognise the fake URL because it was embedded in a button within the poster - We were in the event of going back to school; therefore it attracted my attention, needs and excitement to see the new promotions.
7	Doha Bank Travel Insurance	<ul style="list-style-type: none"> - Usually phishing targets banks and financial institutes - The discount of 50% made me a bit suspicious
8	Protect from viruses and phishing	<ul style="list-style-type: none"> - Some phishers use this trick to get their victims to fall to phishing by attempting to help them to avoid phishing but they are really phishing people. - Microsoft was a common target for phishers
9	You can win fabulous prizes in Dohasooq	<ul style="list-style-type: none"> - It contain sense of excitement by offering fabulous prizes which is usually used by phishers
10	Invitation from Facebook	<ul style="list-style-type: none"> - Recent exploitation of Facebook by phishers - The invitation came from unknown person

5. *What was the most tempting phishing e-mail?*

The e-mail which can know the person you love; this was unexciting and clever trick which attracted people's emotions and beliefs about love.

6. *Which of the given e-mails was difficult/tricky to detect whether phishing or legitimate? And why?*

The e-mail which let you know the person you love since it was exciting, interesting and adventure. However, I was confused that it might be phishing when it required sending the e-mail to my contact list.

7. *Do you think the culture affects people's responses to phishing attacks?*

Yes, it has a major influence of Qataris responses to phishing, the natures of Qataris are trustful, and generous, that's in the culture of Qatar. Also, the religion 'Islam' has a major effect on people's life style and in being good willed and trustful.

8. *Why do you think Qatari people could be vulnerable to falling prey to e-mail phishing attacks (e.g. effect of native language, kindness, etc.)?*

After analysing results, the following factors make Qataris vulnerable to phishing:

1. Qataris are friendly and like making friends and knowing people
2. Qataris feel embarrassed and stupid to report phishing and mention that they had fallen prey to it, that's in their nature.
3. Qataris are affected by the manner of incentives and disincentives which can sometimes lead to circulation and exchange of phishing e-mails and sites among people, which gives it credibility
4. Confidence and trust of friends, this gives the phishing e-mail credibility if it is sent from a person they know.
5. Trust of official communications and of official trustworthy institutes in the society
6. Influence and trust of the native language (Arabic)
7. Courtesy for people, even in giving your confidential information

8. Lack of knowledge on Internet threats and in particular phishing threat since a lot did not absorb the technology, especially with the rapid development in technology experienced in Qatar. This led to the following:
9. A lot expect the limitation of contact for phishing (i.e. they think phishing is usually in English or has not reached Qatar where it is not limited to a geographical area) and the limitation of topics that phishing uses (e.g. disbelief in the existence of phishing in religious and art topics).
10. Some have overconfidence in technological tools, especially anti-viruses, for protecting against all kinds of phishing.
11. Some people have overconfidence in the technical revolution and that everything in the Internet is true.
12. Some do not know how to detect and react and protect against phishing attacks
13. Qataris are motivated by religious and moral conditions in being helpful, generous, emotional and good willed in showing philanthropy, compassion and clemency, especially for people in need, in particular in religious seasons, and in disasters, particularly with the existence of a lot of disasters and famines around the world. This makes people believe phishing e-mails which exploit it, especially with the media coverage of other events which happened in Qatar society.
14. People are trustful and not donot have bad faith in people
15. Seek for curiosity and knowledge and discovery, especially in matters of their interests.
16. Amenable to different kinds of temptations, to satisfy their desires, needs and beliefs, such as magic, superstition , envy, horoscopes, astrology and Jihad, either with money, spreading thought or propagation of religion)
17. Believe that he/she does not have anything to be stolen or worth stealing
18. Overconfidence of their knowledge and thought that they will not be tricked

9. *What do you think is the most successful trick that phishers could use on Qataris and Why?*

Phishing attacks which exploit Qataris' emotions, morals and religion, especially in religious seasons.

10. What have you learnt from the study? Have you achieved new knowledge about phishing?

The majority had found the experiment interesting and had enhanced their knowledge on phishing, especially on how to detect phishing attempts from legitimate ones. It also demonstrates some of the false beliefs such as overconfidence in reliability of anti-viruses to detect phishing, overtrust in official and trustworthy institutes in Qatar, and belief about limitation of use of topics, especially religious ones, for phishing.

11. Did you find it useful? And what did you like and dislike about it?

The experiment was very useful, especially the discussions which brainstormed the factors which make Qataris vulnerable to phishing.

12. Do you have any comments or suggestions on how to improve the study?

Some recommended holding the experiment with more participants towards getting more reliable results.

Interview with the expert in Qatar culture

Date of interview: 24 November 2009

Duration: Approximately 25 minutes

Interviewee: Mohamed Al-Kabi, Cultural attaché of Qatar Embassy in the UK

1. Why do you think Qatari people could be vulnerable to falling prey to e-mail phishing attacks? And do you think Qatari culture affects people's responses to phishing attacks? Explain your answer and state what are the possible cultural factors

I think Qatari culture has a major affects on people's responses to phishing attacks since Qatar is a conservative country with their customs and traditions and culture. He added Qataris are vulnerable to phishing due to cultural, country-specific factors, religion, personal interest and characteristics. Phishers try to utilise all of these factors and exploit them their advantage to persuade and trick their victims to fall prey to phishing.

The interviewee supported the above factors discovered from the discussions which make Qataris vulnerable to phishing. In addition, he pointed out more factors as follows:

1. Qataris are motivated by tribal or sectarian or partisan concerns since the society has a tribal structure
2. Feeling of safety, especially that Qatar is a safe country
3. Love of adventure
4. Love of spreading good, e.g. spreading good ideas which can be used by phishers which is called pyramid system.
5. Believe that he/she has not got enemies which want to hurt them
6. Lack of concerns on the consequence of phishing especially if you are not using your computer (e.g. work PC)

2. What do you think is the most successful trick that phishers could use on Qataris and Why?

Since Qataris are emotional and Islam plays a big role in their life and in being good willed, I think religious topics are more persuasive, especially if it influences their emotions, especially in religious seasons such as Ramadan and in existing disasters.

3. Do you believe Qatari people are well aware of the phishing threat? How to protect themselves? How to spot threats and how to react?

I can't judge that, but I think they are not enough aware because I have seen phishing becoming popular in Qatar and I think the responsible institutes are paying attention to protecting against it and enhancing public awareness on phishing. I believe even experts in computer are not all aware of phishing attacks, he mentioned that he have failed prey to e-mail phishing before were he have got the wrong advice from a computer expert. He has received an e-mail from unknown sender requesting his to verify his Msn e-mail account otherwise it will be blocked and a computer expert mentioned that this e-mail is legitimate. Where then phishers has stolen his e-mail account and impersonate the cultural attaché, he sent an e-mail to all contacts requesting help and money by using the name of the cultural attaché. He stated that he have been now more cautious on phishing because he have to learned from the lesson.

I predicted the young generation will be more aware. Furthermore, the country has got a lot of money and it is valuable to invest in awareness because it is the best way to defend against phishing.

4. Do you believe country-specific factors have helped development of phishing in Qatar? Like, first, the vast development experience in Qatar in all sectors especially the economy and ICT? Second, the absence of an e-law?

Yes, I do, the rapid development experienced in Qatar in recent years has assisted in shedding light on Qatar and therefore phishers found it an attractive place for phishing especially with the availability of a huge amount of money, large numbers of victims and absence of e-law to protect online consumers.

5. Do you think the establishment of an e-law will help in reducing e-crimes, in particular phishing?

Yes, of course. I think they are planning to develop this law soon

6. Do you think Qatari people need more time to cope with the rapid development in ICT and technology in Qatar in recent years?

Yes, Qatar, as other developing nations, is in the stage of development and since the development is rapid, people might not have absorbed this revolution and this will take time. However, the government is working on that by enhancing human resources and improving education curriculum.

C4 Consent Form for Experiment Participants

Participants contributing to penetration test 2 and the laboratory experiments study were asked to sign the following consent form:

CERTIFICATION BY PARTICIPANT IN THE EXPERIMENT

I certify that I am voluntarily giving my consent to participate in an experimental e-mail phishing study for the project entitled: **Reducing the Risk of E-mail Phishing through Awareness and Education: An Empirical Study of the State of Qatar Considering Cultural Differences**, being conducted at Loughborough University, UK by: Ms. Mariam Al-Hamar.

I certify that I have agreed to participate in the experiment of as previously explained by Ms. Mariam Al-Hamar and that I freely consent to participate in this experiment. I have had the opportunity to have any questions answered, I have had a full explanation of the procedures of the experiment and that information gathered will be used only for the benefit of the entitled research and will be confidential and kept strictly private.

Name:
Signed:
Witness other than the participant: Date:
.....

For any queries about the research topic please do not hesitate to contact the researcher (Ms. Mariam Al-Hamar, ph. +974 5553493, E-mail: m.k.j.al-hamar@lboro.ac.uk)

Appendix D: Evaluation of Recommendations

D1 Draft Letter to Interview Participants

Dear Sir/ Madam

E-mail phishing

E-mail phishing is a fraudulent process used by criminals. They aim to acquire sensitive information such as usernames, passwords and credit card details by pretending to be an honest and trustworthy person in an electronic communication such as an e-mail. This can have very serious financial and social consequences for their victims. As a PhD student at Loughborough University in the UK, I am doing research on 'e-mail phishing' as a contribution to foiling those criminal schemes in the State of Qatar. To achieve the desired goals, I have put together a set of recommendations for the Qatar government, organisation officials responsible for ensuring information security and for Qatari citizens, towards helping to reduce the phishing threat in Qatar. In order to evaluate the recommendations I now need to interview officials and citizens on their reactions to them. I hope you will be able to contribute and let us have your valuable feedback by taking part.

Thank you in anticipation of your involvement which will be much appreciated

Yours faithfully,

Mariam Al-Hamar

For any queries about the research topic, please do not hesitate to contact me through my e-mail: m.k.j.al-hamar@lboro.ac.uk.

CERTIFICATION BY PARTICIPANT

I hereby certify that I am voluntarily giving my consent to provide information for the above described research project **Reducing the Risk of E-mail Phishing through Awareness and Education: An Empirical Study of the State of Qatar Considering Cultural Differences** being conducted at Loughborough University, UK, by Ms. Mariam Al-Hamar.

I certify that I have agreed to be interviewed on the subject of e-mail phishing, as previously explained by Ms. Mariam Al-Hamar and that I freely consent to participate in this project. The interview procedures have been fully explained to me and I have been informed that information gathered will be used only for purposes of the research and will be confidential and kept strictly private. I have had the opportunity to have any questions answered.

Signed:

Witness other than the interviewee: Date:

.....

For any queries about the research topic, please do not hesitate to contact the researcher Ms. Mariam Al-Hamar, Phone: +974 5553493, E-mail: m.k.j.al-hamar@lboro.ac.uk.

D2 Interview questions

The recommendations were shown to the interviewees and then a discussion was held in which they were evaluated on their effectiveness, feasibility and difficulties to implement. The following questions were asked for each were

1. Do you find the recommendation is valuable and effective in reducing the risk of e-mail phishing in Qatar? Why?
2. Is it feasible? Why?
3. Are there any difficulties which might be experienced if it was implemented (e.g. in cost, resources)?
4. Overall, is the recommendation useful and do you think it will help in reducing the risk of e-mail phishing in Qatar? Why?
5. Do you have any further suggestions or comments?

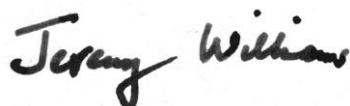
D3 Example of signed Consent Form

CERTIFICATION BY PARTICIPANT

I certify that I am voluntarily giving my consent to provide information for the above described project entitled: **Reducing the Risk of E-mail Phishing through Awareness and Education: An Empirical study of the State of Qatar Considering Cultural Differences**, being conducted at Loughborough University, UK, by Ms. Mariam Al-Hamar.

I certify that I have agreed to be interviewed in the subject of as previously explained by Ms. Mariam Al-Hamar and that that I freely consent to participate in this project. I have had the opportunity to have any questions answered, I have been fully explained the procedures of interview and that information gathered will be only used for the benefit of the entitled research and will be confidential and kept strictly private.

Signed:

A handwritten signature in black ink that reads "Jeremy Williams". The signature is written in a cursive style with a large initial 'J'.

Date: 29 Dec 09

For any queries about the research topic please don't hesitate to contact the researcher: Ms. Mariam Al-Hamar, ph. +974 5553493, E-mail: m.k.j.al-hamar@lboro.ac.uk).

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



CERTIFICATION BY PARTICIPANT

I, certify that I am voluntarily giving my consent to provide information for the above described project entitled: **Reducing the Risk of E-mail Phishing through Awareness and Education: An Empirical study of the State of Qatar Considering Cultural Differences**, being conducted at Loughborough University, UK by: Ms. Mariam AL-Hamar.

I certify that I have agreed to be interviewed in the subject of as previously explained by Ms. Mariam AL-Hamar and that that I freely consent to participate in this project. I have had the opportunity to have any questions answered, I have been fully explained the procedures of interview and that information gathered will be only used for the benefit of the entitled research and will be confidential and kept strictly private.

KHALID ALI AL OBAIDLI

Judge of Appeal Court
Doha - Qatar

Signed:

Date: 27.12.2009



D4 Details of expert interviews

Interview 1

Date of interview: 21 December 2009

Duration: Approximately 1 hour

Interviewees: Two officials from the Ministry of Interior, interviewed together:

Mahmoud Salah D. Ibrahim, Officer of the Computer Crimes Unit, Economic Crimes Prevention Division, General Admin. of Public Security, Criminal Investigation Dept., Ministry of Interior, Qatar.

Abdullah Al-Muftah, Manager of Public Relations Dept., Ministry of Interior.

1. Overall, are the recommendations useful and do you think they will help in reducing the risk of e-mail phishing in Qatar? Why?

Yes, I think they are useful if they are implemented successfully. Certainly, they will help in reducing the risk of e-mail phishing in the State of Qatar since they are well defined and established from a research base carried out in the region.

With regard to government recommendations:

The effectiveness of e-law would be defined only after the law comes into practice and this could be achieved with co-operation from all sectors including governmental and private organisations and Qatari citizens. It is unreasonable to build e-law from scratch, therefore it is worth while to learn from others' experience in e-law. It is important to announce the law and make it open source for the public.

I proved that the ipark is currently not monitored, therefore a lot of e-crimes inside Qatar come from there since there is no method of tracing the user. I think adding a kind of registration process to prove the identity of the user is a valuable solution, e.g. SMS registration is very valuable since a lot of Qatari citizens have mobile phones, even children, and all mobile phones in Qatar are registered, therefore it will be easy to trace the user in case of misuse of the Internet technology provided in the park.

With regard to organisation recommendations:

They were all valuable. I believe that within the organisation there should be an incident management centre which will report, react and work on the incidents and there is no shame to require help from responsible organisations in such a manner. If each organisation has an incident management centre, our duty will be

uncomplicated, since we can know with whom we should interact and we can further investigate the case with them.

It is important to define understandable and reasonable guidelines to avoid phishing. However, employers still define guidelines as unreasonable because they think this will enhance their security level and sometimes guidelines are forced to follow. For example, some organisations require a compulsory reset for the network password every three months where, although it is more secure, employees are still forced to do that and most of them find difficulties in remembering their password. This leads them sometimes to write it on a sticky note in front of their desks. This therefore makes them vulnerable to social engineering attacks.

With regard to adding a security level on the e-mail account which will not allow the e-mail user to send their confidential information (e.g. username and password) to anyone over the e-mail, they found this is a valuable, safeguard feature and it is technically feasible.

With regard to Qatari citizens' recommendations:

They are useful but too many points, I think they have to be reduced.

They are well defined since citizens usually perform such actions without considering that they are incorrect and they should avoid them to prevent phishing.

Some of the recommendations were not illustrated sufficiently, such as the reason why technological solutions are not 100% reliable to detect e-mail phishing attempts, how to protect yourself against phishing attacks, how to inspect security indicators and how official institutes could be phished. Not all people know what you mean, so it is better to make it clearer for normal people to help illustrate the points and maybe you could add some examples.

2. Are they feasible? Why?

With regard to government recommendations:

We found difficulties in defining the resources for the awareness programme and approving co-operation from many institutes in Qatar (e.g. educational institutes, media and governmental organisations) towards facilitating applying a successful awareness programme on phishing.

With regard to organisation recommendations:

Many organisations are reluctant to spend enough money to provide an incident management centre and a good quality education and awareness training. They are likely targets only to react once an incident happened by usually referring to us and to trustworthy experts and responsible organisations to perform the required actions, such as banks and Q-CERT.

Organisations did not pay attention to measurement tools to measure employees' vulnerability to possible threats such as phishing. They usually spent a lot of money on technological tools and react on incidents. However, planning and measuring the extent of the problem is essential by holding a phishing penetration test, a measurable awareness programme towards identifying the problem, assessing the current strategy of defence and working to improve it. Nevertheless, a lot of organisations do not prefer holding penetration tests within their organisation because of legal and ethical issues.

I think providing such a test is possible if it was held by trustworthy organisation such as Q-CERT, noting that it depends on the organisation size. For example, it might be essential to perform such a test regularly for top ministries which hold sensitive information whereas other organisations do not necessarily require it. Providing a certificate for audit is very useful, but it has to be certified and approved nationally and internationally, if possible, such as ISO9001 towards motivating organisations to do such an audit.

With regard to Qatari citizens' recommendations:

Usually people are reluctant to follow negative recommendations; therefore they recommend diverting the recommendations into "do" and "should" instead.

3. Are there any difficulties which might be experienced if they were implemented (e.g. in cost, resources)?

I have already covered some of the difficulties which might be experienced with your recommendations.

4. Do you have any further suggestions or comments?

No, I think it is a precious work and the government certainly has to benefit from your valuable findings.

Interview 2

Date of interview: 23 December 2009

Duration: About 40 minutes

Interviewee: Ahmed Rashid Al-Suwaidi, Manager of ISPs, Qtel, Qatar.

1. Overall, are the recommendations useful and do you think they will help in reducing the risk of e-mail phishing in Qatar? Why?

Yes, I think they are useful.

With regard to government recommendations:

All are useful, especially establishing a research centre on phishing and creating a database of the incidents.

About monitoring issues associated with ipark, Q-tel pointed out that this SMS service becomes common in Qatar. It already exists in the Ministry of Interior, many banks and institutes. Therefore, people could accept it. Technically, it is not hard to be implemented and it is reliable and the user can receive SMS of login details within a few seconds, since there are no difficulties with mobile signals in all of the iparks. However, the request for such service should come from Q-CERT. Also, there should be a co-operation with telecommunication service providers including Vodafone, since there is a proportion of mobile users who have Vodafone service.

With regard to organisation recommendations:

I agree on all of your suggestions. Organisations should work hard to protect themselves from phishing threat, they should set up a clear strategy of defence, including technological tools, policies and awareness, and the strategy must be evaluated regularly to prove its effectiveness in defending the organisation against phishing.

With regard to Qatari citizens' recommendations:

I think they are good ones, people need to know what they have to do and not do to avoid phishing.

2. Are they feasible? Why?

All recommendations defined for organisations are valuable. However, it requires sufficient budget and sometimes co-operation and approval from other organisations and from the government. With regard to the phishing audits, I think it is unfeasible because of ethical issues associated and employees might complain and feel they are being watched and this therefore might affect their work performance and trust in the organisation.

3. Are there any difficulties which might be experienced if they were implemented (e.g. in cost and resources)?

I think there are no difficulties which might be found if the above mentioned issues were studied and prepared. For example, employers should explain to their employees the reason for any auditing, defining reasonable guidelines and effective awareness. There might be people who might not accept to be involved in an

awareness programme on phishing because it might not be of interest to them, therefore comes the need to get them interested and encourage them.

4. Do you have any further suggestions or comments?

Phishing is a huge field of research although it is hard to understand why people and especially Qataris are vulnerable to phishing, but it is excellent to find a research done on that and a set of recommendations defined which are easy to follow and which will definitely help in reducing phishing threat in Qatar. I think it would be beneficial to do a similar study in other countries to see whether there is similarity with the findings discovered in Qatar or not.

Interview 3

Date of interview: 22 Dec 2009

Duration: Reply through e-mail on 24 Dec 2009

Interviewees: Three experts from Q-CERT, together:

Mounir Kamal, Senior Incident Specialist, Incident Management, Q-CERT, Qatar.

Omar Sherin, Analyst, Critical Infrastructure Protection, Q-CERT, Qatar.

Nora Al-Abdulla, Public Awareness Manager, Q-CERT, Qatar.

The following is a print screen of communication with the Q-CERT:

Re: Mariam AL-Hamar recommendations

From:  nabdulla@qcert.org

Sent: Thursday, December 24, 2009 3:29:18 PM

To: mariam alhamar (arab_eyes@hotmail.com)

Cc: mkamal@qcert.org; AAIAshmawy@qcert.org; Khalid N.Sadiq Al-Hashmi (kalhashmi@ict.gov.qa)

 2 attachments | [Download all attachments](#) (112.5 KB)[QCERT Rec...doc](#) (58.5 KB), [QCERT Rec...doc](#) (54.0 KB)

Dear Mariam,

Thank you for acknowledging the role of Q-CERT throughout your paper and referring to us for editing it. We are very delighted to help ambitious Qataris that are interested in information security, for together we help build a stronger cyber shield for our nation.

I have attached a new version from your document that contains our comments and recommendations. A general remark, as you will see in the document, is that you might need to rephrase some of the advice for Qatari citizens. Whenever you're mentioning something that you think others shouldn't do, it's very essential to tell them what they should do. In other words, it's important to give the solution when raising the problem specially when your talking about awareness.

If you need further help, please do not hesitate to approach us.

We wish you the best of luck.

(See attached file: QCERT Recommendation Evaluation-Comments from Q-CERT.doc)

Sincerely,

Nora al-Abdulla

1. Overall, are the recommendations useful and do you think they will help in reducing the risk of e-mail phishing in Qatar? Why?

Yes, definitely the recommendations were helpful.

With regard to government recommendations:

About ipark, yes, it's currently not monitored and users could not be traced, therefore it can be misused in hacking, scanning...etc. As a result, I agreed that there is a need for registration process to prove the identity of the user and I think using SMS technology is a good idea. We found this recommendation feasible, but require a lot of resources, co-operation with Internet service providers. Also there is a need to provide a unique username and password for each registered user which will expire immediately when the user is disconnected from the Internet. Although this might be annoying for people to have a different log each time, it is safer since it ensures each time the identity of the user. Although there is a risk that mobile phones could be stolen and used by phishers for this purpose, there is no 100% solution, and the user has to report immediately once this happens towards blocking the SIM card.

With regard to the researcher's recommendations for the creation of a statistical database for e-crimes and in particular phishing attacks, there are databases that

already exist in Q-CERT's incident database and law enforcement database. However, the records are still not gathered into a single database. Once all incidents are gathered into a single database and then classified, it would be useful for further research.

With regard to organisation recommendations:

Phishing audit is useful to measure employees' vulnerability to phishing and the awareness of employees. However, it is not part of our role to provide such audit for organisations; it could be done by any other information security institutes. Also it is valuable not to allow the e-mail users to send their confidential information to anyone over the e-mail.

With regard to Qatari citizens' recommendations:

The pieces of advice that contain the threat should also contain the cure. So when you tell people not to do something, tell them what they should do. Otherwise, you're only sending a scare that might drive people away from using technology. In other words, it's important to give the solution when raising the problem, especially when you're talking about awareness.

2. Are they feasible? Why?

Yes, Qatar e-law is on the way to reality and the team of Q-CERT is involved in co-operation with associated organisations including ITU (International Telecommunication Union), Ministry of Interior, Ministry of Public Prosecution, High Judicial Council and others. It is important to consider the dependability and adaptability of the law, especially with the fast improvement in technology. The new e-law has taken into consideration experience of other countries in e-law; basically it is a combination of e-law of Australia, America, UK, UAE and Saudi Arabia. However, it is customised to be unique for the State of Qatar. The law will be improved regularly as required.

3. Are there any difficulties which might be experienced if they were implemented (e.g. in cost, resources)?

Yes, there is a need for sufficient budget, resources and approval of recommendations to be implemented. Usually organisations do not spend a lot of resources on providing an incident management centre and awareness. They usually refer to us or Ministry of Interior or Q-tel to solve the incident. And there might face difficulties in people's acceptance of holding phishing audit, awareness, following policies, adding registration to ipark.

4. Do you have any further suggestions or comments?

You can also mention that it's a trusting environment and criminals may thus take advantage of this. You could mention the importance of security policies within organisations and how the enforcement of such policies helps in reducing risks, but

that's a general recommendation for all security issues. Try to research how you can utilise it to deter phishing. Also I suggest not clicking on links in e-mails even if they are from senders you know. Retype the link.

Interview 4

Date of interview: 24th Dec 2009

Duration: About 20 minutes

Interviewee: Abdullah Al-Malki, Head of Prosecution, Ministry of Public Prosecution, Qatar

1. Overall, are the recommendations useful and do you think they will help in reducing the risk of e-mail phishing in Qatar? Why?

By going over them I think they are useful and they will help the country to protect against phishing.

2. Are they feasible? Why?

A law will definitely provide a framework for us, but still the law is hard to implement, especially for crimes coming from abroad, from countries such as Nigeria, where it is hard to reach the phishers and punish them, even if there were a co-operation with them, since there is no stability in such countries. I suggest to make people aware to be cautious with e-mails from those countries. The only thing we can do is to wait until the country becomes stable and then we could build a cooperation.

With regard to the need for public prosecution, justices and lawyers to enhance their knowledge on how to deal with e-crimes, I think there should be an optional course for people who are interested to be experts in e-crimes. It would be enough to have a team of experts in e-crimes where all e-crimes cases will then be referred to them for investigation.

I believe there is a need for a research centre on e-crimes in Qatar, especially since Qatar is now investing in education and research and there is a huge revolution in technology, but this required huge resources from experts in the field, money and tools. However, with support from government and other institutes, especially educational, once the centre could be reputable.

I found that keeping a record of phishing incidents in a database, although it seems to be an easy step, most organizations do not do it. It is part of our culture, people do

not want to report, they just want to react and solve the problem, they think it is a waste of paper and time.

3. Are there any difficulties which might be experienced if they were implemented (e.g. in cost, resources)?

In everything, we might find difficulties, for example the difficulty might be faced with co-operation with unstable countries such as Nigeria on e-crimes and in particular phishing.

4. Do you have any further suggestions or comments?

No, I found recommendations were clear and well defined.

Interview 5

Date of interview: 27 December 2009

Duration: Reply by e-mail, 4th January 2010

Interviewee: Khalid Ali Abdullah Al-Obaidli, Judge at the Courts of Justice under the category of the Senior Civil Court Judges, The High Judicial Council, Department of Administrative & Financial Affairs, Qatar.

1. Overall, are the recommendations useful and do you think they will help in reducing the risk of e-mail phishing in Qatar? Why?

By looking at the proposed recommendations, I do find them valuable, especially that they covers different target groups and the recommendations were clear and concluded from a research base.

2. Are they feasible? Why?

Overall, I found them feasible especially that the country has sought for development in all sectors, especially in terms of technology, and there is a huge amount of money associated for that. I strongly agree on the need to have a specialised research centre and a clear database of e-crimes in Qatar towards investigating the extent of the problem.

With regard to e-law, it is on the way to reality in the near future and your recommendations with regard to the law to be general and modified regularly were considered. However, the law will help in reducing the phishing problem although there are some difficulties which have to be considered, such as the ability to build a co-operation with other countries, especially those from which crimes usually come,

e.g. Nigeria. However, I still think it is hard to build cooperation, especially with those countries, because of stability of governments in these areas of the world. Also, I agree with you that there should be a team of experts in e-crimes in the court, since it is important that they could have enough knowledge on how to deal with e-crimes.

3. Are there any difficulties which might be experienced if they were implemented (e.g. in cost, resources)?

Overall, there might be minor difficulties as I mentioned in terms of e-law and maybe the ability to motivate the government to accept the recommendations and get approval to implement them. This sometimes might take a long time to process the recommendations and find how effective they are in reality to reduce the risk of phishing.

4. Do you have any further suggestions or comments?

I suggest trying to transform these recommendations into reality by passing them to the government to look at them and benefit from this research.

Interview 6

Date of interview: 14th December 2009

Duration: 45 minutes

Interviewee: Dr. M. Kamala, Computer Systems Administration Course Leader, Bradford University, UK.

1. Overall, are the recommendations useful and do you think they will help in reducing the risk of e-mail phishing in Qatar? Why?

Yes, they are. My main concern is where those recommendations come from. They are proved to be based on deep research in the field from literature, surveys, interviews and experiments which builds up a contribution to your findings and recommendations.

2. Are they feasible? Why?

I think so. Qatar is a rich country and there is currently a huge development in all areas, especially in technology, that's why I think they would be practicable.

3. Are there any difficulties which might be experienced if they were implemented (e.g. in cost, resources)?

I think the only problem is getting people's agreement because some might complain or get annoyed when some recommendations are implemented, e.g. performing phishing audit and adding registration to ipark.

4. Do you have any further suggestions or comments?

Since recommendations defined for Qatari citizens are based on the factors which make Qataris vulnerable to phishing, it is better to pay attention to make sure the discovered factors are based on experiments as well as deep research in the area of Qatar culture and on previous literature available on what makes people vulnerable to phishing. I think that, as well, citizens' recommendations have to be shorter and understandable for the normal person.

Interview 7

Interviewee: Mr. Peter Wood, Chief of Operations, First Base Technologies, leader in providing information security and testing services, UK., interviewed by a structured questionnaire sent by e-mail due to inability to arrange a face-to-face interview. Since the interviewee has no knowledge on the phishing problem in the State of Qatar, he was asked to evaluate only the recommendations assigned for citizens and organisation officials responsible for ensuring information security (see Sections 8.2 and 8.3). The questions were generally associated with reducing the e-mail phishing problem. The following are print screens of communication with the company:

▶ Subject: Re: Interview	From: Peter Wood	09-12-2009 12:07
---------------------------------	-------------------------	------------------

Hello Mariam

Thank you very much for sharing your recommendations with me. It's obvious that you have put a great deal of effort and thought into your work.

Here is my feedback, which I hope you find useful.

1. Do you find the recommendation is valuable and effective in reducing the risk of e-mail phishing? Why?

Your recommendations for the organisation are thorough and sensible. I have no suggestions to improve these.

Your recommendations for users are also very thorough. However I feel that there may be too many points for the average person to consume. It may be worthwhile consolidating some points to make the list shorter. It would also be valuable to include some real examples (perhaps with screenshots?) to help illustrate the points you make.

2. Is it feasible? Why?

Yes, it is feasible, but only if there is sufficient budget for the organisation to fund your approach. We find many organisations are reluctant to spend enough money to provide good quality education and awareness, so any advice you can offer to your audience to help them gain funding would be welcome.

The above print screen contains the following responses:

1. Overall, are the recommendations useful and do you think they will help in reducing the risk of e-mail phishing in Qatar? Why?

Your recommendations for the organisation are thorough and sensible. I have no suggestions to improve these.

Your recommendations for users are also very thorough. However I feel that there may be too many points for the average person to consume. It may be worthwhile consolidating some points to make the list shorter. It would also be valuable to include some real examples (perhaps with screenshots?) to help illustrate the points you make.

2. Are they feasible? Why?

Yes, they are feasible, but only if there is sufficient budget for the organisation to fund your approach. We find many organisations are reluctant to spend enough money to provide good quality education and awareness, so any advice you can offer to your audience to help them gain funding would be welcome.

3. Are there any difficulties which might be experienced if they were implemented (e.g. in cost, resources)?

As my answer above, I think funding and resources will be the largest obstacle to implementing your suggestions.

4. Do you have any further suggestions or comments?

Include real world examples and screenshots to increase the impact and help understanding.

Interview 8

Date of interview: 19th August 2009

Duration: About 1 hours

Interviewee: M. Al-Kabi, Cultural Attaché of Qatar in the UK

1. Overall, are the recommendations useful and do you think they will help in reducing the risk of e-mail phishing in Qatar? Why?

I found them very valuable and useful and they are clear, understandable and defined from deep research in the field.

2. Are they feasible? Why?

Yes, they are to some extent. It depends as well on the availability of resources and approval from the Qatar government and responsible organisations in Qatar.

3. Are there any difficulties which might be experienced if they were implemented (e.g. in cost, resources)?

In every proposed solution there are always some difficulties which might be faced. I mentioned earlier there might be some difficulties in terms of resources, approval and co-operation. In addition, there is a problem that Qataris do not prefer reporting and documenting things, they prefer reacting more. Also, the difficulties to get these recommendations into reality, to measure how they would help in solving e-mail phishing problem in Qatar.

4. Do you have any further suggestion or comments?

Not really, I find the research valuable and interesting and I think it would be useful to get it into action in reality.

Interview 9

Date of interview: 27th December 2009

Duration: Reply by e-mail 28th December 2009

Interviewee: J. Williams, Manager Director of HandShaikh Ltd., UK. The company provides cross-cultural seminars and consultancy for business with Arabs. He is as well a researcher on Gulf culture and author of the book *Don't they know it's Friday*.

1. Overall, are the recommendations useful and do you think they will help in reducing the risk of e-mail phishing in Qatar? Why?

They are too confined to Qatar. The problem is worldwide. Qatar could become a world leader in the fight against phishing, though.

2. Are they feasible? Why?

Education is the ONLY answer. Qataris (and everyone else) need to wake up to the problem.

3. Are there any difficulties which might be experienced if they were implemented (e.g. in cost, resources)?

Qatar could lead the world in this matter. How about al-Jazeera taking up the matter?

4. Do you have any further suggestions or comments?

There is no technology to protect you fully from phishing. Your suspicion is your only friend.

De-couple your argument/logic from Qatar and make your thesis more international. Or at least more GCC-centric. By looking at citizens' recommendations, I found they are useful but I still think it is beneficial for other nations, not only Qataris, since they are based on the factors which make Qataris vulnerable to phishing and those factors are similar to other people not just Qataris. There is no technology to protect you fully from phishing. Your suspicion is your only friend. Just be suspicious – all the time. Trust no machine. None should trust an e-mail from a stranger, and be suspicious of a friend who sends you a bad e-mail because his/her email address might be forged. Even the English e-mails use compassion, etc. in their messages.

D5 Interviews with Qatari citizens

A sample of 30 Qatari e-mail users above 12 were randomly selected to evaluate the following proposed recommendations towards assessing people's acceptability, and feedback on the following recommendations:

1. Proposals for Qatari citizens
2. The need for applying an awareness framework, by government and organisation officials responsible for ensuring information security to enhance public awareness on phishing threat towards reducing the phishing problem in Qatar.
3. Adding a kind of ID proof such as Visa card, ID number or a type of registration process before accessing the free Internet in iparks.
4. Simulating e-mail phishing penetration test to measure organisation's vulnerabilities to such threat and to take part in an awareness programme to enhance awareness of phishing.
5. Setting up some clear and reasonable guidelines to help in defending against phishing, bearing in mind that employees should be motivated without intimidating them to follow such guidelines.
6. Adding security level to e-mail account which will not allow the e-mail user to send their confidential information (e.g. username and password) to anyone over the e-mail.

D6 Summary of outcomes of interviews

1. The majority of Qatari citizens state the need for applying an effective awareness framework to enhance public awareness of the phishing threat, especially through the media, towards reducing the phishing problem in Qatar.
2. The majority found that adding registration is valuable and necessarily, but it might be not accessible for people who do not have mobile phones. A lot say that they will still use it even if registration is added because they get used to SMS services and they found it fast and effective, especially with their experience with SMS banking services were with few seconds of performing any transactions on their bank account they receive an SMS to verify the transactions.
3. Most disagree on holding penetration tests because it is annoying, create distrust on organisation, and they do not like to be watched and audited regularly since this might negatively influence on their work performance.
4. With regard to the need for defining understandable and reasonable guidelines to avoid phishing, citizens found it important, However they mentioned that employers still define unreasonable guidelines because they think this will enhance their security level and sometimes guidelines are forced to follow because they are not realistic. They added it is important to motivate employees to follow such guidelines although most employers do not pay attention for motivating employees' weather by financial or moral support.
5. About adding security level on e-mail account which will not allow the e-mail user to send their confidential information to anyone over the e-mail, some citizens disagree and state that they sometimes send their log in detail for their trusted families or friends once required.
6. The majority of citizens found the recommendations defined for them were useful towards reducing the risk of phishing but they feel that there may be too many points for them to remember and follow. So they suggest shortening them. Also they pointed to the need to clarify to them what they should do as well as what they should not. Some state that they usually perform such actions without considering that they are incorrect and they should avoid them. Some think recommendations need to be illustrated sufficiently such as how to detect, react and protect yourself against phishing attacks, how you should continuously improve your knowledge of phishing. Therefore, they suggest helping by illustrating the points with real phishing incidents, scenarios, screenshots and literature, but in the end, keeping them short and precise.

Appendix E: Phishing Awareness Programme

E1 Copyright

1. Freej characters

► **Subject: RE: Could I have the authority to use your char for my PHD only**

This message has attached files. [Show](#)

Dear Mariam,

Your projects seems to be interesting, wish you the best of luck .

As discussed, to guarantee the artwork won't be misused and to protect our IP, Please fill in the attached document, sign and send it back to me along with your passport copy.

Warm regards,


Khalid Abu Hmidan
Operations Manager
Dubai Media City, Loft Office 3
Entrance C, Office 213
P.O. Box 502274, Dubai, UAE
T +971 4 37 57 474
F +971 4 42 90 949
M +971 50 3966628
khalid@lammtarapictures.com

Undertaking

I am **Maryyam AL-Hamar**, a **Qatari** national and holder of passport no. **00692464**, of **71 RAIKES LANE, BRADFORD, BD46RD, UK** hereby agree, acknowledge and undertake to Lammtara Pictures FZ-LLC and Mr. Mohammad Saeed Mohd Ahmad Harib of P.O. Box 500766, Building 1, Suite 02, Dubai Media City, Dubai, United Arab Emirates (hereinafter the "Rights-holders") as follows:

1. The Rights-holders are the exclusive owners of the registered copyrights and trade marks Um Khammas™, Um Allawi™, Um Saloom™, Um Saeed™ and Freej™ skyline and the Freej™ trade marks, all intellectual property rights in and relating to the Freej show, its graphics, tunes, songs and music (the "**Intellectual Property Rights**") and all the goodwill associated with the same and the Rights-holders have the exclusive right to use and exploit the said Intellectual Property Rights;
2. I have been provided with materials/artwork/logos, other confidential information in relating to the FREEJ™ show and/or copies of the Intellectual Property Rights (the "**Material**") specifically for the purposes of using the same in my **educational program for enhancing awareness of phishing e.g. my designed flash game** to be used specifically for academic purposes only and to be submitted strictly to **Loughborough university** where I am studying **PHD "Doctor of philosophy" in information security field**.
3. I will add the following copyright/proprietary notice on the **Educational program where I will use the Freej characters and also in my PHD thesis**:

© 2006 Lammtara Pictures FZ-LLC. This material/artwork/logo is owned by Lammtara Pictures FZ-LLC. You may not, whether in whole or in part, use, copy, duplicate, reproduce, adapt or otherwise incorporate into other formats, media or derivative works of any kind any or all parts of this artwork without the prior written consent of Lammtara Pictures FZ-LLC.
4. I will not deal in the Material or parts thereof in any commercial manner whatsoever or use the Material for any purpose other than the **educational program for enhancing awareness of phishing** to be submitted to the **Loughborough university**;
5. I will not provide the Material or any copy or any parts thereof to any third parties apart from the **Loughborough university**;
6. I will return all unused Materials or copies thereof as well as all copies of the Material (whether in print, electronic or other form) to the Rights-holders within five (5) days of submitting the above mentioned **educational program for enhancing awareness of phishing**.

Signed: 
 Name: **Maryyam Khalid AL-Hamar**
 Place: **UK**
 Date: **18/March/09**

2. Finding Nemo



Disney Publishing Worldwide

December 17, 2009

VIA FAX & MAIL

Ms. Mariam AL-Hamar
PHD Student
Loughborough University
27 Apartment
27 The Empress
Sunbridge Road
BD1 2AY
United Kingdom

Dear Mariam:

Thank you for the copy of the image depicting Nemo and Bruce from DISNEY/PIXAR's animated feature FINDING NEMO that you want to reproduce on your educational poster for your PHD thesis.

Before we can proceed further with your request, we need to know how many copies of your poster will be printed and who will be the recipient(s) of these copies. Additionally, will your poster be sold or given away free-of-charge?

Upon receipt of the above-requested information, we will be happy to consider your request. My fax number is: (818) 560-5171.

We thank you for your interest in DISNEY, and I look forward to hearing from you soon.

Best regards,

A handwritten signature in blue ink, appearing to read 'Margaret Adamic', written in a cursive style.

Margaret Adamic
Paralegal Specialist, Publishing
Corporate Administration

E2 E-learning System requirements

To run the game efficiently, basic requirements are essential on both the administrator and user workstations. This is explained below: (Appendix F contains the e-learning files)

Administrator requirement:

- WAMP server: It contains Apache server, PHP and Mysql. PHP version: 5.2.9, Apache server 2.2.11, Mysql 5.1.32
- Flash Mx 2004 or Flash 8
- Action script 2 is the scripting language used in the development of Flash.
- Coldfusion (server and language)
- Microsoft Access

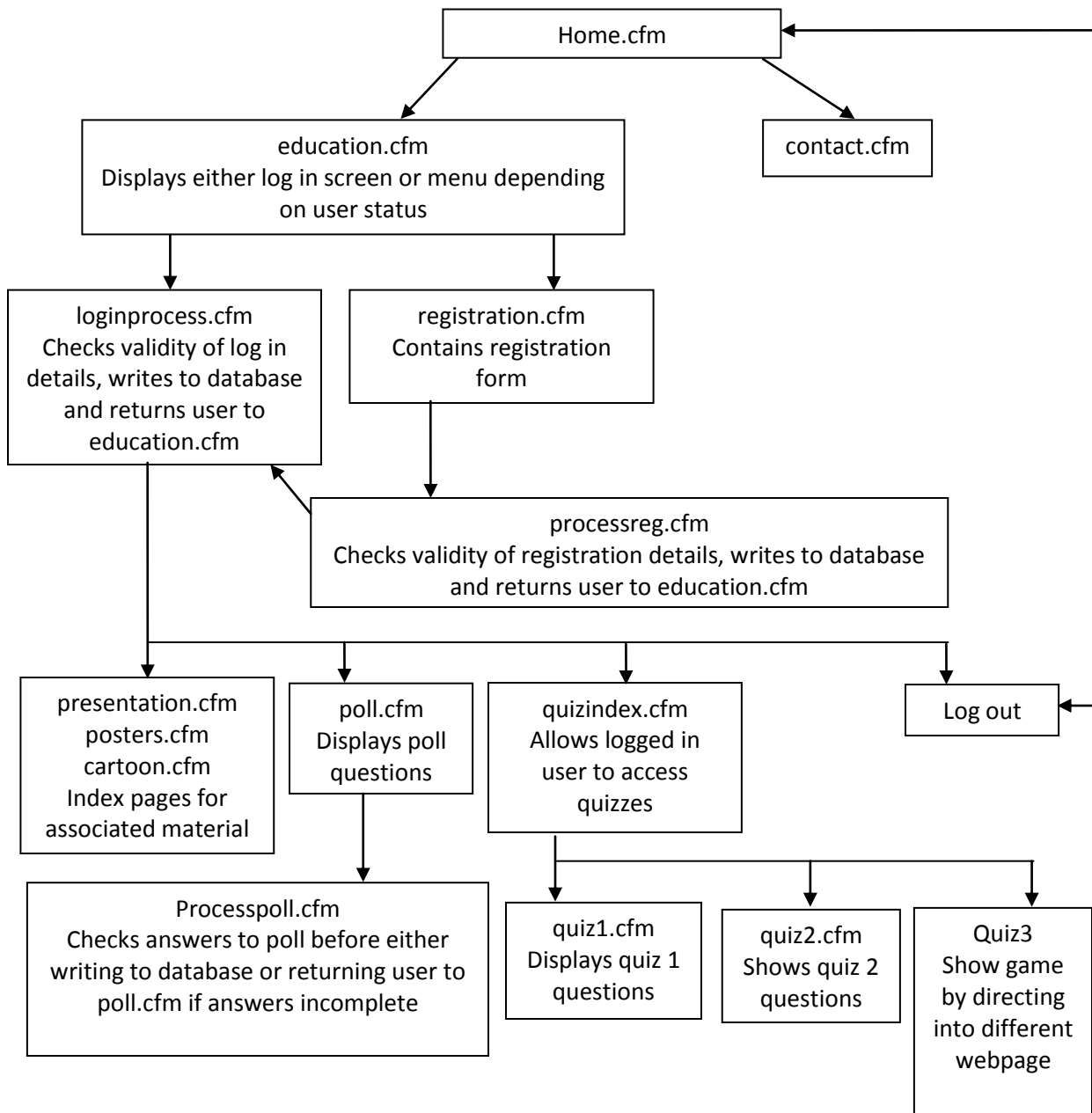
User requirement:

- Macromedia Flash player 6 or higher.
- Internet browser (e.g. Internet Explorer, Mozilla Firefox)
- Sound card and speakers
- Computer with 64M b of RAM or higher
- Minimum connection speed 56K modem, recommended T1 or higher.
- Screen resolution 800*600 or higher

E3 Description of Database Tables

Name of Table	Description	Comments
tblUsers	Stores details of all registered users	
tblAges	Stores details of age range categories (under 30, under 40,etc.)	Data from these tables referenced via primary key in tblUsers table
tblEducations	Stores details of education levels users can select	
tblOccupations	Stores details of range of occupations users can select	
tblComplevels	Stores details of different levels of computer ability user can select	
tblPolls	Stores all responses to Poll	Name of user referenced via primary key in tblUsers
tblQuizzes	Stores names of quizzes	
tblQuestions	Stores all questions to all quizzes	Quiz referenced by primary key in tblQuizzes
tblResponses	Stores answers to all quizzes	User referenced via primary key in tblUsers and question referenced via primary key in tblQuestions
tblAnswers	Stores all answers to quizzes and on screen responses to user	Corresponding question referenced via primary key in tblQuestions
tblScores	Stores user results	User referenced via primary key in tblUsers and quiz referenced via primary key in tblQuizzes

E4 Site structure



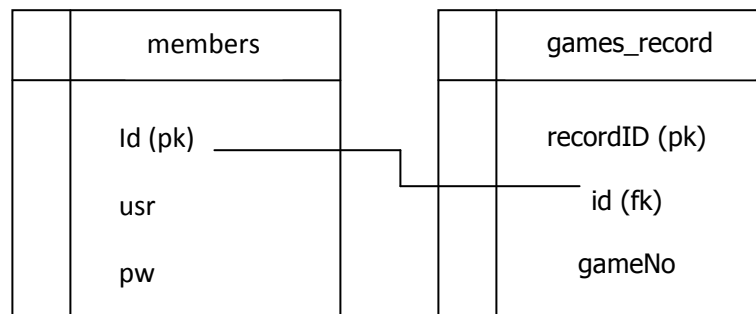
E5 Game development

Macromedia MX Flash 2004 is installed on the administrator PC. This becomes the Integrated Development Environment (IDE) for the game. WAMP Server is installed on the administrator PC. WAMP server consists of PHP, MySQL and Apache Server. This allows for the whole application to be developed on one machine without the need to upload files to a remote server for testing. Once the development is complete, an executable swf file (Shockwave file) is created from within the IDE. This is an executable file available to any PC that has a Flash player installed. This swf file is uploaded to the web server along with the php and mySQL files. A description of the PHP files is shown in the table below.

File	Summary
db_connect.php	This file tests database connectivity. It returns a list of all registered users
game1.php	This file accepts variables from one of the three Flash games. These are: game (1, 2 or 3), userID (unique number that identifies which user is playing and score (score for completed game). It then connects with database and writes these details to games_record table along with current date.
login.php	This file accepts two variables from Flash containing user name and password entered at log in stage. Then connects with database and checks for user name. If name exists, checks if password is correct. Depending on outcome, file returns to Flash two variables showing validity of both user name and password (either 'OK' or 'Bad'). Flash will only allow user to proceed if both variables have been set to OK. File also sends to Flash a variable containing unique ID of user used to monitor game play.
step1.php	This file forms part of registration process. Accepts variable from Flash that contains proposed user name. File then connects with database and checks if user name has been used previously. Returns variable to Flash showing validity of user name (either 'OK' or 'Bad'). If 'OK' received, Flash moves on to password stage of registration
step2.php	This file continues registration process. Accepts variable from Flash containing proposed password. Then connects with database and checks if password used previously. Returns variable to Flash showing validity of password (either 'OK' or 'Bad'). If 'OK' received , Flash moves on to email stage of registration

step3.php	This file continues registration process. Accepts variable from Flash containing proposed email. Then connects with database and checks if email used previously. Returns variable to Flash showing validity of email (either 'OK' or 'Bad'). If 'OK' received, Flash invites user to sign up
step4.php	When user registers validated user name, password and email are sent to this file. File then connects to database and writes details to members' table. Also dynamically adds unique ID for each user and then returns this ID to Flash so that it can be used to monitor game play.

The MySQL database file keeps records of user's data. Called phishing, consists of two tables, members and games_record. Database Entity Relationship Diagram (ERD) is shown in the following figure.



The members table consist of four fields, the 'id' set as (pk) stands for primary key, which means it gives each user a unique identifier, also the table keeps records of users' username, password and email in the 'usr', 'pw' and 'email' fields, respectively. The games_record table consists of five fields. The 'recordID' gives each record a unique identifier and the 'id', specified as (fk) foreign key, creates a relationship with the members' table. This means it is duplicated from the 'id' in the members' table to specify the user.

The other three fields are the ‘gameNo’ which is either game 1, 2 or 3, the ‘score’ and the ‘date’(see table below).

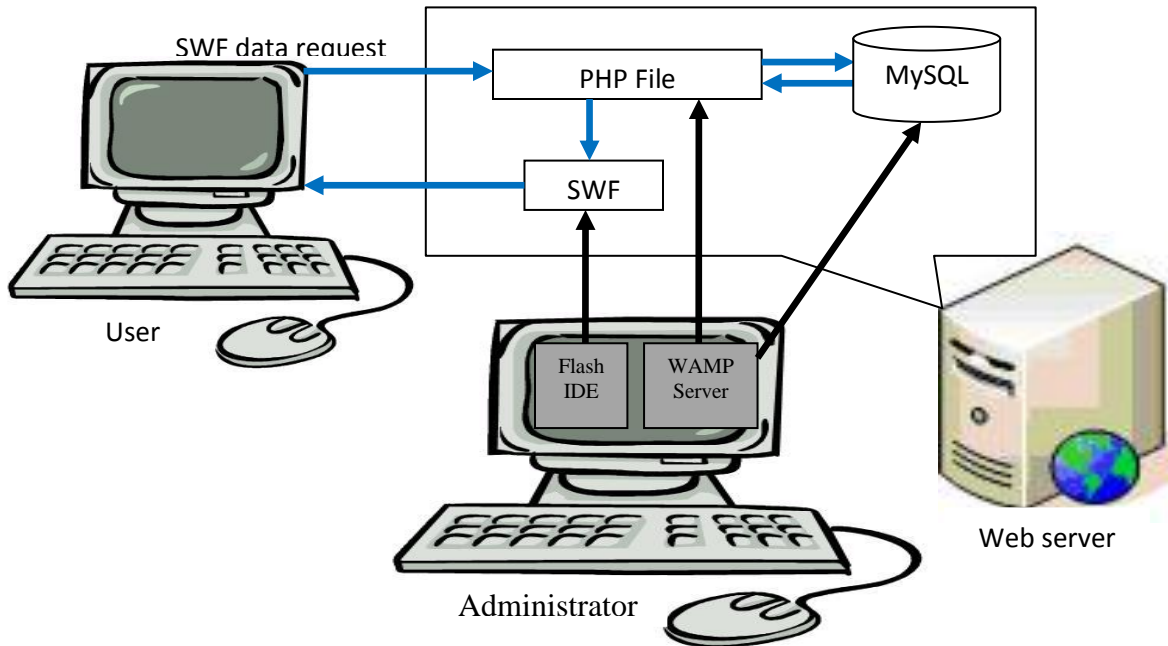
Data Dictionary for Phishing database

Table	Members	
Field	Data	Extra
Id	Integer(11)	Auto Increment
Usr	VarChar(50)	
Pw	VarChar(50)	
Email	VarChar(50)	

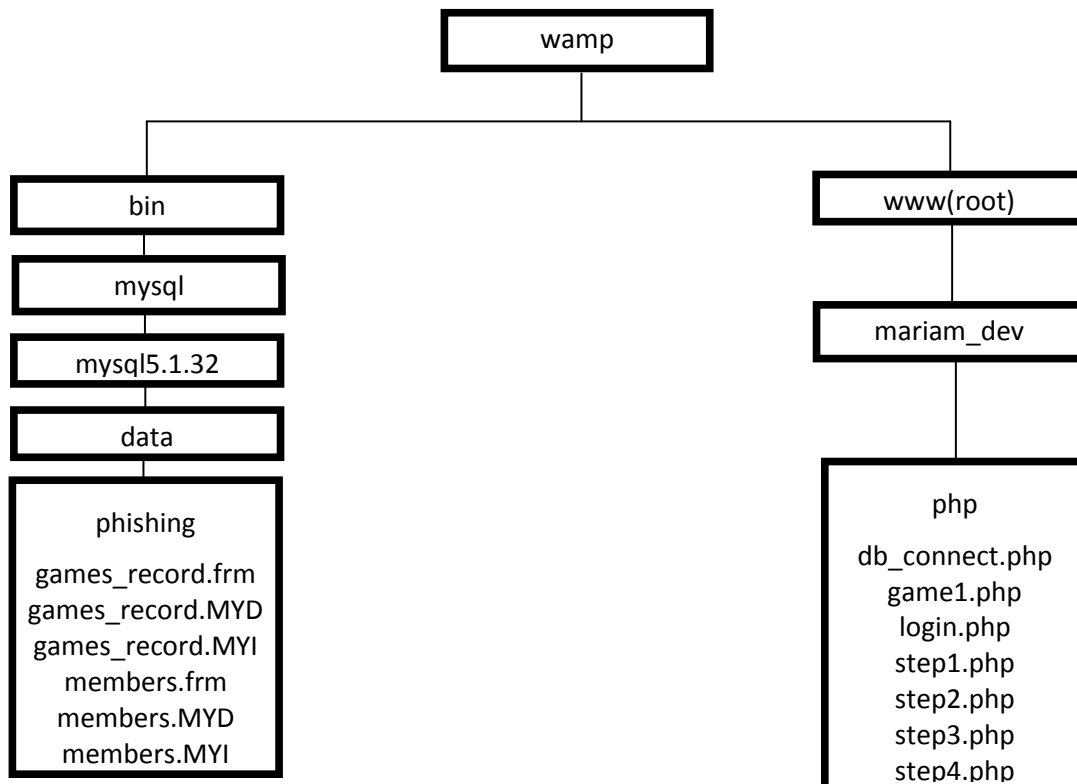
Table	games_record	
Field	Data	Extra
Recorded	Integer(11)	Auto Increment
Id	Integer(11)	
GameNo	Integer(11)	
Score	Integer(11)	
Date	Date	

Once the user is registered in the game, user information will be stored in the members’ table and an id will be uniquely assigned for each user. Each time the user plays a game, his/her game record will be stored in the games_record table and a recordID will be uniquely assigned for the game record. It is important that the file structure created on the administrator PC is exactly replicated on the web server. The user requests the swf file from the server (usually by entering the URL into a browser). The swf is then downloaded to the user’s PC.

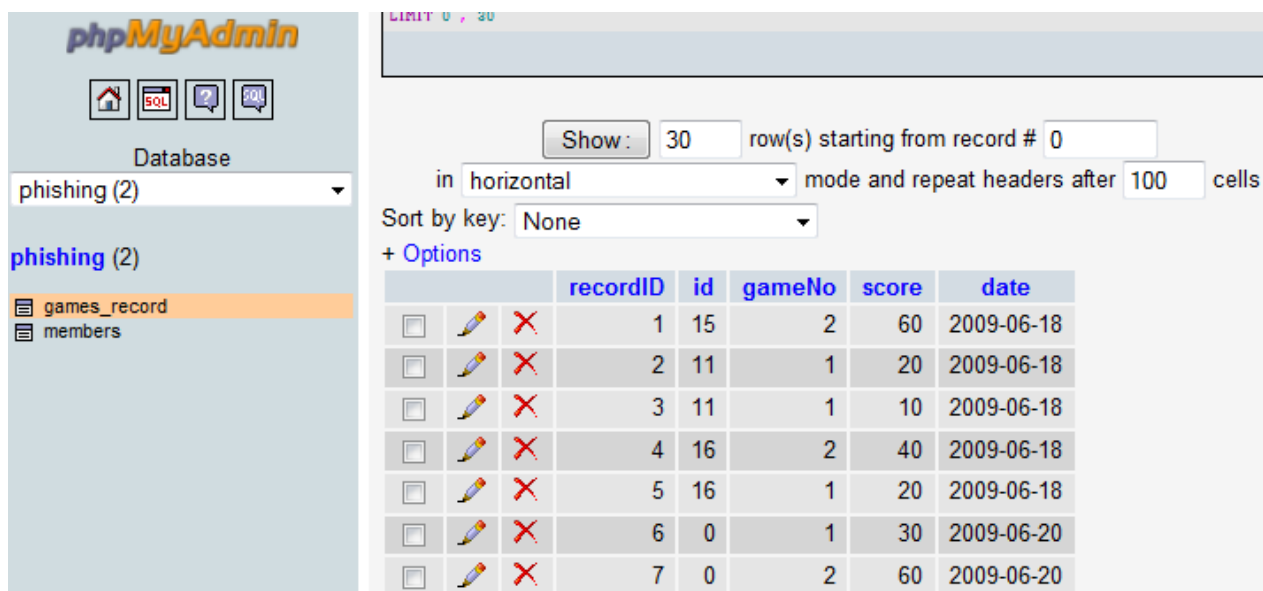
While playing the game and while logging in, data are exchanged between the the user's PC and the php files stored on the server (see figure below). The php files then either read or write to the mySQL database before returning data to the user's machine for the swf file to use.



System architecture of the game is illustrated in the figure below.



A screen of the players' record database is shown in the next figure.

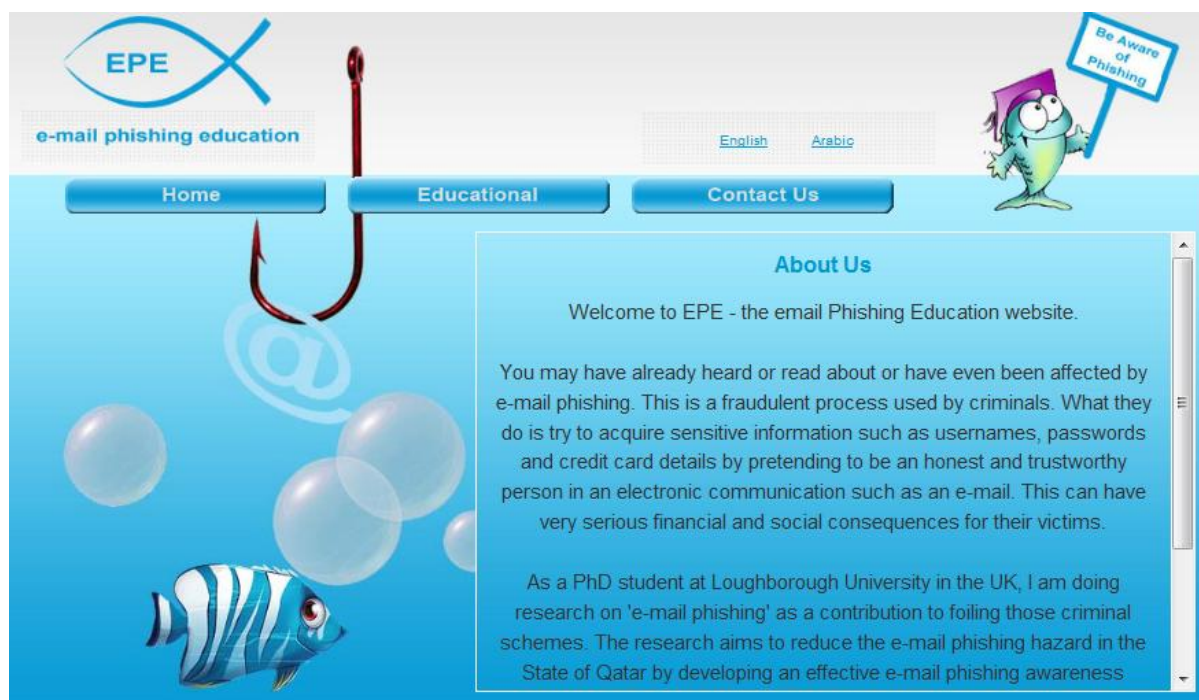


The screenshot shows the phpMyAdmin interface for a database named 'phishing'. The table 'games_record' is selected, and its contents are displayed in a table format. The table has the following columns: recordID, id, gameNo, score, and date. There are 7 records listed.

	recordID	id	gameNo	score	date
<input type="checkbox"/>	1	15	2	60	2009-06-18
<input type="checkbox"/>	2	11	1	20	2009-06-18
<input type="checkbox"/>	3	11	1	10	2009-06-18
<input type="checkbox"/>	4	16	2	40	2009-06-18
<input type="checkbox"/>	5	16	1	20	2009-06-18
<input type="checkbox"/>	6	0	1	30	2009-06-20
<input type="checkbox"/>	7	0	2	60	2009-06-20

E6 Print screen of e-learning site

Home page



The screenshot shows the home page of the EPE (e-mail phishing education) website. The page has a blue background with a large fishing hook and a striped fish. The header includes the EPE logo and navigation buttons for Home, Educational, and Contact Us. A cartoon fish character is holding a sign that says "Be Aware of Phishing".

About Us

Welcome to EPE - the email Phishing Education website.

You may have already heard or read about or have even been affected by e-mail phishing. This is a fraudulent process used by criminals. What they do is try to acquire sensitive information such as usernames, passwords and credit card details by pretending to be an honest and trustworthy person in an electronic communication such as an e-mail. This can have very serious financial and social consequences for their victims.

As a PhD student at Loughborough University in the UK, I am doing research on 'e-mail phishing' as a contribution to foiling those criminal schemes. The research aims to reduce the e-mail phishing hazard in the State of Qatar by developing an effective e-mail phishing awareness

Login page

EPE
e-mail phishing education

English Arabic

Home Educational Contact Us

Be Aware of Phishing

Welcome

To view these pages you must log in with your user name and password

User Name

Password

Log In

If you are new user please by following the link below

[Register](#)

Registration page

EPE
e-mail phishing education

English Arabic

Home Educational Contact Us

Be Aware of Phishing

Registration

1. Your Country: (Please select a country)

2. Gender:
 Male Female

3. Age:
 Under 18 18 to 29 30 to 49 Over 50

4. Education:
 School Further Education Higher Education Post Graduate Other

5. Occupation:
 Student Business Man Unemployed Employee

6. Do you have an e-Mail address?:
 Yes No

7. What is your level of computer knowledge?:
 None Poor Average Good Expert

8. Please choose a user name and password

User Name:

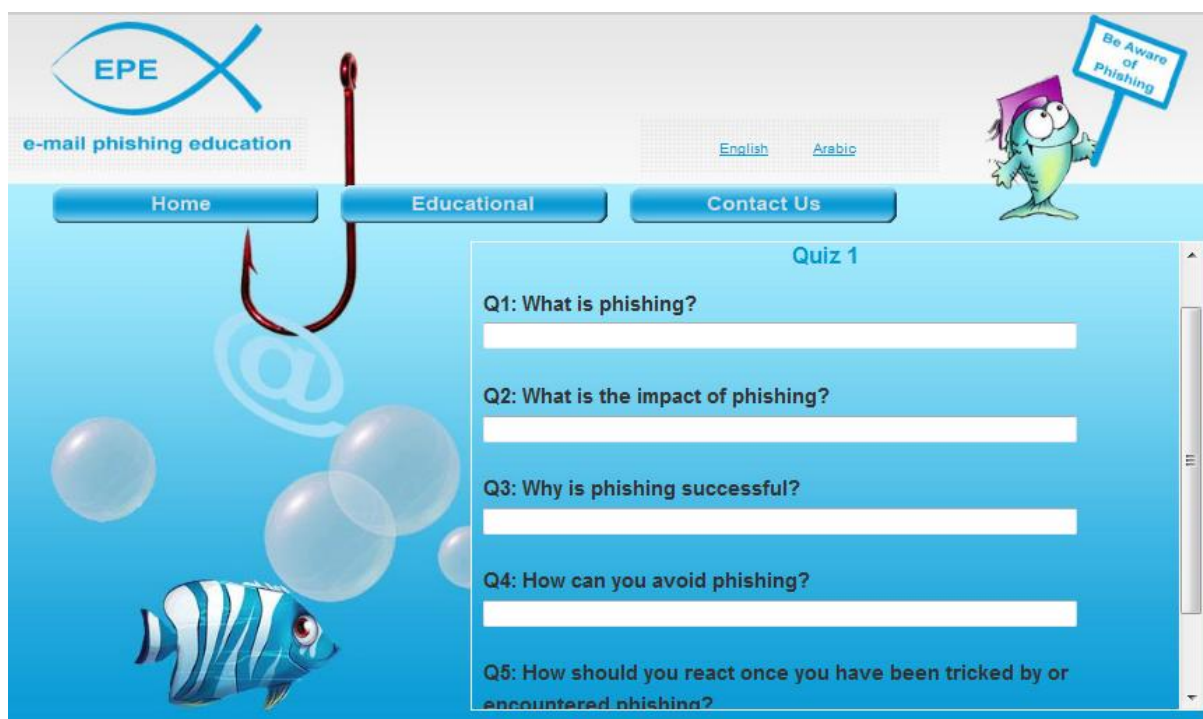
Password:

submit

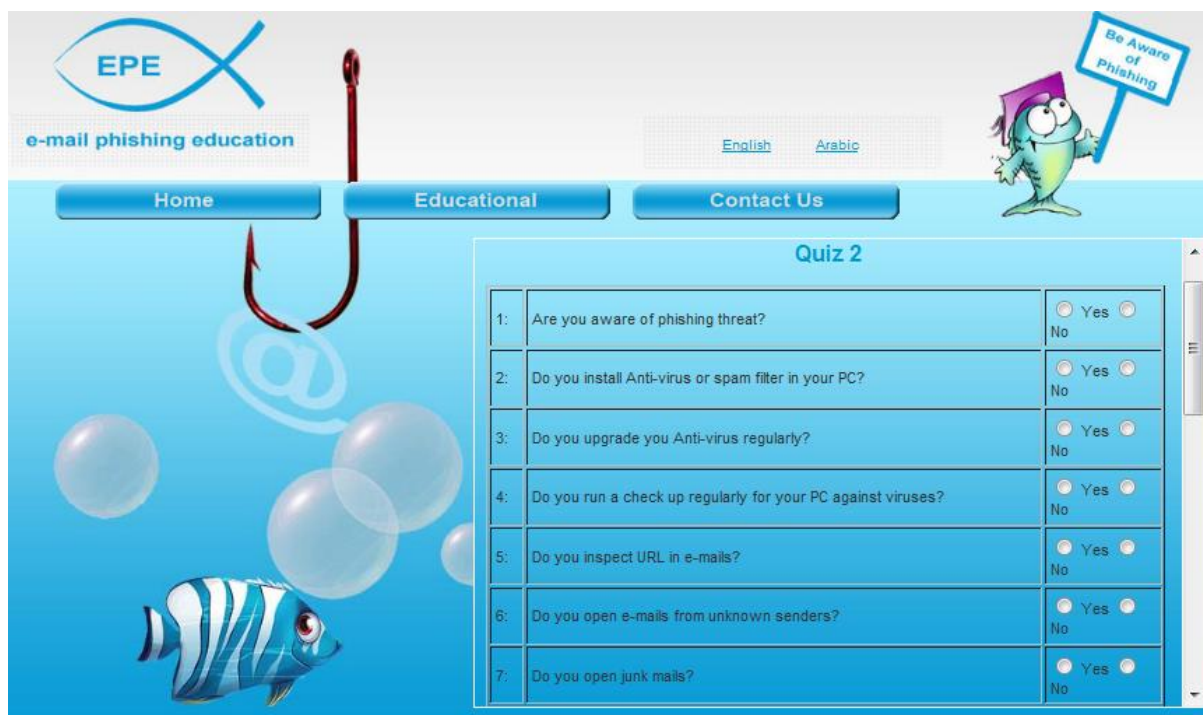
Educational material



Quiz 1



Quiz 2



EPE
e-mail phishing education

English Arabic

Home Educational Contact Us

Be Aware of Phishing

Quiz 2

1:	Are you aware of phishing threat?	<input type="radio"/> Yes <input type="radio"/> No
2:	Do you install Anti-virus or spam filter in your PC?	<input type="radio"/> Yes <input type="radio"/> No
3:	Do you upgrade you Anti-virus regularly?	<input type="radio"/> Yes <input type="radio"/> No
4:	Do you run a check up regularly for your PC against viruses?	<input type="radio"/> Yes <input type="radio"/> No
5:	Do you inspect URL in e-mails?	<input type="radio"/> Yes <input type="radio"/> No
6:	Do you open e-mails from unknown senders?	<input type="radio"/> Yes <input type="radio"/> No
7:	Do you open junk mails?	<input type="radio"/> Yes <input type="radio"/> No

Quiz 3 (Game)



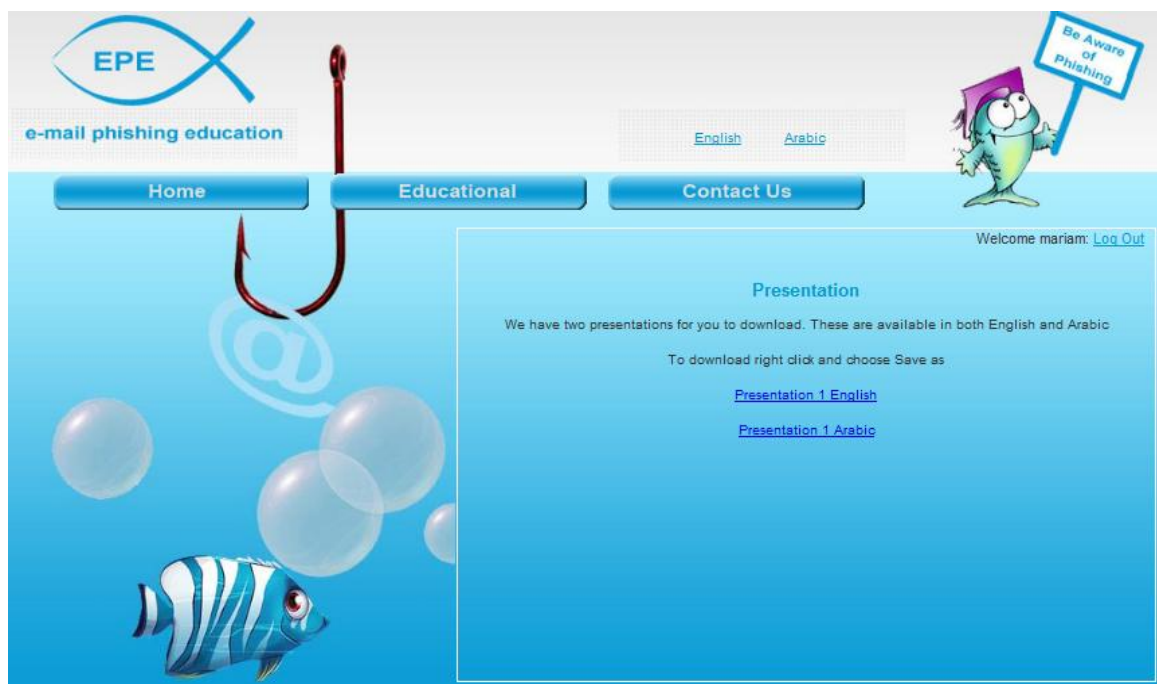
Welcome

Existing User

New User

II

Presentation



The screenshot shows the 'Presentation' page of the EPE website. The header includes the EPE logo (a fish-shaped icon with 'EPE' inside) and the text 'e-mail phishing education'. There are language selection links for 'English' and 'Arabic'. A navigation bar contains buttons for 'Home', 'Educational', and 'Contact Us'. A cartoon fish character wearing a purple graduation cap holds a sign that says 'Be Aware of Phishing'. A welcome message reads 'Welcome mariam: [Log Out](#)'. The main content area is titled 'Presentation' and contains the following text: 'We have two presentations for you to download. These are available in both English and Arabic. To download right click and choose Save as'. Below this text are two links: '[Presentation 1 English](#)' and '[Presentation 1 Arabic](#)'. The background features a blue gradient with bubbles and a striped fish.

Posters



The screenshot shows the 'Poster' page of the EPE website. The header and navigation elements are identical to the previous page. The main content area is titled 'Poster' and contains the following text: 'There are 3 posters to help you understand the dangers of phishing. Click on the images to view the full size poster or right click the links and choose Save as to download.' Below the text is a large image of a poster titled 'LET'S AVOID PHISHING'. The poster features a cartoon character in a yellow uniform pointing to a computer screen displaying a phishing email. The background of the poster is dark red with white text and images.





التصيد هو الهجوم الذي يسعى لخداعك من اجل الحصول على معلومات سرية أو خاصة أو أي معلومات قد لا تراها مهمة في مقابل سلع وخدمات وهمية

ناصر ينصح

ثبت برنامج مكافحة الفيروسات ومرشحات البريد وحدّته أولاً بأول
لا تثق بالعروض المبالغ فيها
لا تقم بفتح الرسائل التي تم تصنيفها على أنها غير مرغوب بها إلا إذا كانت موثوق بها
كن حذرا من الرسائل التي تطلب منك معلومات شخصية أو سرية
لا تخمّل مرفق من مرسل مجهول، لأنه قد يحتوي على فيروسات
يجب أن لا ترد على الرسائل المشبوهة
يجب أن تتأكد من صحة رابط الموقع الوجود في الرسالة
يجب أن تأخذ بعين الاعتبار التنبيهات الامنية لأنظمة التشغيل

التصيد بأنواعه في فريج



هنا أنا أم خماس
مبروك مسكن معلومات حسابك البنكي
ها معلومات حسابي ، أوكي الرقم 55...

هنا بعض النصائح لتجنب الخداع

- ثبت برنامج مكافحة الفيروسات ومرشحات البريد وحثته أوكاً بأول
- لا تنق بالعروض المبالغ فيها
- لا تقم بفتح الرسائل التي لم تصنفها على أنها غير مرغوب بها
- إلا إذا كانت موثوق بها
- كن حذراً من الرسائل التي تطلب منك معلومات شخصية أو سرية
- لا تقبل مرفق من مرسل مجهول. لأنه قد يحتوي على فيروسات
- يجب أن لا ترد على الرسائل المشبوهة
- يجب أن تتأكد من صحة رابط الموقع الموجود في الرسالة
- يجب أن تأخذ بعين الاعتبار التنبيهات الامنية لأنظمة التشغيل

Cartoons



EPE
e-mail phishing education

[English](#) [Arabic](#)

[Home](#) [Educational](#) [Contact Us](#)

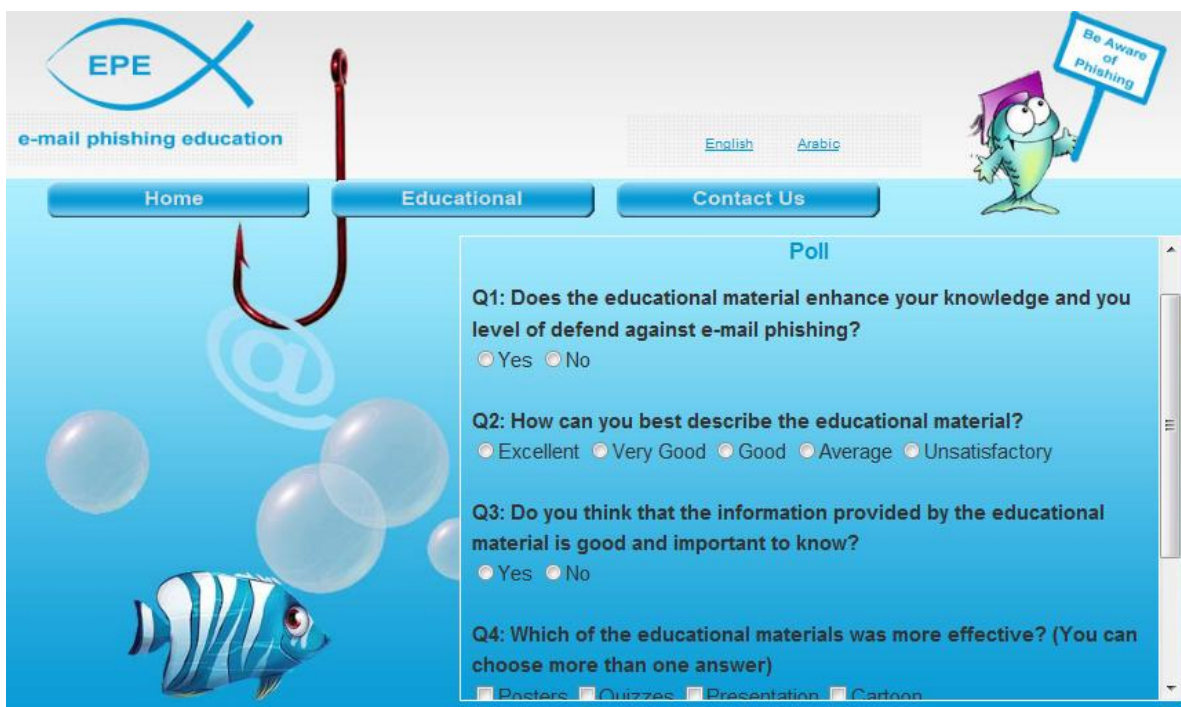
Cartoons

We have two cartoons to help you understand the dangers of phishing. Click on the images to view the full size cartoon (opens a new window) or right click the links and choose Save as to download.

In Phishing You are the fish, Don't bite!

Ho Ho Ho... I'm phishing for You for Promised goods, Services & more I can't list You.

Poll



EPE
e-mail phishing education

[English](#) [Arabic](#)

[Home](#) [Educational](#) [Contact Us](#)

Poll

Q1: Does the educational material enhance your knowledge and you level of defend against e-mail phishing?
 Yes No

Q2: How can you best describe the educational material?
 Excellent Very Good Good Average Unsatisfactory

Q3: Do you think that the information provided by the educational material is good and important to know?
 Yes No

Q4: Which of the educational materials was more effective? (You can choose more than one answer)
 Posters Quizzes Presentation Cartoon

Admin website



References

- Abad, C. (2005). "The economy of phishing: a survey of the operations of the phishing market". *First Monday*, Vol. 10, No. 9. Available at www.firstmonday.org [accessed 14/7/08]
- Abdullah Abdulghani & Brothers Company (AAB) (2003). "Company profile". Available at <http://www.aabqatar.com/profile.htm> [25/8/09]
- Aburrous, R, M., Hossain, A., Dahal, K., Thabatah, F., (2009). "Modelling intelligent phishing detection system for e-banking using fuzzy data mining". In *Proceedings, 2009 International Conference on CyberWorlds: Piscataway, NJ, USA*, pp. 265-72.
- Acohido, B (2009). "Unstoppable new phishing attacks blanket Facebook, Twitter, Hotmail". Available at <http://lastwatchdog.com/unstoppable-phishing-attacks-blanket-facebook-twitter/> [accessed 28/06/09]
- ActivCard (2004). "How to catch a phish". Available at www.activecard.com [accessed 01/03/09]
- Al Jaber, H. (2009). "Protecting Qatar's Children in Cyberspace". ICT Qatar, Available at <http://www.ictqatar.qa/output/page1257.asp> [accessed 10/11/09]
- Alavi, M. (1994). "Computer-Mediated Collaborative Learning: An Empirical Evaluation." *MIS Quarterly*, Vol. 2, No. 18, pp. 159-174.
- Alavi, M. and Carlson, P. (1992). "A review of MIS research and disciplinary development". *Journal of Management Information Systems*, Vol. 8, No. 4, pp. 45-62.
- Alnajim, A. and Munro, M. (2009). "An Anti-Phishing Approach that Uses Training Intervention for Phishing Websites Detection" In *Proceedings, 2009 Sixth International Conference on Information Technology: New Generations, Las Vegas, Nevada, April 27*, pp.405-410.

- AME Info (2004). "Literacy in the Arab world remains below the developed nations' minimum average of 95%". Available at <http://www.ameinfo.com/33975.html> [accessed 18/09/09]
- AME Info. (2008). "Vodafone and Qatar Foundation take first steps towards launch of Vodafone Qatar". Available at <http://www.ameinfo.com/154793.html> [accessed 07/12/09]
- American Red Cross (2005). "Hurricane Season 2005: Facts and Figures". Available at www.redcross.org [accessed 14/6/09]
- Amiri Diwan (2009). "Economy Development". Qatar. Available at [www:
http://www.diwan.gov.qa/english/qatar/Qatar_now.htm#Economy](http://www.diwan.gov.qa/english/qatar/Qatar_now.htm#Economy) [accessed 01/01/10]
- Anandpara, V., Dingman, A., Jakobsson, M., Liu, D. and Roinestad, H. (2007) "Phishing IQ tests measure fear, not ability". In *Proceedings: 11th International Conference on Financial cryptography and 1st International conference on Usable Security*, Scarborough, Trinidad and Tobago, pp. 362-366. Available <http://usablesecurity.org/papers/anandpara.pdf> [accessed 22/02/10]
- Anderson, A. D. S., Fleizach, C., Savage, S. and Voelker, G. M. (2007). "Spamscatter: Characterizing Internet Scam Hosting Infrastructure". In *Proceedings USENIX Security Symposium*, Boston, MA, pp. 135-148.
- Anderson, E. R. (2006). "Cryptography and Competition Policy - Issues with 'Trusted Computing'", in *Economics of Information Security*, series *Advances in Information Security*, Vol. 12, pp.3-10. New York, NY, USA
- Anderson, G. J., Aydin, C. E., and Jay, S. J. (1993). "Evaluating Health Care Information Systems: Methods and Applications". Thousand Oaks, CA: Sage.
- Anderson, J. R. (1993). "Rules of the Mind". Lawrence Erlbaum Associates.
- Anderson, J. R. and Simon, H. A. (1996). "Situated learning and education". *Educational Researcher*, Vol. 25, No. 4, pp. 5-11.

- Andrews, A.B., McLeese, D.G. and Curran, S. (1995). "The impact of a media campaign on public action to help maltreated children in addictive families". *Child Abuse and Neglect*, Vol.19, No. 8, pp. 921-932.
- Anti-Phishing Working Group (APWG) (2005). "Phishing Activity Trends Report, December 2005". Available at http://www.antiphishing.org/reports/apwg_report_DEC2005_FINAL.pdf [accessed 09/12/2009]
- Anti-Phishing Working Group (APWG) (2006). "Phishing Activity Trends Report". Available at www.antiphishing.org [accessed 18/11/2009]
- Anti-Phishing Working Group (APWG) (2007), "Phishing Activity Trends Report", July 2007. Available at www.antiphishing.org [accessed 28/01/10]
- Anton, A. I., Earp, E. A. J. B., Bolchini, D., He, Q., Jensen, C. and Stufflebeam, W. (2004). "The Lack of Clarity in Financial Privacy Policies and the Need for Standardization." *IEEE Security and Privacy*, Vol, 2, No. 2, pp. 36-45. Available at http://www.theprivacyplace.org/papers/glb_secPriv_tr.pdf [accessed 20/01/10]
- Apostolopoulos, G., Peris, V. and Saha, D. (1999). "Transport layer security: how much does it really cost?" In: *Proceedings, INFOCOM'99, 18th Annual Joint Conference of the IEEE Computer and Communications Societies 1999*, vol. 2, pp. 717-25.
- Arabic Network for Human Rights Information (2004). "The Internet in the Arab World A New Space of Repression?". Available at <http://www.hrinfo.net/en/reports/net2004/qatar.html> [accessed 25/05/2009]
- Arnott, D. and Pervan, G. (2005). "A critical analysis of decision support systems research", *Journal of Information Technology*, Vol.20, No.2, pp. 67-87
- Ashrafi, R., Yasin, M., Czuchry, A. and Al Hinai, Y. (2007). "E-commerce practices in the Arabian Gulf GCC business culture: utilisation and outcomes patterns". Vol. 2, Iss. 4, pp. 351-371. Available at <http://portal.acm.org/citation.cfm?id=1356448.1356449> [accessed 17/04/2009]

- Aston, M., McCombie, S., Reardon, B. and Watters, P.A. (2009). "A preliminary profiling of Internet money mules: An Australian perspective". In *Proceedings Cybercrime and Trustworthy Computing Workshop (CTC-2009)*.
- AVIRA (2010). "Phishing Statistics". Available at <http://www.avira.com/en/threats/section/worldphishing/top/90/index.html> [accessed 21/3/10]
- Awang, N.F.B. (2009). "Trusted computing - opportunities & risks". Piscataway, NJ, Washington, DC, USA, pp.5.
- B. ICANN Security and Stability Advisory Committee (SSAC) (2008). "SSAC Advisory on Fast Flux Hosting and DNS". Available at <http://www.icann.org/committees/security/sac025.pdf> [accessed 13/01/10]
- Babbie, E. R. (1973). "Survey Research Methods". Belmont, CA:Wadsworth Publishing.
- Barron, B, J, S., Schwartz, D, L., Vye, N, J., Moore, A., Petrosino, A.,Zech,L., and Bransford J, D (1998). "Doing with understanding: Lessons from research on problem and project-based learning." The Cognition and Technology Group at Vanderbilt
- Basnet, R., Mukkamala, S. and Sung, A.H.(2008). "Detection of phishing attacks: A machine learning approach". *Studies in Fuzziness and Soft Computing* 226, Vol. 226/2008, pp. 373-383.
- Bellovin, S.M. (2004). "Spamming, phishing, authentication, and privacy". *Communications of the ACM*, Vol. 47, No. 12, pp. 144-144. Available at www.proquest.umi.com [accessed 23/4/09].
- Benbasat, I.G., Goldstein, D.K. and Mead, M. (1987) "The case research strategy in studies of information systems", *MIS Quarterly*, Vol. 11, No. 3, pp. 369-386
- Bielski, L. (2004). "Phishing phace-off", *ABA Banking Journal*, Vol. 96, No. 9, p. 46. Available at www.proquest.umi.com [accessed 09/12/09].
- Bjørn-Andersen, N. (1985) "IS Research - A Doubtful Science". In Mumford E., Hirschheim, RA., Fitzgerald, G. and Wood-Harper, A.T. (eds.) *Proceedings IFIP 8.2*

- Colloquium, Research Methods in Information Systems, 1-3 September 1984, Manchester Business School, Elsevier: Amsterdam. pp. 273-277.
- Bluman, A.G. (2008). "A Brief Version Elementary Statistics, A Step by Step Approach" (4th edn.), McGraw-Hill Higher Education.
- Bock, D.E., Velleman, P.F. and De Veaux, R.D. (2007). "Stats Modeling the World" (2nd edn.), Pearson, Addison Wesley
- Bouma, G. D. (1996). "The Research Process", Melbourne, Oxford University Press.
- Brandt, A. (2005). "Phishing Anxiety May Make You Miss Messages", *PCWORLD*, October, p. 34.
- Breu, K. and Peppard, J. (2001) "The participatory paradigm for applied information systems research", In *Proceedings*, 9th European Conference on Information Systems, Bled, Slovenia, pp. 243-252
- Brown, J. S., Collins, A. and Duguid, P. (1989). "Situated cognition and the culture of learning". *Educational Researcher*, January-February, pp. 32-42. CHECK VOL.18, NO.1, pp. 32-42.
- Bryman, A. and Cramer, D. (1990). "Quantitative Data Analysis for Social Scientists", London, Routledge.
- Burrows, D. (1988). "Mass media campaigns: Worthwhile or wasted resources", *Connexions*, Vol. 8, No. 4, pp.14-16.
- Bush, S. (2003). "Arabic Culture in Qatar - Do's and Dont's for Expats. The world for expats in Qatar". Available at <http://www.thewordinqatar.com/information/arabic-culture-in-qatar-dos-and-donts-for-expats.html> [accessed 26/04/10]
- Butler, R. (2005), "An investigation of phishing to develop guidelines to protect the Internet consumer's identity against attacks by phishers", *The South African Journal of Information Management*, Vol. 7, No. 3. Available at www.sajim.co.za [accessed 11/02/09]

- Butler, R. (2007). "A framework of anti-phishing measures aimed at protecting the online consumer's identity." *Electronic Library UK 2007*, Vol.25, No.5, pp. 517-33. Available at <http://www.emeraldinsight.com/Insight/ViewContentServlet?contentType=Article&FileName=Published/EmeraldFullTextArticle/Articles/2630250502.html> [accessed 18/12/08].
- Caglayan, A., Toothaker, M., Drapeau, D., Burke, D., Eaton, G. (2009). "Real-Time Detection of Fast-Flux Service Networks". In *Proceedings Cybersecurity Applications and Technologies Conf. for Homeland Security*, IEEE CS Press, pp. 285-292.
- Campbell, D.T. and Stanley, J.C.(1971) "Experimental and Quasi-Experimental Designs for Research". Chicago: Rand McNally & Co.
- Campion, M.A., Campion, J.E. and Hudson, J.P., Jr. (1994). "Structured Interviewing: A Note on Incremental Validity and Alternative Question Types", *Journal of Applied Psychology*, Vol. 79, pp.998-1002,
- Carnegie Mellon University (2006). "Survey shows e-crime incidents are declining yet impact is increasing". Software Engineering Institute's CERT Coordination Centre. Available at www.cert.org/archive/pdf/ecrimesurvey06.pdf [accessed 15/08/08].
- Cavaye, A. (1996). Case study research: a multi-faceted approach for IS. "Information Systems Journal", Vol.6, No.4, pp.227-242
- CC-SG (2005). "The Concept and Foundation". Available at <http://www.gcc-sg.org/Foundations.html> [accessed 05/08/09].
- Central Intelligence Agency (CIA) (2008a). "Middle East: Qatar". Available at <https://cia.gov/library/publications/the-world-factbook/geos/qa.html> [accessed 27/09/08]
- Central Intelligence Agency (CIA) (2008b). "Europe: United Kingdom". Available at <https://www.cia.gov/library/publications/the-world-factbook/geos/uk.html> [accessed 27/09/08].

- Chaddock, D. (2007). "Qatar: The Business Traveller's Handbook". Qatar, Department of Information and Researches, Ministry of Foreign Affairs.
- Chaddock, D. (2008). "Qatar". Qatar, Department of Information and Researches, Ministry of Foreign Affairs.
- Chen, K., Chen, J., Huang, C., Chen, C. (2009). "Fighting phishing with discriminative key-point features". *IEEE Internet Computing USA*, Vol.13, Issue 3, pp. 56-63.
- Chen, W. and Zhang, C. (2009). "Image spam clustering: an unsupervised approach". In *Proceedings First ACM workshop on Multimedia in Forensics*. Beijing, China, pp. 25-30.
- Clark, R. C. and Richard, E. M. (2002). "E-Learning and the science of instruction: proven guidelines for consumers and designers of multimedia learning". San Francisco, USA, Pfeiffer.
- Clark, R. E. (1994). "Media will never influence learning". *Educational Technology Research and Development*, Vol. 53, No.2, pp. 21-30.
- Clark, R. E. and Solomon, G. (1986). "Media in teaching". In Wittrock, M. (Ed.), *Handbook of Research on Teaching* (3rd edition), New York, Macmillan, pp.464-478.
- Clarkson, D. (2005). "Humans still the weak security link". Available at www.itweb.co.za. [accessed 24/12/08]
- Computing & Information Services (CIS) (2009). "Phishing: How Not to Get Hooked". The Information Security Group (ISG), Brown University. Available at http://www.brown.edu/cis/information_security/phishing.php [accessed 08/03/09]
- Consumer Reports (2006). "Don't bite at phishers' e-mail bait". Available at www.consumerreports.org [accessed 17/04/09].
- Cooperation Council for the Arab States of the Gulf (GCC) Secretariat General (2000) "Foundation and objectives". Available at <http://www.gcc-sg.org/eng/index.php?action=Sec-Show&ID=3&W2SID=33174> [accessed 05/01/09]

- Cooperation Council for the Arab States of the Gulf (GCC), Secretariat General (2001). "The Economic Agreement between the GCC States Adopted by the GCC Supreme Council (22nd Session, 31 December 2001)". Available at <http://library.gcc-sg.org/English/Books/econagree2004.htm> [accessed 05/01/09]
- Cooperation Council for the Arab States of the Gulf (GCC), Secretariat General (2006). "A Brief Overview of the Achievements of the GCC On the occasion of the 25th Anniversary of the establishment of the Cooperation Council for the Arab States of the Gulf (GCC)". Available at http://www.gcc-sg.org/GCC_Achievements_in_Brief.mht#Economic_Affairs [accessed 05/01/09]
- Cornford, T. and Smithson, S. (1996). "Project research in information systems: A student's guide". Houndmills, Basingstoke, UK, Palgrave.
- Corrons, L. (2005). "Phishing scam twist: bogus sites built to snatch credit cards", *TechWeb*, 7 April. Available at www.proquest.umi.com [accessed 10/02/09].
- Cowie, A.P. (ed.) (2005). "*Oxford Advanced Learner's Dictionary*, Seventh edition". Oxford University Press, Available at <http://www.oup.com/elt/catalogue/teachersites/oald7/lookup?cc=global> [accessed 25/07/08]
- Creswell, J. W. (2003). "Research Design: Qualitative, Quantitative, and Mixed Methods Approaches". Thousand Oaks, Sage.
- Crossan, F. (2003). "Research Philosophy: Towards an Understanding". *Nurse Researcher*, Vol.11, No.1, pp. 46-55.
- Cyota's FraudAction Service (2005). "PSECU Battles Phishing, Pharming and Online Fraud". Available at http://www.rsasecurity.com/press_release.asp?doc_id=6809&id=1034 [accessed 15/06/09]
- Dalrymple, M. (2006). "IRS warns taxpayers on fake debt collectors", 7 April, Available at <http://washingtonpost.com> [accessed 18/05/09]

- Darke, P., Shanks, G. and Broadbent, M. (1998). "Successfully completing case study research: combining rigour, relevance and pragmatism". *Information Systems Journal*, Vol. 8, No.4, pp.273-289
- Dede, C. (1996). "Emerging technologies and distributed learning". *American Journal of Distance Education*, Vol.10, No. 2, pp. 4-36.
- Der Hovanesian, M. (2005). "Hackers and phishers and fraud, oh my!". *Business Week*, No. 3935, 30 May. Available at http://people.deas.harvard.edu/~rachna/papers/why_phishing_works.pdf [accessed 03/02/09]
- Dhamija, R, Tygar, J.D. and Hearst, M. (2006). "Why phishing works". In *Proceedings SIGCHI Conference on Human Factors in Computing Systems*, Montreal, Quebec, Canada, pp. 581-90.
- Dhamija, R. and Tygar, J.D. (2005). "The battle against phishing: Dynamic Security Skins". In *Proceedings 2005 Symposium on Usable Privacy and Security, Pittsburgh, PA*, 6 - 8 July. SOUPS '05, Vol. 93, pp. 77-88. New York, NY, ACM Press. Available at <http://doi.acm.org/10.1145/1073001.1073009> [accessed 05/12/08].
- Dierks,T. and Rescorla E. (2006). "The transport layer security (TLS) protocol version 1.1", Internet request for comment (RFC) number 4346; April 2006. Available at http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6V8G-4TPHRHV-2&_user=122861&_coverDate=03%2F31%2F2009&_rdoc=1&_fmt=full&_orig=search&_cdi=5870&_sort=d&_docanchor=&view=c&_acct=C000010080&_version=1&_urlVersion=0&_userid=122861&md5=a9898724b3e162643e039b477a7e0bfe#bib6 [accessed 09/12/08]
- Dodge, J. (2009). "Twitter, Facebook fertile phishing grounds". Available at <http://www.smartplanet.com/technology/blog/thinking-tech/twitter-facebook-fertile-phishing-grounds/2050/> [accessed 20/10/09]
- Dodge, R, C., Carver, C., and Ferguson, A (2007). "Phishing for user security awareness". *Computers & Security*, Vol. 26, No.1, pp. 73-80.

- Dodge, R.C. (2006). "Using phishing for user email security awareness". *Security and Privacy in Dynamic Environments*, Vol. 201/2006, pp. 454-459.
- Doha sooq. (2009). "About Doha sooq". Available at <http://doha.dbanksouq.com/DohaBank/English/General/AboutUs> [accessed 07/11/09]
- Donovan, M. S., Bransford, J. D. and Pellegrino, J.W. (1999). "How people learn: Bridging research and practice". Washington, D.C., National Academy Press.
- Downs, J., Holbrook, M. and Cranor, L. (2006). "Decision strategies and susceptibility to phishing". In *Proceedings Second Symposium on Usable Privacy and Security*, Pittsburgh, PA, 12 - 14 July. SOUPS '06, Vol. 149, New York, NY, ACM Press, pp. 79-90. Available at <http://doi.acm.org/10.1145/1143120.1143131> [accessed 03/01/10].
- Downs, J.S., Holbrook, M. and Cranor, L.F. (2007). "Behavioral Response to Phishing Risk". *Proceedings 2nd Annual eCrime Researchers' Summit*, October 4-5, pp. 37-44.
- Easterby-Smith, M., Thorpe, R. and Lowe, A. (1991). "Management research: an introduction". London, Sage.
- Eastlake, J., Reagle, J. and Solo, D. (2002). "XML-signature syntax and processing, RFC 3275". Available at <http://www.w3.org/TR/2002/REC-xmlsig-core-20020212/> [accessed 19/03/10].
- eBay (2009). "Spoof Email Tutorial". Available at <http://pages.ebay.com/education/spooftutorial/> [accessed 07/03/10]
- Edelson, D. C. and O'Neill, D. K. (1994). "The CoVis collaboratory notebook: Supporting collaborative scientific inquiry." In: *Proceedings National Educational Computing Conference, Recreating the Revolution* (pp. 146-152). Eugene, OR: International Society of Technology in Education.
- Edelson, D. C., Gordin, D. N. and Pea, R. D. (1999). "Addressing the challenges of inquiry-based learning through technology and curriculum design". *The Journal of the Learning Sciences*, Vol. 8, Nos.3&4, pp.391-450.
- Elsidafy,M. (2009) "E-commerce in UAE to hit \$36bn by 2010". Available at: <http://www.zawya.com/story.cfm/sidZAWYA20090705034011> [accessed 08/11/09]

- Embassy of Qatar, Washington, DC (2005). "Laws, Constitution of Qatar". Available at <http://www.qatarembassy.net/constitution.asp> [accessed 05/12/09]
- Emigh, A. (2005). "Online identity theft: phishing technology, chokepoints and countermeasures". 3rd October, Available at www.antiphishing.org/phishing-dhs-report.pdf [accessed 10/11/09]
- Evensen, D. H. and Hmelo, C. E. (Eds.). (2000). "Problem-based learning: A research perspective on learning interactions". Mahwah, NJ: Lawrence Erlbaum Associates.
- Evers, J. (2007). "Security Expert: User education is pointless". CNET News. Available at http://news.com.com/2100-7350_3-6125213.html [accessed 13/01/09].
- Explorer Publishing (2009a). "Qatar Complete Residents' Guide". Qatar, Qtel.
- Explorer Publishing (2009b). "Qatar Mini Essential Visitors Guide". Qatar, Qtel.
- Federal Trade Commission (FTC) (2005). "Take charge: fighting back against identity theft". Available at www.consumer.gov/idtheft [accessed 13/09/08]
- Federal Trade Commission (FTC) (2006a). "Identity Task Force Announces Interim Recommendations". 19 September. Available at www.ftc.gov [accessed 01/02/09]
- Federal Trade Commission (FTC) (2006b). "How Not to Get Hooked by a Phishing Scam".
- Feily, M., Shahrestani, A., Ramadass, S. (2009). "A survey of botnet and botnet detection". Piscataway, NJ, Athens, Glyfada, USA, pp. 268-73.
- Feldstein, M. (2002) "What Is "Usable" e-Learning?" *e-Learn Magazine*. Available at http://www.elearnmag.org/subpage/sub_page.cfm?section=4&list_item=6&page=1 [accessed 03/11/08]
- Felten E.W., Balfanz, D., Dean, D. and Wallach, D.S. (1997). "Web Spoofing: An Internet Con Game". In *Proceedings Twentieth National Information Systems Security Conference*, Baltimore. (Also Technical Report 540-96, Department of Computer Science, Princeton University, October 1997).

- Ferguson, A. J. (2005). "Fostering E-Mail Security Awareness: The West Point Carronade". *EDUCASE Quarterly*, Educause, USA, VOL. 28, NO.1, pp. 54-57. Available at <http://www.educause.edu/ir/library/pdf/eqm0517.pdf> [accessed 22/11/08]
- Fette, I., Sadeh, N.M. and Tomasic, A. (2007). "Learning to detect phishing emails". In *Proceedings 16th International Conference on World Wide Web (WWW'07)*. Banff, Alberta, Canada, pp. 649 - 656
- Fischer, C. and Layman, J.D. (1986). "Edge: Constructing a Questionnaire". Ohio State University, Ohio Cooperative Extension Service.
- Fletcher, J.D. (1990). "Effectiveness and Cost of Interactive Videodisc Instruction in Defense Training and Education", Washington DC: Institute for Defense Analyses
- Fletcher, J.D. (1991). "Multimedia Review". pp 33-42.
- Foddy, W. (1993). "Constructing Questions for Interviews". Cambridge University Press.
- Forte, D. (2009). "Phishing in depth". *Network Security UK*, Vol. 2009, No.5, pp. 19-20. Available at http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6VJG-4WGKC31-B&_user=8033985&_coverDate=05%2F31%2F2009&_rdoc=1&_fmt=full&_orig=search&_cdi=6094&_sort=d&_docanchor=&view=c&_acct=C000010119&_version=1&_urlVersion=0&_userid=8033985&md5=f7bdeee48dd75495570f6eaa028542fe&artImgPref=F [accessed 27/02/10]
- Fox, S. (2005). "Here comes phishing on steroids", *Plugged in*, Vol. 23, No. 6, p. 32. Available at www.pcworld.com, [accessed 15/03/10]
- Franco, R. (2005). "Better Website Identification and Extended Validation Certificates in IE7 and Other Browsers", *Microsoft Developer Network's IEBlog*. Available at <http://blogs.msdn.com/ie/archive/2005/11/21/495507.aspx> [accessed 21/11/09].
- Gabrilovich, E. and Gontmakher, A. (2002). "The homograph attack". *Communications of the ACM*, Vol. 45, No.2, p.128

- Gaffney, P. D.(2003). “Khutba, Encyclopedia of Islam and the Muslim World”. Macmillan Reference, USA.
- Gall, M. D., Borg, W. R. and Gall, J. P. (1996). “Educational research: An introduction”, Longman, New York.
- Galliers, R. D. (ed.) (1992). “Information Systems Research: Issues, Methods and Practical Guidelines”. Oxford, Blackwell Scientific Publications.
- Gan, G., Ling, N.T., Yih, C, G., Eze, C, U. (2008). “Phishing: A Growing Challenge for Internet Banking Providers in Malaysia”. *Innovation and Knowledge Management in Business Globalization: Theory & Practice*, Vols. 1 and 2, pp. 1276-1285
- Gartner (2002a). “There Are No Secrets: Social Engineering and Privacy (TU-14-5662)”, vol. 1, no. 1, Feb. Available at <http://www.gartner.com/gc/webletter/security/issue1/index.html> [accessed 13/10/08].
- Gartner (2005). “Gartner Survey shows frequent data security lapses and increased cyber attacks damage consumer trust in online commerce”. Available at www.gartner.com [accessed 21/01/09]
- Gartner (2006a). “Hype Cycle for Cyberthreats”, 13 September. Available at www.gartner.com [accessed 16/05/09]
- Gartner (2006b). “New Gartner Hype Cycle highlights five high impact IT security risks”. Available at www.gartner.com [accessed 06/12/09]
- Gasparini, L.A. and Gotlieb, C.E. (2006). “Method and apparatus for authentication of users and web sites”. Aug 29.
- Gee, J. P. (2003). “What Video Games Have to Teach Us About Learning and Literacy”. Palgrave Macmillan, Hampshire, England.
- Gillham, B. (2000). “Case study research methods”. London: Continuum
- Goddard, C. and Saunders, B.J. (2001). “Child abuse and the media”. Issues Paper 14, National Child Protection Clearinghouse, Australian Institute of Family Studies, Melbourne.

- Goldsborough, R. (2004). "Don't get phished out of cyberspace", *Black Issues in Higher Education*, Vol. 21, No. 21, p. 37. Available at www.proquest.umi.com [accessed 01/02/09]
- Gomez, L. M., Gordin, D. N. and Carlson, P. (1995). "A case study of open-ended scientific inquiry in a technology supported classroom". In J. Greer (Ed.), *Proceedings AI-Ed '95, Seventh World Conference on Artificial Intelligence in Education*, pp. 17-24. Charlottesville, VA: Association for the Advancement of Computing in Education.
- Gordin, D. N., Polman, J. L. and Pea, R. D. (1994). "The climate visualizer: Sense-making through scientific visualization". *Journal of Science Education and Technology*, Vol. 3, No. 4, pp. 203- 226.
- Gorling, S. (2006). "The myth of user education". In *Proceedings 16th Virus Bulletin International Conference*.
- Gulf Times (2009). "Economy set for over 7% growth, says QCB". Available at http://www.gulf-times.com/site/topics/article.asp?cu_no=2&item_no=290390&version=1&template_id=36&parent_id=16 [accessed 08/03/09]
- H.H. Shikha Mozah Bint Nasser Al Missned (2009). "Education and Opportunity" Qatar. Available at <http://www.mozahbintnasser.qa/output/page4.asp> [accessed 19/05/09]
- Hall, B. (1997). "Web-Based Training Cookbook, Everything you need to know for online training". Wiley Computer Publishing, New York, p. 10.
- Hara, M., Yamada, A. and Miyake, Y. (2009). "Visual similarity-based phishing detection without victim site information". Piscataway, NJ, Nashville, TN, USA.
- Harl (1997). "People Hacking: The Psychology of Social Engineering". Talk at Access All Areas III Conference, 7 May. Available at <http://cybercrimes.net/Property/Hacking/Social%20Engineering/PsychSocEng/PsySocEng.html>. [accessed 18/01/09]

- Harper, B. M., Hedberg, J. G., Wright, R. J. and Corderoy, R. M. (1995). "Multimedia reporting in science problem solving". *Australian Journal of Educational Technology*, Vol.11, No.2, pp.23-37. Available at <http://www.ascilite.org.au/ajet/ajet11/harper.html> [accessed 21/06/09]
- Hasle, H., Kristiansen, Y., Kintel, K. and Snekkenes, E. (2005) "Measuring Resistance to Social Engineering". In *Proceedings the First International Conference on Information Security Practice and Experience - ISPEC'05 (LNCS 3439)*, pp.132-143.
- Heinich, R., Molenda, M. and Russell, J.D. (1993). "Instructional media and the new technologies of instruction". New York NY, Macmillan Publishing.
- Herzberg, A. (2008). "Why Johnny can't surf (safely)? Attacks and defenses for web users". Department of Computer Science, Bar Ilan University, Ramat Gan, Israel. Available at http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6V8G-4TPHRHV-2&_user=122861&_coverDate=03%2F31%2F2009&_rdoc=1&_fmt=&_orig=search&_sort=d&view=c&_acct=C000010080&_version=1&_urlVersion=0&_userid=122861&md5=5313986123a396545d980ae21f914c9d [accessed 20/04/09].
- Herzberg, A. and Jbara, A. (2004). "Security and Identification Indicators for Browsers against Spoofing and Phishing Attacks", *ACM Transactions on Internet Technology (TIOT)*, Vol. 8, No. 16, Iss. 4, Sept. 2008. Earlier version: *Protecting (even) Naïve Web Users, or: Preventing Spoofing and Establishing Credentials of Web Sites* published as DIMACS Technical Report 2004–23, May 2004.
- Hickey, A.R. (2006). "SMS phishing is here", 6 September, Available at www.computerweekly.com [accessed 20/04/09]
- Hirschheim, R.A. (1985). "Information systems epistemology: An historical perspective", In *Research Methods in Information Systems*. E. Mumford, R. Hirschheim, R. Fitzberald et al., Eds. North-Holland, Amsterdam, 1985, pp. 13-38.
- Hollowitz, J. and Wilson, C.E. (1993). "Structured Interviewing in Volunteer Selection". *Journal of Applied Communication Research*, Vol.21, NO.1, pp.41-52

- Holz, T., Gorecki, C., Rieck, K., and Freiling, F (2008). "Measuring and Detecting Fast-Flux Service Networks" *Proceedings*. 15th Network and Distributed System Security Symposium (NDSS), The Internet Society. Available at www.isoc.org/isoc/conferences/ndss/08/papers/16_measuring_and_detecting.pdf. [accessed 18/02/10]
- Honeynet Project and Research Alliance (2005). "Know Your Enemy: Phishing Behind the Scenes of Phishing Attacks", 16 May, Available at www.honeynet.org/papers/phishing [accessed 04/01/10]
- Horgan, D. (2005). "The Phishing Phleet". Available at http://blogs.courant.com/travel_columnists_horgan/2005/11/the_phishing_ph.html [accessed 02/12/09]
- Horton, W. (2000). "Designing Web-Based Training", New York,. Wiley.
- Howcroft, D. and Trauth, D. (2005). "A Handbook of Critical Information Systems Research: Theory and Application", Cheltenham, UK, Edward Elgar.
- Hubbard, D. (2005), "Phishers moving away from e-mail lures", *Techweb*, 28 March. Available at www.proquest.umi.com [accessed 26/07/09]
- Hussey, J. and Hussey, R. (1997). "Business research". Basingstoke, Palgrave
- Ibp Usa (2005) "Qatar Customs, Trade Regulations and Procedures Handbook" (World Business, Investment and Government Library) Washington, DC. Publication Lightning Source Inc
- ICDL GCC Foundation (2009). "Our role" Qatar. Available at <http://www.icdlgcc.com/aboutus.htm> [accessed 23/01/09]
- ICT Qatar (2009a). "Supreme Council of Information and Communication Technology" Qatar. Available at <http://www.ict.gov.qa/output/Page9.asp> [accessed 23/01/09]
- ICT Qatar (2009b). "Vodafone wins Qatar's second mobile license". Qatar. Available at <http://www.ictqatar.gov.qa/output/NewsPage.aspx?PageID=561> [accessed 24/01/09]

ICT Qatar (2009c). “Free wireless Internet in Qatar's public parks” Qatar. Available at <http://www.ict.gov.qa/output/NewsPage.aspx?PageID=422> [accessed 24/01/09]

ICT Qatar (2009d). “Integrated e-government” Qatar. Available at <http://www.ict.gov.qa/output/Page28.asp> [accessed 01/02/09]

ICT Qatar (2009e). “QR 930m e-payments via e-Gov and Hukoomi” Qatar. Available at <http://www.ict.gov.qa/output/NewsPage.aspx?PageID=684> [accessed 25/01/09]

ICT Qatar (2009f), “Qatar Moves to Top 30 in the Rankings of the Global Information Technology Report 2008-2009” Qatar. Available at <http://www.ictqatar.qa/output/page1129.asp> [accessed 28/01/09]

INTELSAT (2010), “Qatar Telecom Secures Capacity on Intelsat 15 to Expand International Services”. Available at <http://www.intelsat.com/news-release/2010/20100303-1.asp> [accessed 28/09/10]

International Monetary Fund (IMF), (2007) “World Economic Outlook Database” Available at <http://www.imf.org/external/country/QAT/index.htm> [accessed 28/01/09]

Internet World Stats (2009a), “World Internet Users and Population Stats”. Available at <http://www.internetworldstats.com/stats.htm> [accessed 05/03/09]

Internet World Stats (2009b). “Internet Usage in the Middle East and in the World”. Available at <http://www.Internetworldstats.com/stats5.htm> [accessed 05/03/09]

Irani, Z., Grieve, R.J. and Race, P. (1999). “A case study approach to carrying out information systems research: A critique.” *International Journal of Computer Applications in Technology*, Vol. 12, No.2, pp. 190-198.

Jackson, C., Simon, D., Tan, D. and Barth, A.(2007). “An evaluation of extended validation and picture-in-picture phishing attacks.” In *Proceedings Workshop on Usable Security (USEC'07)*. Available at <http://usablesecurity.org/papers/jackson.pdf> [accessed 07/12/09]

Jackson, T.W., Dawson, R.J. and Wilson, D., (2000) “E-Communication Analysis: The Cost of an Internal Email Messaging System within Organisations”, Preparing to E-Business, Thoma, H., Mayr, H.C. and Erkollar, A. (eds), Osterreichische Computer

Gesellschaft 2000, 6th International Conference on Re-Technologies for Information Systems, Zurich, Switzerland, February 2000, pp 129-140, ISBN 3-85403-132-7.

Jagatic, T., Johnson N., Jakobsson M. and Menczer F. (2007). "Social Phishing", *Communications of ACM*, vol. 5, No.10, pp. 94-100. Available at <http://www.indiana.edu/~phishing/social-networkexperiment/phishing-preprint.pdf>

Jakobsson, M. (2005) "Modeling and Preventing Phishing Attacks". Phishing Panel in Financial Cryptography, School of Informatics, Indiana University at Bloomington, Feb. 2005.

Jakobsson, M. and Ratkiewicz, J. (2006). "Designing ethical phishing experiments: a study of (ROT13) rOnl query features". In *Proceedings 15th International Conference on World Wide Web*. Edinburgh, Scotland, DATES, pp. 513 -522.

Jensen, J.L. and Rodgers, R. (2001). "Cumulating the intellectual gold of case study research." *Public Administration Review*, Vol.61, No.2, pp.236-246.

Jiu-Xin, C., Bo, M., Jun-Zhou, L., Bo, L (2009). "A phishing Web pages detection algorithm based on nested structure of Earth Mover's Distance (Nested-EMD)." *Chinese Journal of Computers China*, Vol.32, No.5, pp. 922-9.

Johnson, B. R. and Koedinger, K. R. (2002). "Comparing instructional strategies for integrating conceptual and procedural knowledge." *Proceedings Annual Meeting [of the] North American Chapter of the International Group for the Psychology of Mathematics Education*, Vol. 1-4, pp. 969-978.

Kajava, J. and Siponen, M. (1997) "Social Engineering - IT Security Threat of Informatics". Available at <http://iris.informatik.gu.se/conference/iris20/9.htm> [accessed 05/10/09]

Kalathil, S. and Boas, T. C. (2003). "Arabic Network for Human Rights Information: The Internet in the Arab world: a new space of repression?" Available at www.hrinfo.net/en/reports/net2004/ [accessed 26/01/10]

- Kaplan, B. and Duchon, D. (1988). "Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study" *Management Information Systems Quarterly*, Vol.12, NO. 4, pp.571-586
- Kaplan, B. and Maxwell, J.A. (1994). "Qualitative research methods for evaluating computer information systems." In Anderson, J. G., Aydin, C., and Jay, S. J., editors, *Valuating Health Care Information Systems: Methods and Applications*, pp. 45-68. Sage, Thousand Oaks, CA.
- Kapp, K. M. (2001). "Integrated Learning for ERP Success: A Learning Requirements Planning Approach", Boca Raton, FL, St. Lucie Press.
- Kearsley, G. (Ed.) (2005). "Online learning: Personal reflections on the transformation of education". NJ: Educational Technology Publications.
- Keinan, G. (1987). "Decision making under stress: scanning of alternatives under controllable and uncontrollable threats". *Journal of Personality and Social Psychology*, Vol 52, No.3, pp., 639-644.
- Kerstein, P.L. (2005). "How Can We Stop Phishing and Pharming Scams?" Available at <http://www.csoonline.com/talkback/071905.html> [accessed 27/11/08]
- Khan, B. (Ed.) (1997). "Web-based instruction". NJ, Educational Technology Publications.
- Kirkley, J. R., Kirkley, S. E., Myers, T. E., Lindsay, N., and Singer, M, J (2003). "Problem-based embedded training: An instructional methodology for embedded training using mixed and virtual reality technologies" In *Proceedings Interservice/Industry Training, Simulation, and Education Conference (IITSEC)*, Available at <http://www.iforces.org/downloads/problem-based.pdf> [accessed 13/04/09].
- Kirkman, T.W. (1996) "Statistics to Use". Available at <http://www.physics.csbsju.edu/stats/chi-square.html> [accessed 22/01/09]
- Klein, G. (1999) "Sources of power: How people make decisions?" Cambridge, Mass., London, England

- Knickerbocker, P., Dongting Yu and Jun Li (2009). "Humboldt: a distributed phishing disruption system". Piscataway, NJ, Tacoma, WA, USA.
- Kondakci, S. (2009). "A concise cost analysis of Internet malware" *Computers & Security*, Vol. 28, No. 7, pp. 648-659. Available at <http://dx.doi.org/10.1016/j.cose.2009.03.007> [accessed 27/03/09]
- Konte, M., Feamster, N. and Jung, J. (2009). "Dynamic of online scam hosting infrastructure," In *Proceedings International Conference on Passive and Active Measurement (PAM)*, Seoul, Korea, April 2009, Springer-Verlag, pp. 219-228.
- Korea Internet Security Center (2006), "Korea Phishing Activity Trends Report". Available at http://www.antiphishing.org/reports/200601_KoreaPhishingReport_Jan2006.pdf [accessed 20/03/09]
- Krebs, B. (2005). "Paris Hilton Hack Started With Old-Fashioned Con" *Washington Post*, May 19. Available at http://www.washingtonpost.com/wp-dyn/content/article/2005/05/19/AR2005051900711_pf.html [accessed 14/07/09]
- Krugman, R.D. (1996). "The media and public awareness of child abuse and neglect: It's time for a change", *Child Abuse and Neglect*, Vol. 20, No. 4, pp. 259-260.
- Kuhn, T. (1960). "The Structure of Scientific Revolution", Chicago, University of Chicago Press
- Kulik, J. A. (1985). "The importance of outcome studies: A reply to Clark." *Educational Communications and Technology Journal*, Vol.34, No.1, pp.381-386.
- Kumar, A.(2005). "Phishing - A new age weapon". Technical report, Open Web Application Security Project (OWASP).
- Kumar, R. (1996). "Research Methodology: A Step-By-Step Guide for Beginners", South Melbourne, Longman.
- Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., and Nunge, E. (2007). "Protecting people from phishing: the design and evaluation of an embedded training email system" *Proceedings SIGCHI Conference on Human Factors in Computing*

- Systems,CHI '07. San Jose, California, USA, 28 April - 03 May, New York, NY, ACM Press, pp.905-914. Available at <http://doi.acm.org/10.1145/12406241240760> [accessed 03/08/09]
- Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F. and Hong, J. (2007). "Teaching Johnny not to fall for phish". Technical report, Carnegie Mellon University. Available at <http://www.cylab.cmu.edu/files/cmucylab07003.pdf> [accessed 05/10/08].
- Kvale, S. (1996). "Interviews: An Introduction to Qualitative Research Interviewing", Thousand Oaks, Calif, Sage.
- Lank, A.D. (2006). "Taxpayer beware: phishers target IRS; E-mails promise refund", 17 September. Available at www.findarticles.com/p/articles/mi_qn4196/is_20060717/ai_n16734222
- Larkin, E. (2009). "Organized Crime Moves Into Data Theft". *PC World*, Vol.27, pp.33-34.
- Leedy, P. and Ormrod, J.E. (2001). "Practical research: planning and design", 7th edition. New Jersey, Prentice-Hall
- Leedy, P. D. (1997). "Practical Research: Planning and Design", New Jersey, Prentice-Hall.
- Leone, M. (2006). "Italy sees rise in phishing scams" *Janes' Intelligence Review*, Vol.18, No.12, pp. 47-49
- Levy, B. (1999). "The Media, *Child Abuse and Neglect*", Vol.23, No. 10, pp.995-1001.
- Lindlof, T.R. and Taylor, B. C. (2002). "Qualitative Communication Research Methods". *Second Edition*. Thousand Oaks, CA: Sage.
- Liping, Ma, Yearwood, J. and Watters, P. (2009). "Establishing phishing provenance using orthographic features". Piscataway, NJ, Tacoma, WA, USA, pp. 1-10.
- Litan, A. (2004). "Phishing victims likely will suffer identity theft fraud". 14 March, ID No. M-22-8474. Available at www.gartner.com [accessed 15/11/09]

- Litan, A. (2006). "Credit report and internet data theft results in more fraud in 2005", 13 January, ID No. G00137219. Available at <http://www.gartner.com> [accessed 02/10/09]
- Lord, M. (2001). "They're Online and On the Job." *US World & News Report*. US News & World report, Vol.131, No.15, pp.72-75
- Lumsdaine, A. A. (1963). "Instruments and Media of Instruction". In N. Gage (Ed.), *Handbook of Research on Teaching*, pp. 583-682, Chicago, Rand McNally.
- Maldonado, H., Lee, J.-E. R., Brave, S., Nass, C., Nakajima, H., Yamada, R., Iwamura, K. and Morishima, Y. (2005). "We learn better together: enhancing elearning with emotional characters" *Proceedings on International Computer support for collaborative learning CSCL '05*, Mahwah, NJ: Lawrence Erlbaum Associates, International Society of the Learning Sciences, pp. 408-417.
- Maniar, N., Bennett, E., Hand, S. and Allan, G. (2008). "The effect of mobile phone screen size on video based learning." *Journal of Software*, Vol. 3, No. 4, pp. 51-61.
- Mark, M.M. and. Cook, T.D. (1984) "Design of randomized experiments and quasi-experiments." In L. Ruttman (ed.) *Evaluation Research Methods*. Beverly Hills, CA, Sage.
- Martin, L., Gutiérrez y Restrepo, E., Barrera, C., Rodríguez Ascaso, A., Santos, O.C. and Boticario, J.G. (2007). "Usability and Accessibility Evaluations along the eLearning Cycle." *Proceedings Web Information Systems Engineering 2007 Conference*, Nancy, France, pp. 453-458.
- Masatoshi Kawakami, Hiroshi Yasuda, Ryoichi Sasaki (2010). "Development of an E-learning Content-Making System for Information Security (ELSEC) and its Application to Anti-phishing Education." *Proceedings, 2010 International Conference on e-Education, e-Business, e-Management and e-Learning*, pp. pp.7-11.
- Masters, K. and Ng'ambi, D. (2007). "After the broadcast: disrupting health sciences' students' lives with SMS." *Proceedings IADIS International Conference Mobile Learning*. Lisbon, Portugal, 5-7 July 2007, Lisbon, Portugal, pp. 171-175.
- Mayer, R.E. (2001). *Multimedia Learning*. New York, Cambridge University Press.

- McConnetha, D. (2007) "Mobile Learning in the Classroom". West Chester University. Delivered at SALT Conference, Arlington, VA, August
- McGrath, D.K., Kalafut, A.M. and Gupta, I. (2009). "Phishing Infrastructure Fluxes All the Way". *IEEE Security and Privacy*, Vol. 7, No. 5, pp. 21-28
- McLellan, H. (Ed.) (1996). "Situated learning perspectives", Educational Technology Publications.
- McNamara, C. (1999). "General Guidelines for Conducting Interviews", Authenticity Consulting, LLC, Minnesota.
- Media Awareness Network (2005). "Detecting bias in the news". Available at <http://awareness.ca/english/index.cfm> [accessed 04/04/09]
- Merrienboer, J. V., de Croock, M. and Jelsma, O. (1997) "The transfer paradox: Effects of contextual interference on retention and transfer performance of a complex cognitive skill". *Perceptual and Motor Skills*, Vol. 84, pp.784-786.
- Merwe, A., Loock, M., and Dabrowski, M.(2005). "Characteristics and responsibilities involved in a Phishing attack." *Proceedings*. ACM WISCT 05, pp.249-254.
- Microsoft (2006) "Protecting a business from online threats", April. Available at www.microsoft.com [accessed 11/10/08]
- Mielke, K. W. (1968). "Questioning the questions of ETV research". *Educational Broadcasting Review*, 2, 6-15.
- Mifflin, H. (2000). "American Heritage® Dictionary of the English Language" (Vol. Fourth Edition).
- Miles, M.B. and Huberman, A.M. (1994). "Qualitative data analysis", 2nd edition. Newbury Park, CA, Sage.
- Miller, R. L. (1990) "Learning Benefits of Interactive Technologies", *Multimedia and Videodisc Monitor*, February, pp. 15-17
- MillerSmiles.co.uk (2006) "Phishing archive". Oxford Information Service. Available at <http://news.millersmiles.co.uk/archive>. [accessed 15/04/09]

- Millettary, J. (2006). "Technical trends in phishing attacks", CERT Coordination Center1. Available at www.cert.org [accessed 17/02/09]
- Mills,E. (2009). "Facebook hit by phishing attacks for a second day". Cnet news. Available at http://news.cnet.com/8301-1009_3-10230980-83.html [accessed 18/06/09].
- Ministry of Culture, Art and Heritage (2008). "Our Mission". Available at http://www.nccah.com/e_mcah.htm [accessed 07/11/09]
- Ministry of Foreign Affairs (2007a). "General information". Available at <http://english.mofa.gov.qa/details.cfm?id=6> [accessed 05/08/09].
- Ministry of Foreign Affairs (2007b) "Communications and transport". Available at <http://english.mofa.gov.qa/details.cfm?id=107> [accessed 05/08/09].
- Ministry of Foreign Affairs (2007c). "Education". Available at <http://english.mofa.gov.qa/details.cfm?id=28> [accessed 5 August 2009].
- Ministry of Industry & Commerce, Kingdom of Bahrain (2002). "GCC E-commerce Statistics". Available at <http://www.commerce.gov.bh/English/DomesticTrade/ECD/Statistics.htm> [accessed 01/07/09]
- Ministry of Public Prosecution (2004). "Penalties Law No. 11 of 2004". Legal Information Network for Gulf Cooperation Countries. Available at <http://www.gcc-legal.org/MojPortalPublic/BrowseLawOption.aspx?country=3&LawID=2597> [accessed 20/08/09].
- Mitchell, D.C. (2005). "Trusted Computing", Institution of Electrical Engineers.
- Mitnick, K. (2002). "The Art of Deception". Indianapolis,Wiley.
- Miyamoto, D., Hazeyama, H., Kadobayashi, Y. (2009). "An evaluation of machine learning-based methods for detection of phishing sites". Nara Institute of Science and Technology, Takayama, Ikoma, Nara, Japan, Vol. 5506/2009, pp.539-546.
- Monaghan, A. (2009). "UK economy slumped by 1.9pc in first three months of 2009 as recession deepens". Available at

- <http://www.telegraph.co.uk/finance/financetopics/recession/5212295/UK-economy-slumped-by-1.9pc-in-first-three-months-of-2009-as-recession-deepens.html> [accessed 24/11/09]
- Moore, J. (2009). "A portable document search engine to support off-line mobile learning". *Proceedings IADIS International Conference Mobile Learning*. Barcelona, Spain, 26th, February. Available at <http://eprints.ecs.soton.ac.uk/17441/>. [accessed 18/07/09]
- Moreno, R., Mayer, R. E., Spires, H. A. and Lester, J. C. (2001) "The case for social agency in computer-based teaching: Do students learn more deeply when they interact with animated pedagogical agents?" *Cognition and Instruction* Vol.19, No.2, pp. 177-213.
- Myers, M. D. and Avison, D. E. (2002). "An Introduction to Qualitative Research in Information Systems", London, Sage.
- Myers, M.D. (1997). "Qualitative research in information systems." *MIS Quarterly*, Vol. 21, No.2, pp.241-242.
- Nagy, J.; Pecho, P (2009). "Social networks security" *Proceeding, Emerging Security Information, Systems and Technologies, 2009. SECURWARE '09. Third International Conference on Digital Object Identifier*, pp.321 - 325
- Nagy, M. (2009), "Staying Safe in Cyber Space", ICT Qatar. Available at <http://www.ictqatar.qa/output/page1206.asp> [accessed 07/11/09].
- Naidu, S. (2004). "Learning design as an indicator of quality in teacher education." In. Rama, K. and Menon, M. (Eds.) (2004) *Innovations in teacher education - International practices for quality assurance* (pp. 65-76) Bangalore, NAAC.
- Naismith, L., Lonsdale, P., Vavoula, G. and Sharples, M. (2005). "Literature Review in Mobile Technologies and Learning". Report 11, NESTA Futurelab. Bristol: NESTA Futurelab.
- Nasr, L, N. (2009). "Living in Qatar". Motivate Publishing

Nazario, J. and Holz, T. (2008). "As the Net Churns: Fast-Flux Botnet Observations." *Proceedings International Conference on Malicious and Unwanted Software (Malware)*, IEEE Press, pp. 24-31

New York State Office of Cyber Security & Critical Infrastructure Coordination (2005). "Gone Phishing". A Briefing on the Anti-Phishing Exercise Initiative for New York State Government. Aggregate exercise results for public release.

NIST (National Institute of Standards and Technology Information Technology Laboratory). (2008). "NIST's Policy on Hash Functions". Available at <http://csrc.nist.gov/groups/ST/hash/policy.html> [accessed 06/03/09]

O'Brien, T.L. (2005) "Gone spear-phishing". *The New York Times*, 4 December. Available at <http://www.nytimes.com/2005/12/04/business/yourmoney/04spear.html?pagewanted=1&ei=5088&en=2f313fc4b55b47bf&ex=1291352400&partner=rssnyt&emc=rss> [accessed 28/12/09]

Office of the United States Trade Representative, Executive Office of the President. (2006). "Gulf Co-operation Council: Trade summary". Available at http://www.somalilandchamber.com/downloads/GCC_foreign_trade_barriers.pdf [accessed 20/01/09]

Ollman, G. (2004). "The phishing guide: understanding and preventing phishing attacks". White Paper, Next Generation Security Software Ltd. Available at <http://ngsconsulting.com> [accessed 28/07/09]

Orlikowski, W.J. and Baroudi, J.J. (1991). "Studying Information Technology in Organizations: Research Approaches and Assumptions." *Information Systems Research*, Vol. 2, No.1, pp. 1-28

Orr, T (2008). "Qatar, Cultures of the World". Qatar

Ossian, J.D. (2005). "The Qatar Edge", Qatar.

Pal, P. and Atighetchi, M. (2009). "The PhishBouncer experience". Piscataway, NJ, Washington, DC, USA, pp. 150-4.

- Pan, Y. and Ding, X.(2006). "Anomaly based web phishing page detection." *Proceedings 22nd Annual Computer Security Applications Conference (ACSAC'06)*.
- Pandit, M. (2006). "Go phish: how to prevent identity fraud", *Bank Technology News*, Vol. 19, No. 7, p. 33. Available at <http://proquest.umi.com/pqdweb?did¼1070767061&sid¼2&Fmt¼3&clientId¼57290&RQT¼309&VName¼PQD> [accessed 04/12/08].
- Pastor-Satorras, R. and Vespignani, A. (2007). "A Brief History of the Internet" in *Evaluation and Structure of the Internet, A Statistical Physics Approach*, Lavoisier., pp. 1-6
- Pather, S. and Remenyi, D. (2004). "Some of the philosophical issues underpinning research in information systems: from positivism to critical realism". *Proceedings 2004 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries*, Stellenbosch, South Africa, pp. 141-146
- Patterson, J. (2006). "Phishing with a phone call". Available at www.bankersonline.com [accessed 07/11/08]
- Pea, R. D. (1994). "Seeing what we build together: Distributed multimedia learning environments for transformative communications." *The Journal of the Learning Sciences*, Vol.3, No.3, pp. 285-299.
- Perry, C. (2001). "Case research in marketing." *The Marketing Review 2001*. Available at www.themarketingreview.com [accessed 30/09/09]
- Pope, A. (1711). "Essay on Criticism".
- Popper, K. (1959). "The Logic of Scientific Enquiry", London, Harper.
- Popper, K. (1971). "The Open Society and Its Enemies". Princeton, New Jersey, Princeton University Press
- Powell, R.R., 1997. "Basic research methods for librarians", 3rd edition. London, JAI Press

- Pruitt, S. (2005), "Firefox users snap up anti-phishing toolbar", *Network World*, Vol. 22, No. 21, p. 20. Available at www.networkworld.com [accessed 13/01/09]
- Punch, K. F. (2003), "Survey research: the basics", London, Sage.
- Qatar Exchange (QE) (2009). "About QE". Available at <http://www.dsm.com.qa/dsmsite/> [accessed 14/01/09]
- Qatar Law Forum (2009). "Qatar Justice in the 21st Century in Qatar". Available at <http://mn940.net/forum/> [accessed 11/08/09]
- Qatar Science and Technology Park (QSTP) (2007). "Qatar innovator, news from the frontline of technology business in Doha", issue 1. Available at <http://www.qstp.org.qa/files/other/QSTP%20Newsletter%20Apr07%20v16.html> [accessed 10/02/09]
- Qatar Statistic Authority (QSA) (2008). "Population in Qatar". Available at http://www.qsa.gov.qa/eng/population_census/2009/population_census_July.htm. [accessed 23/01/09]
- QatarVisitor (2000). "Qatar cultural pointers". Available at <http://www.qatarvisitor.com/index.php?cID=412&pID=973> [accessed 15/01/09]
- Qtel (2009a). "Qtel's Vision". Available at <http://www.qtel.com.qa/IndexPage.do> [accessed 15/01/09]
- Qtel (2009b). "ADSL FAQ". Available at <http://www.qtel.com.qa/ADSLFaq.do> [accessed 21/03/09]
- Qtel (2009c). "Dial Up – FAQ". Available at <http://www.qtel.com.qa/DialupFaq.do> [accessed 25/03/10]
- Qtel (2009d). "Qatar's Companies See Doubled Speeds with Qtel's Ongoing Internet Broadband Business ADSL Enhancement". Available at <http://www.qtel.com.qa/SearchDetails.do?search=16741> [accessed 04/02/10]
- Quinn, C. N. (2005). "Engaging Learning: Designing e-Learning Simulation Games". San Francisco, Pfeiffer.

- Radcliff, D. (2005a). "Phishers use spears, hooks and nets", *Network World*, Vol. 22, No. 12, p. 20. Available at www.proquest.umi.com [accessed 27/02/10].
- Radcliff, D. (2005b). "Fighting back against phishing", *Network World*, Vol. 22, No. 14, p. 48. Available at www.proquest.umi.com [accessed 03/12/09]
- Rapoport, R.N. (1970). "Three dilemmas in action research" *Human Relations*, Vol.23, No. 6, pp.499-513
- Remenyi, D. and Williams, B. (1996) "The Nature of Research: Qualitative or Quantitative, Narrative or Paradigmatic?" *Information Systems Journal*, Vol. 6, pp 131-146.
- Repenning, A. and Lewis, C.(2005). "Playing a game: The ecology of designing, building and testing games as educational activities." *Proceedings ED-Media, World Conference on Educational Multimedia, Hypermedia & Telecommunications, Association for the Advancement of Computing in Education.*
- Rescorla, E. (2000). "SSL and TLS: designing and building secure systems", Addison-Wesley. Available at http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6V8G-4TPHRHV-2&_user=122861&_coverDate=03%2F31%2F2009&_rdoc=1&_fmt=full&_orig=search&_cdi=5870&_sort=d&_docanchor=&view=c&_acct=C000010080&_version=1&_urlVersion=0&_userid=122861&md5=a9898724b3e162643e039b477a7e0bfe#bib9 [accessed 16/01/10]
- Rice, R. and Atkin, C. (eds.) (1989). "Public education campaigns", Newbury Park, Sage.
- Richardson T., "Brits Fall Prey to Phishing." *The Register*. Available at http://www.theregister.co.uk/2005/05/03/aol_phishing/, [accessed 27/11/09]
- Robila, S. A., James,J. and Ragucci, W. (2006). "Don't be a phish: steps in user education." *Proceedings 11th annual SIGCSE conference on Innovation and technology in computer science education. ITICSE '06*, pp. 237-241. New York, NY, USA.

- Rogers, E.M. and Storey, J.D. (1987). "Communication campaigns", In Berger, C.R. and Chaffe, S.H. (eds.) *Handbook of communication science*, Newbury Park, Sage
- Rohs, F. R. (1985) "Questionnaire Construction". Athens, GA: Cooperative Extension Service
- Roman (2009). "Top Fastest Growing Economies in 2009". Available at <http://www.financialjesus.com/2009/01/06/top-fastest-growing-economies/> [accessed 10/07/09]
- Rubin, D. C. and Wenzel, A. E.(1996). "One hundred years of forgetting: A quantitative description of retention" *Psychological Review*, Vol. 103, No. 4, pp. 734-760.
- Salant, P. and Dillman, D. (1994). "How to Conduct Your Own Survey". New York, Wiley
- Salowey, J., Zhou, H., Eronen, P. and Tschofenig, H (2006). "Transport layer security session resumption without server-side state", RFC 4507, Networking Working Group, Internet Engineering Task Force (IETF).
- Sambidge, A. (2009a). "Qatar's economy to see 9.6% growth in 2009 – report". Available at <http://www.arabianbusiness.com/557317-qatars-economy-to-see-96-growth-in-2009---report> [accessed 08/1/10]
- Sambidge, A. (2009b). "Qatar inflation seen falling to 7% in 2010 - report". Available at <http://www.arabianbusiness.com/555206-qatar-inflation-seen-falling-to-7-in-2010---report> [accessed 13/02/10]
- Sambidge.A (2009c). "Qatar predicted to grow during global crisis - World Bank" Available at <http://www.arabianbusiness.com/553132-qatar-predicted-to-grow-during-global-crisis---world-bank> [accessed 23/01/10]
- Saunders, M., Lewis, P. and Thornhill, A. (2000). "Research methods for business students". England: Prentice Hall
- Sausner, R. (2006). "Financial crime: using security to create insecurity", *Bank Technology News*, Vol. 19, No. 7, pp. 29. Available at <http://proquest.umi.com/pqdweb?did=>

- 1070767011&sid=2&Fmt=3&clientId=57290&RQT=309&VName=PQD, [accessed 27/12/09].
- Savill-Smith, C., Attewell, J. and Stead, G. (2006) "Mobile Learning". A report by LSN on the impact of mobile learning activities on teaching, learning and students' engagement in UK colleges.
- Schank, R. C. and Cleary, C. (1995). "Engines for Education". Hillsdale, NJ, Lawrence Erlbaum Associates.
- Schank, R. C., Fano, A., Bell, B., & Jona, M. (1994). "The Design of Goal-Based Scenarios". *The Journal of the Learning Sciences*, Vol.3, No.4, pp. 305-34.
- Schechter, S. E., Dhamija, R., Ozment, A. and Fischer, I. (2007). "The Emperor's New Security Indicators." In *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, Washington, DC, USA, IEEE Computer, Society, pp. 51-65.
- Schmidt, R. A. and Bjork, R. A. (1992) "New conceptualizations of practice: Common principles in three paradigms suggest new concepts for training." *Psychological Science*, Vol. 3, No. 4, pp. 207-217.
- Schofield, J. (2009). "A good day for phishing on Facebook and Twitter". Available at <http://www.guardian.co.uk/technology/blog/2009/may/21/twitter-facebook-phishing> [accessed 05/11/09]
- Schultz, J. (2002). "Effective, Inexpensive E-Learning Expands", Washington Technology. Available at http://www.washingtontechnology.com/news/1_1/daily_news/16728-1.html [accessed 25/06/09]
- Sekaran, U. (1992). "Research methods for business: a skill building approach", 2nd edition, New York, Chichester, Wiley.
- Shadish, W.R., Cook, T.D. and Campbell, D.T. (2002). "Experimental and Quasi-Experimental Designs for Generalized Causal Inference". New York, Houghton Mifflin.
- Sharples, M. (2000). "The design of personal mobile technologies for lifelong learning". *Computers & Education*, Vol. 34, pp. 177-193.

- Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L., Hong, J. and Nunge, E. (2007). "Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish". To appear in *Symposium on Usable Privacy and Security*.
- Shujun Li and Schmitz, R. (2009). "A novel anti-phishing framework based on honeypots". Piscataway, NJ; Tacoma, WA, USA
- Sophos (2005). "Phishing and the threat to corporate networks". Available at www.sophos.com, [accessed. 27/04/10]
- Sotirov, A., Stevens, M., Appelbaum, J., Lenstra, A., Molnar, D., Osvik, D. A. and de Weger, B (2008). "MD5 considered harmful today". Available at <http://www.win.tue.nl/hashclash/rogue-ca/> [accessed 30/12/08].
- Spitzer, R.J. (Ed.) (1993). "Media and public policy". Westport, CT, Praeger.
- Spitzner, L. (2002). "Honeypots tracking hackers". Addison Wesley. ISBN 0321108957.
- Stahl, B.C. (2005). "A critical view of the ethical nature of interpretive research: Paul Ricoeur and the other", *Proceedings 13th European Conference on Information Systems*, Regensburg, Germany.
- Stake, R.E. (1995). "The art of case study research". London, Sage.
- Steyn, T., Kruger, H. and Drevin, L. (2007). "IFIP International Federation for Information Processing", Volume 232, *New Approaches for Security, Privacy and Trust in Complex Environments*, Venter, H., Eloff, M., Labuschagne, M., Eloff, L. and R. von Sohns (eds.) Boston, Springer, pp. 193-203.
- Stray, J. (2008). "Web browser flaw could put e-commerce security at risk". Available at [CNET.com](http://news.cnet.com/8301-1009_3-10129693-83.html). Available at http://news.cnet.com/8301-1009_3-10129693-83.html. [accessed 24/02/09]
- Sudman, S. and Bradburn, N. M. (1982). "Asking Questions: A Practical Guide to Questionnaire Design". San Francisco, Jossey-Bass.

- Sunday Morning Herald (2004). "Phishing Spreads in Europe", Available at <http://www.smh.com.au/articles/2004/05/10/1084041315645.html>, [accessed 05/01/ 09]
- SurfControl (n.d.). "SurfControl plc", Congleton. Available at www.surfcontrol.com [accessed 03/05/10]
- Symantec (2006). "Internet Security Threat Report – Trends for January 2006-June 2006", Vol. 10, September. Available at www.symantec.com [accessed 05/01/10]
- Tally, G. (2009). "Phisherman: a phishing data repository". Piscataway, NJ, Washington, DC.
- Tally, G., Thomas, R. and Vleck, T.V. (2004). "Anti-Phishing: Best Practices for Institutions and Consumers". Technical report. McAfee Research
- Tally, G., Sames, D., Chen, T., Colleran, C., Jevans, D., Omiliak, K., and Rasmussen, R. (2006) "The Phisherman Project: Creating a Comprehensive Data Collection to Combat Phishing Attacks." *Journal of Digital Forensic Practice*, July 2006, Vol. 1, Iss. 2, pp. 115 – 129
- Tanneeru, M. (2005). "A convicted hacker debunks some myths". CNN. Available at <http://edition.cnn.com/2005/TECH/internet/10/07/kevin.mitnick.cnn/index.html> [accessed 01/12/09].
- Technology News Daily (2005), "Phishing attacks solicits donations for bombing victims", 4 August. Available at www.technologynewsdaily.com [accessed 05/01/10]
- Tellis, W. (1997). "Introduction to case study. The Qualitative Report", Vol. 3, No.2. Available at www.nova.edu/ssss/QR/QR3-2/tellis1.html [accessed 30/09/09]
- The Economist. (2008). "GDP growth forecasts, 2009" Available at http://www.economist.com/markets/indicators/displaystory.cfm?story_id=12818136 [accessed 16/12/08]
- The Honeynet Project (2007). "Know Your Enemy: Fast-Flux Service Networks" Available at www.honeynet.org/papers/ff. [accessed 07/12/09]
- Themistocleous, M. (2002). "Enterprise Application Integration", Brunel University.

- Tout, H. and Hafner, W. (2009). "Phishpin: an identity-based anti-phishing approach", Vol.3, pp. 347-52. Piscataway, NJ, Vancouver, BC, USA
- Trochim, W. M. (2006). "*The Research Methods Knowledge Base* 2nd Edition". Available at <http://www.socialresearchmethods.net/kb/>. [accessed 07/11/08]
- Trochim, W.M.K. (2002). "Types of Surveys, Research Methods Knowledge Base", 2nd Edition.
- Tsai, C. (2005). "Survey: 43 percent of adults get 'phished'" Available at www.siliconvalley.com, [accessed 17/06/09].
- U.S. Department of State Diploma in Action (2007). "International Religious Freedom Report 2007 – Qatar" Available at <http://www.state.gov/g/drl/rls/irf/2007/90219.htm> [accessed 13/09/08]
- United Nations Development Programme (2009). "Human Development Report 2007/2008, Fighting climate change: Human solidarity in a divided world" Available at <http://hdrstats.undp.org/fr/indicators/89.html> [accessed 01/09/08]
- United States Department of State (2005). "International Religious Freedom Report (2005)". Bureau of Democracy, Human Rights, and Labor. Available at <http://www.state.gov/g/drl/rls/irf/2005/51608.htm> [accessed 25/03/09].
- Urban Planning and Development Authority (2006). "The Master Plan of Qatar" Available at <http://www.up.org.qa/upeng/modules.php?name=News&file=article&sid=7>. [accessed 18/01/10]
- US-CERT (United States Computer Emergency Readiness Team), (2008)., "MD5 vulnerable to collision attacks". Vulnerability Note VU#836068. Available at <http://www.kb.cert.org/vuls/id/836068> [accessed 20/10/09]
- Uusitalo, I., Catot, J.M., Loureiro, R (2009). "Phishing and countermeasures in Spanish online banking." In *proceedings* Third International Conference on Emerging Security Information, Systems and Technologies, pp.167-172.
- Van Dam, N. (2001) "Where is the Future of Learning?" *e-Learning Magazine*. p. 160.

- Van der Merwe, A., Loock, M. and Dabrowski, M.(2005). “Characteristics and responsibilities involved in a phishing attack”. *Proceedings 4th International Symposium on Information and Communication Technologies (ISICT 2005)*.
- Vecchiatto, P. (2005). “Web scammers cash in on tsunami”, 7 January. Available at www.itweb.co.za [accessed 27/08/09]
- Vegter, I. (2005). “Plugging the ‘phishing’ hole”, *iWeek*, Vol. 5, pp.16-18
- Vodafone (2009) “About Vodafone”. Available at <http://www.vodafone.com.qa/go/en/aboutus/aboutvodafone> [accessed 01/12/09]
- Vreede, G.J.D. (1995). “Facilitating organisational change: The participative application of dynamic modelling”, Delft University of Technology.
- W3C (2010) “A Little History of the World Wide Web”, Available at <http://www.w3.org/History.html> [accessed 10/10/2010]
- Wagner, M. (2004) “Will Trade Passwords for Chocolate”, *Security Pipeline*, April 2004 Available at <http://www.securitypipeline.com/news/18902074> [accessed 04/01/09]
- Walsham G. (1995). “The emergence of interpretivism in IS research” *Information Systems Research*, Vol. 6, No. 4, pp. 376-394.
- Walsham, G. (1993). “Interpreting information systems in organizations”. Chichester, Wiley.
- Wardman, B., Shukla, G. and Warner, G. (2009). “Identifying vulnerable Websites by analysis of common strings in phishing URLs”. Piscataway, NJ, USA Tacoma, WA, USA, 13 pp. 1 – 13.
- Webber, R. (2004). “The rhetoric of positivism versus interpretivism: A personal view” Editor’s comments. *MIS Quarterly*, Vol. 28, No. 1, pp. iii-xii
- Weissman, C (1994). “Penetration Testing”. In *Information Security Essays*. IEEE Computer Society Press.

- Weissman, C (1995). "Penetration Testing". In Handbook for the Computer Security Certification of Trusted Systems. Naval Research Laboratory Technical Memorandum, 24 January 1995.
- Welman, C. and Kruger, F. (1999). "Research methodology for the business and administrative sciences". Cape Town, Oxford University Press
- White House (2006). "Executive Order of President George W. Bush: Strengthening Federal Efforts to Protect against Identity Theft", 10 May, Office of the Press Secretary. Available at www.whitehouse.gov, [accessed 13/04/09].
- Whitten, A. and Tygar, D. (1999). "Why Johnny can't encrypt: A usability evaluation of PGP 5.0". In *Proceedings 8th USENIX Security Symposium*, Washington, D.C., August 1999, vol. 8, pp. 169-183.
- Whitten, W. B. and Bjork, R. A. (1977). "Learning from tests: Effects of spacing." *Journal of Verbal Learning and Verbal Behavior*, Vol. 16, No.4, pp. 465-478.
- Willems, J. (2005). "Flexible learning: Implications of "when-ever", "where ever" and "what-ever"". *Distance Education*, Vol. 26, No.3, pp.429-435.
- Wilson, J. and Wilson, S. (2001). "Mass media, mass culture: An introduction", 5th edition. Boston, MA, McGraw-Hill.
- Wimmer, R. and Dominick, J. (1991). "Mass media research: An introduction", 3rd edition. Belmont, CA, Wadsworth.
- Windahl, S., Signitzer, B., and Olsen, J.T. (1992). "Using communication theory: An introduction to planned communication". London, Sage.
- Winder, D. (2009). "Stupid security attacks". *PC Pro UK*, No.180, pp. 135-7.
- WombatTM Security Technologies (2009). "An Empirical Evaluation of PhishGuroTM Embedded Training". Available at <http://wombatsecuirty.com/> [accessed 06/01/10]
- Wu, M. (2006). "Fighting Phishing at the User Interface". PhD. thesis, MIT. Available at <http://groups.csail.mit.edu/uid/projects/phishing/minwuthesis.pdf>. [accessed 20/09/09]

- Wu, M., Miller, R. C. and Garfinkel, S. L. (2006). "Do security toolbars actually prevent phishing attacks?" *Proceedings SIGCHI Conference on Human Factors in Computing Systems*, Montréal, Québec, Canada, 22 - 27 April) in. R. Grinter, T. Rodden, P. Aoki, E. Cutrell, R. Jeffries and G. Olson (Eds.) CHI '06. ACM Press, New York, NY, pp.601-610. Available at <http://doi.acm.org/10.1145/1124772>. [accessed 02/02/10]
- Xin, L and Qinyu, L. (2007). "Awareness education as the key to ransomware prevention." *Information Systems Security USA*, Vol.16, No.4, pp. 195-202.
- Ye, Z., Yuan. Y. and Smith, S. (2002). "Web Spoofing Revisited: SSL and Beyond". Tech. Rep. Department of Computer Science, Dartmouth College, TR2002-417.
- Ye, Z.T., Smith, S. and Anthony, D. (2005). "Trusted paths for browsers", *ACM Transactions on Information and System Security (TISSEC)*, Vol. 8, No. 2, pp. 153-186. Available at <http://portal.acm.org/citation.cfm?doid=1065545.1065546> [accessed 11/02/10]
- Yee, K. P. and Sitaker K. (2006). "PassPet: Convenient Password Management and Phishing Protection." *Proceedings Second Symposium on Usable Privacy and Security*, Pittsburgh, Pennsylvania, July 12 - 14,). SOUPS '06, Vol. 149. ACM Press, New York, NY, pp. 79-90. Available at <http://doi.acm.org/10.1145/1143120.1143126>. [accessed 18/01/10]
- Yin, R.K. (1989) "Case Study Research: Design and Methods", 1st edition, Beverly Hills, CA, Sage.
- Yin, R.K. (1994). "Case Study Research: Design and Methods", 2nd edition, Newbury Park, Sage.
- Yu, W.D., Nargundkar, S. and Tiruthani, N. (2009). "PhishCatch: a phishing detection tool." In *Proceedings Computer Software and Applications Conference, 2009. COMPSAC '09. 33rd Annual IEEE International* , IEEE Computer Society, Washington, DC, USA, vol.2, pp. 451-456.
- Zaharias, P. (2004). "Usability and e-Learning: The road towards integration." *ACM eLearn Magazine*, vol.2004, N.6.

Zenger, J. and Uehlein, C. (2001) "Why Blended Will Win", *Training and Development Magazine*, VOL. 55, NO. 8, pp. 54-60.

Zhang, C., Chen, X., Chen, W-B., Yang, L., and Warner, G. (2009). "Spam image clustering for identifying common sources of unsolicited emails." *International Journal of Digital Crime and Forensics USA*, Vol.1, No.3, pp. 1-20

Zhang, Y., Egelman, S., Cranor, L. and Hong, J.(2007) "Phinding Phish: Evaluating Anti- Phishing Tools." *Proceedings 14th Annual Network and Distributed System Security Symposium (NDSS'07)*.