

Mutual authentication and phishing – a clear case of user confusion

Jane Elizabeth Adams

Submitted in partial fulfilment of
the requirements of Edinburgh Napier University
for the Degree of
MSc in Advanced Security and Digital Forensics

School of Computing

August 2012

Authorship Declaration

I, Jane Elizabeth Adams, confirm that this dissertation and the work presented in it are my own achievement.

Where I have consulted the published work of others this is always clearly attributed;

Where I have quoted from the work of others the source is always given. With the exception of such quotations this dissertation is entirely my own work;

I have acknowledged all main sources of help;

If my research follows on from previous work or is part of a larger collaborative research project I have made clear exactly what was done by others and what I have contributed myself;

I have read and understand the penalties associated with Academic Misconduct.

I also confirm that I have obtained **informed consent** from all people I have involved in the work in this dissertation following the School's ethical guidelines

Signed:

Date:

Matriculation no: 10017089

Mutual authentication and phishing – a clear case of user confusion

Data Protection Declaration

Under the 1998 Data Protection Act, The University cannot disclose your grade to an unauthorised person. However, other students benefit from studying dissertations that have their grades attached.

Please sign your name below *one* of the options below to state your preference.

The University may make this dissertation, with indicative grade, available to others.

The University may make this dissertation available to others, but the grade may not be disclosed.

The University may not make this dissertation available to others.

Abstract

The aim of this dissertation was to gain a better understanding of how users carry out mutual authentication and protect themselves from phishing, with the intention of enabling the banking industry to offer better educational and technical responses to phishing. It achieved this by looking at how users react to phishing and to existing anti-phishing methods and examining questions of responsibility, how personality affects online behaviours and links between online and offline behaviour.

The methodological approach taken was largely qualitative, following a mixed paradigm of critical analysis and interpretivism. The data for the dissertation was gathered using a literature review, interviews of industry experts and an online survey of computer users. The findings of each approach were compared and analysed.

The results showed differences between expert opinion and user experience with the surveyed users in general appearing concerned and responsible about protecting themselves but hampered by a fundamental lack of understanding about phishing and how to combat it. In particular there was confusion about how it differed from other types of security threats. Contrary to expectations, users displayed higher levels of concern about online crime than physical world crime. There were some differences in attitudes and approaches as a result of age, levels of computing knowledge and impulsiveness. Expert users were not necessarily better at protecting themselves.

The main contribution of the work was in showing that users appear more responsible than expected but are also still confused. It highlights the differences between the technologist's view of the user and how users view themselves online and leaves open the potential for making anti-phishing educational initiatives more relevant and targeted and mutual authentication approaches more personalised and layered.

Table of Contents

1	INTRODUCTION	1
1.1	The research problem and context	1
1.1.1	Context of the dissertation	1
1.2	Studies that have addressed the problem	2
1.3	Existing study deficiencies	3
1.4	Aims	3
1.5	Organisation of the dissertation	3
2	LITERATURE REVIEW.....	5
2.1	Introduction	5
2.2	Phishing.....	5
2.2.1	Why users fall for phishing.....	7
2.2.2	Industry approaches to tackling phishing.....	12
2.2.3	Conclusions about phishing	18
2.3	Identity	19
2.3.1	A summary of relevant thought about identity in general	19
2.3.2	Online identity	20
2.3.3	Implications for understanding identity within online banking.....	21
2.4	Summary and research questions.....	23
3	RESEARCH METHODOLOGY	25
3.1	Introduction.....	25
3.2	Literature search methods and results	25
3.3	Research data required.....	25
3.4	Methodology chosen.....	26
3.4.1	Philosophical assumptions.....	26
3.4.2	Methods	27
3.5	Expert opinion.....	28
3.5.1	Interview content	29
3.6	User data	29
3.6.1	Survey content	30
3.6.2	Sampling used	30
3.7	Disadvantages of chosen methods	30
3.7.1	Alternative methods	32
3.8	Data analysis process	32
3.8.1	Expert opinions	32

3.8.2	User survey	32
3.9	Evaluation framework	33
3.10	Chapter conclusion	33
4	FINDINGS FROM EXPERT INTERVIEWS	34
4.1	Introduction	34
4.2	Interview analysis process	34
4.3	Interview findings	34
4.3.1	What is the relationship between online and offline behaviour and how does it impact the response to phishing?	35
4.3.2	Why do users fall for phishing?	36
4.3.3	Do personality factors have any effect on how people deal with phishing?	40
4.3.4	Whose responsibility is it to protect the user against phishing?	42
4.3.5	How do users react to existing anti-phishing methods?	44
4.3.6	How can existing anti-phishing methods be improved?	52
4.4	Chapter conclusion	56
5	FINDINGS FROM THE USER SURVEY	57
5.1	Introduction	57
5.2	Results of the filtering questions	57
5.3	Perceptions of security	58
5.4	Learning to avoid phishing	60
5.5	Protecting against phishing	62
5.6	User personae	65
5.6.1	Age	65
5.6.2	Knowledge of computing	66
5.6.3	Speed of decision making	67
5.7	Chapter conclusion	67
6	DISCUSSION	68
6.1	Introduction	68
6.2	Research questions	68
6.2.1	Why do users fall for phishing?	68
6.2.2	Do personality factors have any effect on how people deal with phishing?	71
6.2.3	What is the relationship between online and offline behaviour and how does it impact the response to phishing?	72
6.2.4	How do users react to anti-phishing methods?	73
6.2.5	Means of improving anti-phishing methods	75
6.2.6	Responsibility for protecting user against phishing	78

6.3	Chapter conclusion	79
7	CONCLUSION AND FUTURE WORK.....	80
7.1	Aim of the dissertation.....	80
7.1.1	How are users responding to phishing?	80
7.1.2	Do personality factors have any effect on how people deal with phishing?	81
7.1.3	What is the relationship between online and offline behaviour and how does it impact the response to phishing?	81
7.1.4	How do users react to existing anti-phishing methods?	82
7.1.5	How can anti-phishing methods be improved?	82
7.1.6	Whose responsibility is it to protect the user against phishing?	82
7.2	Critical reflection	83
7.2.1	Methodological issues.....	83
7.2.2	Limitations	83
7.3	Future work	84
7.3.1	Inconsistencies between findings	84
7.3.2	Building on findings.....	84
7.4	Contributions to body of knowledge and relationship to larger area of study.....	86
7.5	Recommendations.....	86
7.6	Conclusion	86
8	BIBLIOGRAPHY	87
9	A1 - GLOSSARY.....	95
10	A2 - PROJECT MANAGEMENT	97
10.1	Discussion	97
10.2	Project Plan.....	98
11	A3 - SUMMARY OF LITERATURE REVIEW FINDINGS IN CHART FORM100	
12	A4 - EXPERT INTERVIEW QUESTIONS.....	103
13	A5 - DATA AND QUESTIONS FROM THE USER SURVEY	105
13.1	Answers to survey questions	105
14	A6 - EVALUATION FRAMEWORK.....	134

List of Tables

Table 1 Comparison between levels of concern about online and offline crime (adjusted)	59
Table 2 Preferred channel for receiving anti-phishing educational material	62
Table 3 Preferred source of information by age	65
Table 4 Age of respondents	106
Table 5 Computing knowledge of respondents	107
Table 6 Decision speed of respondents	107
Table 7 Level of concern about online crime	108
Table 8 Level of concern about offline crime	108
Table 9 Victims of online crime	109
Table 10 Victims of other forms of crime	109
Table 11 How often bank security messages are read	110
Table 12 Whether respondents have seen information about phishing	111
Table 13 Source of information seen about phishing	112
Table 14 Whether information seen was read	113
Table 15 How easy the information was to understand	113
Table 16 Whether behaviour changed as a result of seeing information	114
Table 17 Behaviour change by gender and source of information	114
Table 18 Preferred source of information about phishing	115
Table 19 Whether banks should refund phishing losses	117
Table 20 Whether people take precautions against phishing	117

List of Figures

Figure 1 HTML phishing message from 118.45.190.188 in Korea	6
Figure 2 An example of an email where it is unclear whether it is a phishing email or a genuine email from an outsourced email address	13
Figure 3 A phishing warning from Virgin Media	14
Figure 4 Example of an anti-phishing educational message.....	74
Figure 5 Introductory questions of the survey.....	105

Acknowledgements

I would like to thank my supervisor Peter Cruickshank for his valuable and consistent encouragement, suggestions and help, without which this dissertation would not have reached the standard that it has. I would also like to thank my second marker Robert Ludwiniak for his helpful feedback and Dr. Elias Ekonomou, Professor Bill Buchanan and Professor Jessie Kennedy for their assistance. Finally I would like to thank all the interviewees, survey participants and people who publicised the survey who provided such invaluable data for the project.

1 Introduction

1.1 The research problem and context

The introduction to this dissertation will introduce the research problem and background context. It will outline previous research approaches to the topic and will lay out the aims of the study and the dissertation structure.

Phishing is the act of tricking individuals online into revealing sensitive information, for example passwords or PINs and other banking details, which phishers then exploit for fraudulent purposes. Mutual authentication involves not just the user authenticating themselves to the service but the service providing evidence to the user that it is genuine (Alpar, Hoepman, and Siljee, 2011). It is the failure of this that makes phishing possible.

The research aims to help mitigate the problem of phishing by looking at the reasons why computer users fall for phishing attacks, how they carry out mutual authentication and why those methods let them down and to see if any light can be shed on this by considering the problem through the lens of recent thought and theory on the nature of online identity and behaviour. The discussion will primarily cover home users or those not protected by corporate computer security programmes.

1.1.1 Context of the dissertation

The Anti Phishing Working Group, a cross industry association formed to counter phishing, defines phishing as follows:

“Phishing is a criminal mechanism employing both *social engineering* and *technical subterfuge* to steal consumers’ personal identity data and financial account credentials. Social engineering schemes use spoofed emails purporting to be from legitimate businesses and agencies to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as usernames and passwords. Technical subterfuge schemes plant crimeware onto PCs to steal credentials directly, often using systems to intercept consumers online account user names and passwords and to corrupt local navigational infrastructures to misdirect consumers to counterfeit websites (or authentic websites through phisher-controlled proxies used to monitor and intercept consumers’ keystrokes).” (Anti Phishing Working Group, 2011).

Because phishing relies on confusing people, it can also be called a semantic attack (Egelman, Cranor, and Hong, 2008).

Spear-phishing is highly personalised phishing, aimed at specific individuals, often financial management or IT personnel within specific companies and will only be touched on peripherally in this dissertation.

This dissertation will be primarily concerned with phishing techniques that involve social engineering and counterfeit websites rather than phisher-controlled proxies as in the latter case, users have little or no chance of identifying fraud through mutual authentication methods until after it has happened. A glossary of terms used can be found in appendix 1.

Globally, figures from the Anti Phishing Working Group show that the number of phishing websites detected per month in H1 2011 peaked at 38,173 in March 2011, down 32% on the all time high figure of 56,362 detected in August 2009, while the number of phishing attacks reported per month in H1 2011 reached a high of 26,402 in March 2011, down 35% on the all time high, again in August 2009, of 40,621. Attack figures dipped in September 2011 at 18,388 attacks (website numbers did not drop) but rose again later in the year to 32,979 attacks and 48,410 websites in December 2011. Attacks are increasingly focusing on brands based in Latin America, the Middle East and Asia but the country hosting the most phishing sites is the United States (Anti Phishing Working Group, 2011). APWG did not release figures for financial losses resulting from phishing.

According to Financial Fraud Action UK, the industry body that co-ordinates fraud prevention for the UK financial services sector, phishing attacks in the UK in 2011 rose 80% on 2010 figures to 111,286 (N.B. this figure is an annual total against the APWG's monthly totals), although online banking fraud figures for the same period dropped 24% to £35.4 million. Financial Fraud Action UK attributed this drop in monetary value lost to customers using anti-virus software and other software packages provided by banks such as Trusteer Rapport, and also hand-held authentication devices as well as to banks becoming more effective at detecting and removing fraudulent websites (Financial Fraud Action UK, 2012).

These figures suggest that against a background of maintained but fluctuating activity from fraudsters, losses are beginning to fall, in part due to technological fixes from the banks. However there is clearly still a considerable amount of phishing activity going on.

At present, nearly 90% of all phishing attacks focus on targets that are either explicitly financial sector or retail in nature or involve payments in some shape or form (Anti Phishing Working Group, 2011) but in the future there is the concern that unless a more secure means of authentication and mutual authentication is found, compared to usernames and passwords, phishing will also target single sign on systems, laying every aspect of the user's online identity and activity open to phishing. In addition phishers are also turning their attention to sites like Facebook, working on the premise that many people use the same password for banking and other activities.

1.2 Studies that have addressed the problem

Studies to date suggest that identity management is not a primary goal for users online and they often fail to take precautions against identity theft attacks and phishing (Wilson and Argles, 2011) even when technical tools and education are available. The studies examined in the literature review contained in this dissertation primarily cover work done on user behaviours around recognising phishing and carrying out mutual authentication and on how to combat phishing. Conclusions include that users do not view security as a primary activity, that warnings and toolbars have limited efficacy and that users tend to focus on site content and presentation as an indicator of authenticity. The literature is inconclusive as to whether knowledge of security cues and indicators do protect users or not and on whether user education is worthwhile.

The literature review also includes a brief theoretical section on identity and its role in the online world, with an emphasis on the user's understanding of their online identity rather than the technologist's concept of digital identity. The intention is to examine this understanding and then see if it can be applied to the area of online security, in particular both to user reactions to phishing and anti-phishing education, to help illuminate the findings of primary research carried out later in this study.

1.3 Existing study deficiencies

The literature reviewed falls primarily into two camps – quantitative studies on phishing carried out on subjects under laboratory conditions, often involving role play – and reviews of studies producing lists of topics that still need to be researched. There are concerns discussed within the literature that role play based studies cannot adequately reproduce the real life experience of day-to-day behaviour online. The situation is already artificial and in some studies the boundary between primary and secondary activities becomes blurred, whereas in real life security awareness is often not the primary focus or activity. In part, this informed the decision taken in this dissertation to proceed in a qualitative direction, investigating through interviews and a self-reported survey both expert perception and user experience, with an objective of examining phishing without the artificial constraints of laboratory conditions.

There is also a general lack of reference to theory about online identity. Equally the literature on online identity tends to focus more on user activity in online gaming and social networking than on banking and payments types of activity. The discussions in this dissertation are intended to discover whether that is justified and perhaps in some small part to start to remedy that omission. However this is an ancillary part of the work and the main emphasis will be on the outcomes of the primary research.

1.4 Aims

The aim of this dissertation is to gain a better understanding of how users carry out mutual authentication and protect themselves from phishing with the intention of enabling the banking industry to offer better educational and technical responses to phishing. It will achieve this by answering the following research questions, refined from the draft questions from the original proposal, through a literature search, expert interviews and an online user survey:

- Why do users fall for phishing?
- Do personality factors have any effect on how people deal with phishing?
- What is the relationship between online and offline behaviour and how does it impact the response to phishing?
- How do users react to existing anti-phishing methods?
- How can existing anti-phishing methods be improved?
- Whose responsibility is it to protect users against phishing?

1.5 Organisation of the dissertation

Chapter one of the dissertation forms this introduction, outlining the content of the study and the aims.

Chapter two reviews relevant literature, covering both phishing studies and the fundamentals of theory about identity and, in particular, about online identity.

Chapter three presents the chosen methods and methodology of the project, outlining and justifying the approach taken in gathering data.

Chapter four reviews the findings of the expert interviews, split into themes gathered from the literature review.

Chapter five summarises and reviews the findings of the user survey.

Chapter six considers the findings of both the expert interviews and the user survey, reviewing them in the light of the theory outlined in the literature review.

Chapter seven concludes the dissertation, evaluating the findings in the light of the aims of the project and discussing whether the project succeeded in meeting these aims. It also lays out areas for further research.

The appendices contain materials used during the research, including a fuller presentation of the survey data. There is also a discussion of the project management of the research.

2 Literature review

2.1 Introduction

As outlined in chapter one, the research covers the topic of phishing and whether a better understanding of online identity can improve ways in which online users are protected or protect themselves against phishing.

Existing research examined in this review covers work on user strategies for recognising phishing and carrying out mutual authentication and on how to combat phishing. The review touches only briefly on technological responses to phishing, where they concern user experience but does point out that if existing flaws in these solutions can be overcome, they do have the benefit of removing user fallibility from the equation.

There will also be a brief theoretical examination of the broader understanding of the nature of identity and how this is represented in a modern online setting. The intention is to extend this understanding beyond social media and games, where much of the research appears to focus and to apply it to the area of online security and in particular both to user reaction to phishing and anti-phishing education. There does not appear to be many references in existing studies of phishing to these theories. The purpose of this explanation of theory is to discover whether it in any sense illuminates findings of existing studies and whether it can be applied to findings of primary research to be carried out later in this study on questions arising from the literature review.

The literature about phishing therefore primarily involves user studies whereas the literature about identity is largely theoretical.

There is some concern about how well studies of user reactions to phishing attacks can reproduce real life experience – those concerns will be highlighted with respect to specific studies. Studies have either focused on security as a primary task or more realistically have attempted to make it a secondary task but there are questions about how feasible that is in a test environment.

The review starts with a brief discussion of phishing as a general topic, building on the definitions given in chapter one. It then looks at user reactions to phishing before moving on to ways in which service providers have attempted to protect users from phishing. It then examines theory of online identity, tying it in to broader sociological and psychological thought about identity before considering its applicability to online banking use and phishing in particular.

2.2 Phishing

As discussed in the introduction to this dissertation, phishing is the act of tricking individuals online into revealing sensitive information, for example passwords or PINs (Wilson and Argles, 2011). The process generally involves sending emails that then cause the recipient to either visit a fraudulent website and enter their information or to visit a genuine website via a phishing proxy carrying out a man in the middle attack, which then harvests the details

entered into the genuine website. It is a form of social engineering, which is techniques used to dupe people into disclosing information or performing actions (Workman, 2008).

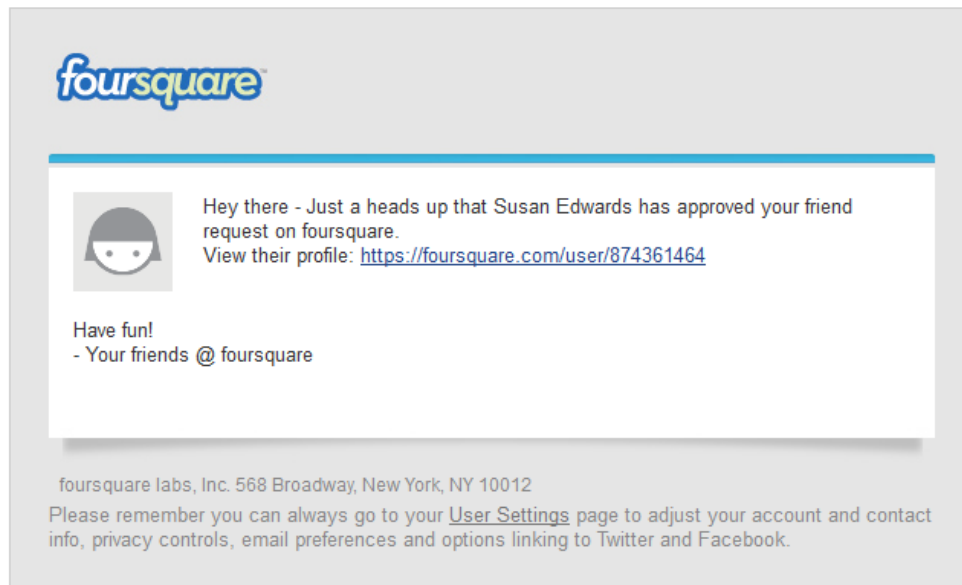


Figure 1 HTML phishing message from 118.45.190.188 in Korea

Most of the papers reviewed here discuss 'phishing websites' and how users recognise them. This process on the part of the user of reassuring themselves that they are on a genuine website is what is described as 'mutual authentication' in this document. Some authors discuss how to recognise phishing emails rather than websites – it is arguable whether that is exactly mutual authentication for the purposes of this document but it is still relevant to the proposed research, particularly since HTML emails are in essence web pages.

In general, banks authenticate their users using a simple user name and password process over a SSL connection and offer valuable pickings to online fraudsters who manage to subvert that process. This makes online banking customers a key target for phishing and making the need for reliable mutual authentication in online banking vital.

However the problem is much broader than just banking or indeed other transaction related phishing targets such as eBay. Indeed the need for reliable mutual authentication mechanisms is identified by authors surveying outstanding issues in identity management as one of the most significant problems still to be solved. Alpar, Hoepman, and Siljee (2011) for example point out that phishing attacks may in the future extend from aiming to obtain credentials from individual service providers (such as banks) to targetting identity provider credentials, compromising users over a wider part of their Internet activities. The use of HTTP redirects as used in OpenID makes that even more of a danger (Dhamija and Dusseault, 2008). Alpar, Hoepman, and Siljee (2011) also state that successful mutual authentication should not require users to use the same computer all the time, nor to install special software. As the following discussions show, there does not appear to be a simple solution to that problem at present. Instead their aim is to highlight areas where there does not appear to be a consensus about what is effective. While the review does consider some technical solutions, the primary focus is on user education.

2.2.1 Why users fall for phishing

There are various theories about why users still fall prey to phishers, even though phishing has been a recognised phenomenon for many years. These include lack of awareness (Yu, Nargundkar, and Tiruthani, 2008) and the associated result that people only react to threats they are aware of, lack of technical expertise (Anandpara, Dingman, Jakobsson, Liu, and Roinestad, 2007), fear of and panic about losing money brought about by wording of phishing emails (Yu, Nargundkar, and Tiruthani, 2008) and failure to read anti-phishing education.

Users may also not be able to decide how to handle security interactions, they may believe that existing protection is stronger than it is, they dislike having task based activity interrupted, they may become fatigued by warning messages, messages are presented in a way that is confusing (ed: Roessler and Saldhana, 2010) and user education is too complex to understand (Sample, 2012). Identity management in general places a considerable cognitive burden on the user already (Dhamija and Dusseault, 2008).

Not only may they not know what security indicators to look out for but many of these can also be spoofed by phishers (Anandpara, Dingman, Jakobsson, Liu, and Roinestad, 2007). Toolbar warnings may also be disregarded because of misapprehensions about what phishing is (Kumaraguru, Sheng, Acquisti, Cranor, and Hong, 2007). Research carried out by Furnell (2007) showed that while nearly all Internet users recognise terms such as 'virus' or 'hacker', only 68% claimed to know what phishing meant (Furnell, 2007). Of those who had heard of it, some understood it incorrectly, thinking that it referred to the topic of the message rather than the intention. For example some people may think phishing concerns only banking or refers only to emails.

On the other hand expert users may also ignore browser toolbar warnings (Egelman, Cranor, and Hong, 2008), presumably because they feel they have sufficient expertise to identify phishing without relying on warnings. This could also potentially apply to people who have previously been victims of phishing and expect all further attacks to be identical. It also suggests that a feeling of high computer self efficacy, where an individual's beliefs about their ability to use a computer system affects their use of it (Compeau and Higgins, 1995), can sometimes lead to counterproductive outcomes when it comes to security.

Taylor quotes earlier research he carried out for 2006 which showed that in a corporate setting, managers were overly optimistic about employee awareness of computer security (Taylor, 2008, p145). It is possible that individuals outside of their work setting feel equally over-confident, despite a range of things that phishers do that could give them away, such as obviously incorrect URLs, specific and incorrect user information and grammatical and spelling mistakes (although this may not be so apparent to Internet users with reduced literacy or English as a second language) (Furnell, 2007).

In addition users do not generally view security as a primary activity and therefore are not looking out for threats in the first place (Anandpara, Dingman, Jakobsson, Liu, and Roinestad, 2007). Phishing attacks are also becoming more sophisticated, based on the knowledge about how users react that phishers build up and on the amount of context that they are able to inject into attacks (Jagatic, Johnson, Jakobsson, and Menczer, 2007).

The concept of bounded rationality may come into play – users will make decisions about emails and websites based on the information they have, not all available information. While people make decisions about risk based on the perceived severity of the consequences and how likely they are to occur (Slovic, 1987) cited by Taylor (2008, p145), if no risk is perceived

then those calculations do not occur. Equally, even if there is risk, if the risk is considered minor because the user knows that the bank will refund any losses in the case of phishing then a cost benefit analysis will suggest that the potential inconvenience caused by losing access to a bank account or whatever the phishing email is threatening is greater than the risk of loss if the email is fraudulent.

Indeed, Rational Choice Theory, which sees the user as a rational, utility maximiser (Grix, 2004, p93) suggests that within their specific context and with the information they have available, the user who falls for a phishing attack is making a rational decision about the best outcome for them.

The Technology Acceptance Model (TAM) states that the degree to which users accept technological systems depends on both perceived usefulness and perceived ease of use (Davis, Bagozzi, and Warshaw, 1989). If users are not particularly concerned about loss of financial credentials, be it in the trial or in real life, and find anti-phishing systems difficult to use, the model predicts that they will not use them.

A later model derived from TAM, the Unified Theory of Acceptance and Use of Technology offers three determinants of intention to use – performance expectancy, effort expectancy, social influence – plus two of usage behaviour – intention and facilitating conditions (factors that make the system easy to use). These factors are also mediated by gender, age, voluntariness of use and experience (Ventakesh, Viswanath, Morris, Davis, and Davis, 2003). So again, a user who does not value his/her financial credentials, thinks that looking out for security cues is hard work and does not have any external parties applying pressure on him/her to do so is unlikely to make much effort to stay secure.

Finally, Lazy User Theory suggests that the user will mainly do the minimum to satisfy their information needs (Tetard and Collan, 2009) based on their need and situation – again if there is no perceived need or desire to make an effort to protect against phishing, the user is unlikely to do so, because it would add to the effort required to fulfil their primary task.

Taylor (2008) makes the point that in the corporate world, it may take a major security related loss for a company to start taking computer security seriously (Taylor, 2008, p144). The same may possibly be the same for phishing awareness.

A further suggestion is that thought does not even come into play. Riegelsberger and Sasse (2008) citing Goffman (1959) explain that once a person is in a situation they recognise, they perform in a ritualised fashion, thanks to the power of internalised norms. They perceive themselves to be interacting with a brand they know and trust and go about doing what they always do in that situation.

There has been a considerable amount of research into these factors – some important studies are discussed below.

2.2.1.1 Major studies into responses to phishing

Downs, Holbrook and Cranor (2007) examined behavioural responses to phishing risk, using role play. They state:

“If we know what factors cause people to fall for phish we gain insights into what specific things to educate people about and to whom to target education.” (Downs, Holbrook, and Cranor, 2007).

Participants were asked to decide how to respond to emails containing links and were also questioned on their interpretation of URLs, their knowledge of security icons and terminology, past web experiences and how they would rate various negative outcomes from computer fraud. Their main findings were that knowing more about web environments and the ability to understand URLs in particular meant lower susceptibility to phishing attacks. Understanding what was happening seemed more effective than simply receiving a warning that the user might not understand and simply wish to dismiss so they could carry on with their primary task. They also found that participants were not greatly motivated to protect their financial information, perhaps on the assumption that their bank would carry the consequences. Behaviour was not affected by the perceived severity of the risk. In this particular study, which had US participants, fear of having their social security number stolen was greater than of having their credit card details stolen (Downs, Holbrook, and Crainor, 2007). They concluded:

“protections against phishing might not gain much traction from warnings about how easy it would be for a phisher to steal one’s card.” (Downs, Holbrook, and Crainor, 2007).

The study by Downs, Holbrook, and Crainor (2007) involved only participants who already had an interest in cyber security, which might have skewed the results. In addition while the authors claimed that role play produced a better approximation of real world behaviour than self reported behaviour (Downs, Holbrook, and Crainor, 2007), it still lacks the pressures of real world behaviour where primary task demands intrude and may affect behaviour. The authors also admitted that role played situations lack direct consequences to the participants.

The theories discussed earlier, Rational Choice Theory, the Technology Acceptance Model, the Unified Theory and Lazy User Theory, may apply both to real life security behaviours and to behaviours within trials and studies. Schechter, Dhamija, Osment and Fischer (2007) tackled the question of role play in their study and found that role playing had a significant negative effect on security vigilance. They compared the reactions of role playing participants to participants using their own security information to three different types of attack indicator – missing HTTPS indicators, missing site authentication images and a warning screen and found that those participants who were role playing were considerably less careful with security than those using their own credentials. They also questioned whether security conscious individuals would consent to take part in a security focused trial in the first place – even trials where the security focus is obscured cannot avoid disclosing a security focus in ethics permissions forms that participants have to sign (Schechter, Rachna, Ozment, and Fischer, 2007).

They also found that participants entered their passwords although HTTPS indicators and site authentication images were missing. 100% of participants disregarded the missing HTTPS indicator and 97% disregarded the missing site authentication image. They also suggested that the presence of site authentication images (such as the SiteKey system), which can theoretically be spoofed by man-in-the-middle attackers, causes users to disregard other security indicators (Schechter, Rachna, Ozment, and Fischer, 2007).

Pattinson, Jerram, Parsons, McCormac and Butavicius (2012) carried out a larger role play based study with two groups, one informed that the study concerned emails and the other phishing. This was intended to control for and measure the subject expectancy effect. There were 117 student participants from non-computing courses and 50 emails. The study also included demographic questions, a personality test and a cognitive impulsivity measure. Participants were asked how they would deal with each email – keep and follow up, keep, delete or delete and block (Pattinson, Jerram, Parsons, McCormac, and Butavicius, 2012).

Participants who had been informed the study concerned phishing managed phishing emails better than the other group. Those with more computing experience also managed phishing emails better than those with less experience but only if they knew the study concerned phishing. In terms of personality traits, those who were more extraverted and more open also managed phishing emails better. Those with lower cognitive impulsivity managed phishing emails better but only if they were not informed about the phishing aspect – if they were informed there was no significant difference. Overall, genuine emails were managed better than phishing emails, whether or not the participants were informed of the phishing nature of the trial. Because informed participants were significantly better at managing phishing emails, the authors recommended that users should be regularly reminded about the dangers of phishing (Pattinson, Jerram, Parsons, McCormac, and Butavicius, 2012).

Kumaraguru, Rhee et al. (2007) also used the same impulsivity measure – the Cognitive Reflection Test (CRT), which is designed to measure whether people jump to immediate intuitive but incorrect answers or stop and reflect (Frederick, 2005). In fact a high cognitive reflection rating is also associated, perhaps counterintuitively, with a higher willingness to take risks, but only concerning gains. With respect to loss, people with high CRT scores are less likely to take risks (Frederick, 2005). Pattinson et al. (2012) states that Kumaraguru, Rhee, Sheng, Hasan, Acquisti, Cranor and Hong (2007) found results that agreed with their own. However a closer reading of Kumaraguru, Rhee et al. (2007) shows that they found that while there was no significant difference between people with high and low CRT scores as to whether they were likely to click on links in phishing emails from organisations with which they had accounts, people with high CRT scores were more likely to click on links in phishing emails from organisations with which they did not have accounts, as a result of their higher willingness to take risks. The authors did caution though that although people with high CRT scores might take the risk because of curiosity, that did not imply they would go on to enter personal information into a phishing site (something that was not examined in the study) (Kumaraguru, Rhee, et al., 2007).

This therefore suggests conflicting findings between the two studies rather than corresponding findings. It would therefore be interesting to investigate, given the findings about cognitive impulsivity, whether susceptibility to phishing correlates with other poor banking habits like incurring unauthorised overdrafts.

In an earlier study Downs, Holbrook, and Crainor (2006) found that while participants in a study about dealing with possibly fraudulent emails, looked out for and noticed security indicators, they did not necessarily interpret them correctly. In judging whether to react to emails, they focused more on the text content of the email or on familiarity with similar scams than on links and URLs. They also had trouble dealing with pop-up messages, especially those that did not require action.

They quote one study participant as worrying that deleting a possibly fraudulent email was “not so nice on my part” (Downs, Holbrook, and Crainor, 2006), i.e. displaying concern about what the sender of the email thought of her or about social norms of politeness and how they conflict with security (Pieters and Coles-Kemp, 2011).

In contrast to their 2007 study (Downs, Holbrook, and Crainor, 2007) Downs et al. concluded that awareness about phishing and security cues was not enough to protect against phishing and suggested that measures that shifted users away from being able to spot scams towards always responding cautiously to emails would be a more effective strategy i.e. following specific positive routines rather exercising passive awareness (Downs, Holbrook, and Crainor, 2006).

Social context i.e. who appears to have sent the email can be significant. Jagatic, Johnson, Jakobsson and Menczer (2007) carried out an experiment where students at Indiana University received emails that appeared to come from social contacts. Their study suggested that users were over four times more likely to become phishing victims if the message appeared to come from someone they knew. Email recipients were not aware of the study so the study came close to reproducing real life. As a result complaints were received about lack of consent and ethical issues, a problem in reproducing real life attacks.

Dhamija, Tygar and Hearst (2006) analysed a set of phishing attacks, developing three hypotheses about how they trick users. These were that users lacked security system and computing knowledge, that phishing sites were visually deceptive and that user attention was focused on issues other than security. The hypotheses were then tested by displaying websites to users and asking them to state which were fraudulent and which weren't. Their third hypothesis in particular was interesting – security, they believed, was often a secondary goal for the user, after whatever task focused activity they were involved in. They also hypothesised that it was hard for users to reliably notice the absence of something, in this case security indicators (Dhamija, Tygar, and Hearst, 2006).

Wu, Miller and Garfinkel (2006) also address this distinction between security as a primary and secondary task, stating that studies where security is the primary goal cause participants to pay more attention and take precautions they might not take in real life.

Dhamija, Tygar and Hearst (2006) found in their study that anti-phishing browsing cues were not effective and that 23% of study participants looked at neither the address bar, nor status bar nor security indicators. Study participants made mistakes in identifying fraudulent sites in the study 40% of the time. Sixty eight percent of participants ignored pop up warnings. Some well designed phishing sites fooled 90% of participants. They also found no correlation between ability to detect phishing sites and sex, age, education, hours spent on a computer and previous use of the browser, operating system or website. They concluded that standard security indicators were not effective for many users and that alternative approaches were necessary (Dhamija, Tygar, and Hearst, 2006).

Part of their third hypothesis, concerning lack of attention, was not fully tested – the study involved the users knowing that they were looking out for fake sites, i.e. this was their primary task. They did nevertheless verify the hypotheses concerning lack of knowledge and visual deception and they also discovered that some users are simply unaware of web fraud and others have misconceptions about security. One particular misconception was that pages lacking images and links (for example bank login pages) were in fact less trust worthy than those with many visual elements (Dhamija, Tygar, and Hearst, 2006). However their study was limited in scope with only 22 participants and 20 sites.

Furnell too (2007) in a study involving 179 participants attempting to categorise 20 emails as phishing or non-phishing found that participants found that the presence of logos, banners, trademarks etc convinced them that the message was genuine. Technical cues on the other hand were often misinterpreted. Participants also failed to recall or realise that legitimate organisations do not ask customers to 'verify' or 'confirm' details via email (Furnell, 2007).

In the face of this, suggestions like that of Yu et al (2008) that:

“...users must also educate themselves about the security software, updates, loop holes etc, so that they can suspect phishing in certain scenarios.” (Yu, Nargundkar, and Tiruthani, 2008)

seems optimistic, especially in the case of non-computer expert users.

2.2.2 Industry approaches to tackling phishing

So what is being done to help users identify phishing sites and emails?

Wilson and Argles (2011), in their survey of anti-phishing measures, state that there are three ways of tackling phishing – technical responses, educational approaches and legislative programmes. The topic of legislation is outwith the scope of this paper as the primary focus is user education but there will be some discussion of technical responses where they overlap with education and user experience.

2.2.2.1 Technical responses

Wilson and Argles (2011) also state that there are three main technical solutions to phishing. Blacklisting can be done manually or automatically with the former less prone to false positives. The short lifespan of some phishing sites can also impact accuracy because of the time lag involved in identifying and blacklisting sites. Heuristic techniques, which look out for phishing-like behaviour, also score highly for false positives and are relatively easy for phishers to bypass. Page similarity detection can be computationally demanding and has low accuracy rates.

While the ideal might appear to be for technical protection to be a background process, with no user involvement, in practice the number of false positives makes that impractical.

In addition that approach runs counter to the idea that security is primarily a social issue rather than a technical issue (Taylor, 2008, p141). This is an idea that is often applied to corporate IT security – Taylor cites early research from Bikson and Gutek (1984) suggesting that 90% of system failures were a result of human/social issues rather than technology – but it can apply to users in the wider environment too. Phishing is also a threat with a human rather than a technological cause (Taylor, 2008, p143).

Instead these three technological approaches are often used in toolbars which alert the user to potential phishing dangers. However users may find it hard to interpret or act on the information provided by the toolbar (Kumaraguru, Sheng, Acquisti, Cranor, and Hong, 2007) and may simply ignore them (Downs, Holbrook, and Crainor, 2007).

Wilson and Argles (2011) suggest that more effective would be a solution combining all these techniques but states that none have been identified as yet. They say, though, that:

“Phishing scams take advantage of human vulnerabilities rather than technical ones.” (Wilson and Argles, 2011).

Their recommendation is a combined solution of anti-phishing legislation on an international scale, increasing user awareness and improving existing technical solutions (Wilson and Argles, 2011).

Wu, Miller and Garfinkel (2006) evaluated toolbars and found them ineffective. They simulated 3 different types of toolbar and five different phishing attacks and found that users failed to heed warnings given in the toolbars. The main indicator users relied on was look and feel of the website; dangerous, as discussed, if the phisher is relying on a man-in-the-middle attack. Users also made rationalisations about the security of the site, focused on the primary task and did not notice the toolbar

They also pointed out that many genuine website owners have poor security practices, using inconsistent domain names, not using SSL and making their outsourcing relationships visible

to the user, increasing user confusion (Wu, Miller, and Garfinkel, 2006). In the example shown below, the email is ostensibly from Lulu.com but is sent from and links to bronto.com, an email marketing provider.



Figure 2 An example of an email where it is unclear whether it is a phishing email or a genuine email from an outsourced email address

Wu et al.'s pilot study showed that the presence of a printed tutorial on using the toolbar information greatly reduced the rate at which participants were fooled by spoof sites. In the actual study, the tutorial was introduced halfway through the exercise, after half of the emails had been dealt with (Wu, Miller, and Garfinkel, 2006).

Their recommendations were that active interruptions like popups, timed to interrupt dangerous actions, were more effective than toolbars. Warnings should also include an alternative path rather than just a suggestion to not to continue and should be designed so that the user cannot ignore them (Wu, Miller, and Garfinkel, 2006).

Research carried out by Egelman, Cranor and Hong (2008) into the comparative effectiveness of active and passive phishing warnings, using a warning analysis model from the warnings sciences, showed that users in their survey were more likely to heed active warnings than passive ones. Firefox's active warning was significantly more effective than Internet Explorer's, suggesting that there are differences between different browsers in how they protect users. It also showed that even when users heeded browser warnings about fraudulent sites, they still believed that the phishing emails sent to them containing links to those sites were genuine, something that Egelman et al said,

“raises grave concerns about Internet users' susceptibility to phishing.” (Egelman, Cranor, and Hong, 2008).

When users did recognise warnings, they often failed to read them, leading the authors to recommend that serious warnings should be designed to look different to other types of browser warning (Egelman, Cranor, and Hong, 2008). Some of the participants who ignored

warnings did so because they trusted the look and feel of the phishing website or the brand it was purporting to represent. The authors therefore recommended that phishing warnings should distort the look and feel of the site.

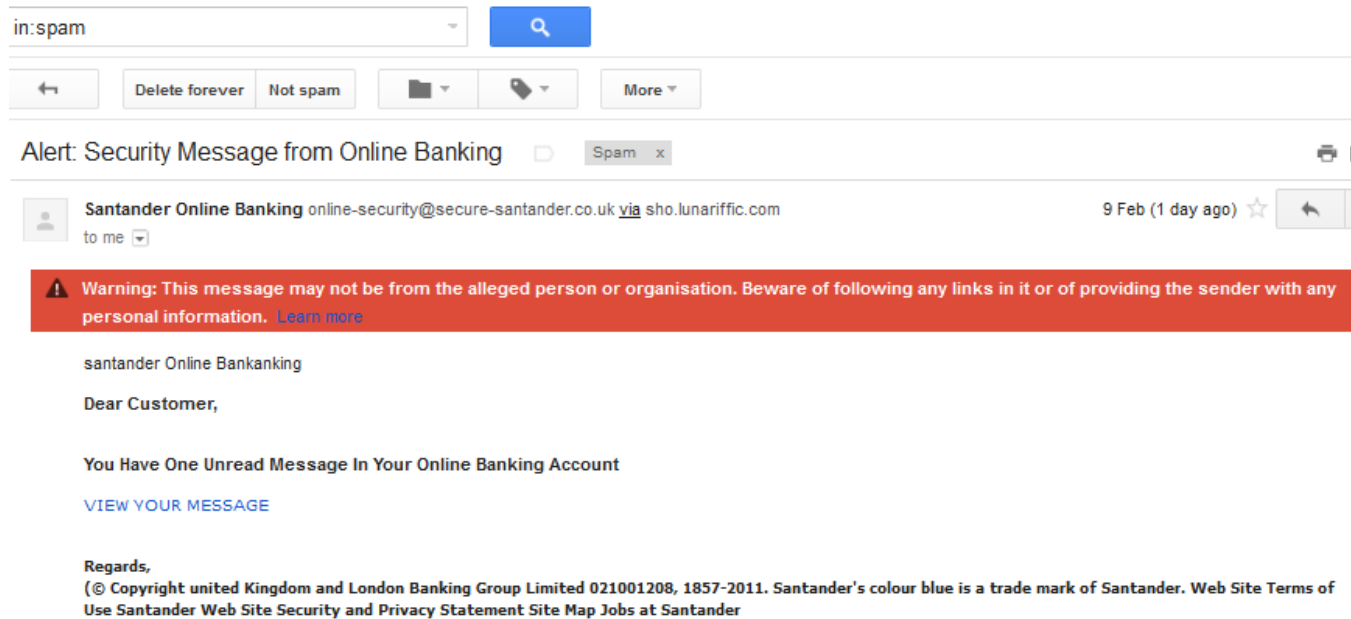


Figure 3 A phishing warning from Virgin Media

Their other recommendations were that effective phishing indicators had to interrupt the primary task of the user, i.e. be active. They had to provide clear choices about how to proceed and those choices should not include the option to ignore the warning without actively choosing to ignore it (Egelman, Cranor, and Hong, 2008).

However Dhamija et al (2006) found that when presented with a warning for a self signed certificate, users failed to read the warning and immediately selected OK (Dhamija, Tygar, and Hearst, 2006).

Another approach is to improve user interface guidelines for site security, adding consistency across different sites (Dhamija and Dussault, 2008). At present, security indicators such as the lock icon can be confusing or even misleading (Grover, Berghel, and Cobb, 2011).

Ed: Roessler and Saldhana (2010) proposes a number of measures including ensuring that identity information about the web site being interacted with is available as part of the primary or secondary user interface and using information in the identity signal that is from validated certificates, not from untrusted sources and that must be human readable. Caution messages must be designed to interrupt the user's primary task so that they can't be ignored, must contain enough information and must contain the option of discontinuing the task rather than just accepting the warning and continuing.

This is a form of choice architecture or nudge so that users are not placed in a situation where they might make choices that are unhelpful to themselves in terms of reducing security (Pieters and Coles-Kemp, 2011).

Passive security indicators (such as the padlock sign) should also not be displayed in a location that allows for mimicking using favicons (ed: Roessler and Saldhana, 2010).

Something else which might be usefully eliminated is banks contradicting their own advice about avoiding phishing. For instance Anderson describes a UK bank sending out marketing emails from URLs not registered to the bank and advising customers who enquired that it was a phishing email when in fact it was not (Anderson, 2007).

Many of these recommendations ensure that users cannot ignore security indicators and warnings but some still require a degree of awareness and knowledge about security on the part of the user. Indeed they warn that:

“users will habituate to over-frequent warnings, weakening the impact of the messages and their ability to effectively interrupt the user’s task flow.” (ed: Roessler and Saldhana, 2010).

In addition, as previously mentioned, some security indicators can be spoofed.

Rather than relying on the user to observe warnings or negative signs that the site visited is not genuine, an alternative approach is to use a positive sign that the site visited is genuine. Again though, this might be easy to spoof.

Iliev and Sun (2010) propose a personalised authentication process that requires the user to recognise a personalised avatar phrase pair from a range of pairs after entering user name and before they are able to enter their password. This differs from the Sitekey system used by Bank of America where the user passively views an avatar they recognise as their own as a means of mutual authentication but does not have to interact with it as part of the process. Hence this overcomes the problem of users who may or may not notice whether the mutual authentication avatar is present or not (Iliev and Sun, 2010) or who proceed regardless of its presence (Schechter, Rachna, Ozment, and Fischer, 2007). The user must also select the avatar and phrase from a range of possible avatars, overcoming the problem of an attacker in possession of a username thus being able to access the avatar. This does not however appear to overcome man in the middle attacks where the user accesses the genuine site through a phisher proxy, for example as demonstrated by Soghoian and Jakobsson (2007).

A further approach which relies on technology rather than user awareness or judgment involves introducing additional devices into transactions. For example mobile devices may be used to encrypt passwords before the user can enter them into the authentication page of the website they are trying to access, making the password useless to the phisher or to any keylogging software running on the PC (Mannan and van Oorschot, 2010). They can also be used to perform mutual authentication for the user (Parno, Kuo, and Perrig, 2006), although this may be subject to session hijacking or attacks on the connection between the PC and phone (Mannan and van Oorschot, 2010). Alternatively the session can be managed entirely from peripheral devices, bypassing any malware on the PC and allowing the device to carry out the mutual authentication, for example the Zone Trusted Information Channel (Weigold and Hiltgen, 2011) or the standardised Finread card reader, used in association with a smart card (Finread, 2009). This still depends though on the user using those devices and not being deceived by phishing messages stating that security is being upgraded.

2.2.2.2 Training and educational responses

User training and education may be offered in the shape of online information about phishing, offered by government, businesses or not for profit organisations (Kumaraguru, Sheng, Acquisti, Cranor, and Hong, 2007). Users can also take tests or play games and education can also be carried out in a classroom setting, although this seems inappropriate outside university or work settings.

Research suggests that when it is carried out, some anti-phishing education can be effective, for example as discussed previously in Wu, Miller and Garfinkel's pilot study (2006).

Kumaraguru, et al. (2009) discuss deception theory, citing a model adapted by Grazioli (2004) to detect deception on the Internet. It incorporates discrepancies between what is seen and what is expected, hypotheses about what appears to be happening, testing those hypotheses and the ultimate decision about what to do. Successful anti-phishing education therefore has to train users to form and test better hypotheses (Kumaraguru, et al., 2009).

Based on this Kumaraguru, et al. (2009) showed that after receiving training with the PhishGuru training tool, which is embedded into mock phishing emails, study participants were, even 28 days after training, less likely to click on a phishing link. Receiving the training twice increased its effectiveness. A previous evaluation of PhishGuru showed that it was more effective than security notices and than non-embedded training (Kumaraguru, Rhee et al., 2007). Unlike Dhamija et al. (2006) they did find a correlation with age – younger participants were more likely to be deceived (Kumaraguru, et al., 2009).

Their approach which delivered the training within fake phishing emails, could, they suggested, be used over time to educate users about new phishing threats. However because they were able to show retention, overly frequent retraining, which might cause habituation, could be avoided (Kumaraguru, et al., 2009).

They also cite researchers at West Point (2005) and at the New York State Office of Cybersecurity (2005) who tested users who had received anti-phishing training and found it improved their ability to spot phishing emails (Kumaraguru, et al., 2009). According to Wu, Miller and Garfinkel (2006) both of these studies involved employees/cadets receiving phishing emails from within the organisation – 80% of cadets at West Point were fooled by an email from a senior against 15% at New York State, which might suggest attitudes to authority may affect how recipients respond to phishing.

Prior to the 2009 study, Kumaraguru, Sheng, Acquisti, Cranor, and Hong (2007) examined the effectiveness of existing online anti-phishing training materials. Materials tested were from Microsoft, US Federal Trade Commission, MySecureCyberspace and eBay, selected from 24 types of material. They found that participants were better able to identify fraudulent websites after training. They also found that the primary cause of errors after training was confusion over interpreting long URLs (Kumaraguru, Sheng, Acquisti, Cranor, and Hong, 2007). They recommended that effective training should include information about URLs and domain names, as well as teaching that it is a poor strategy to focus on the design and content of websites for cues to authenticity. Indeed, where phishing is carried out using a man-in-the-middle attack on a genuine site, then site content is of no help in detecting phishing (Wu, Miller, and Garfinkel, 2006).

It seems probable though that these training interventions were carried out within a defined and controlled environment – at work or at university where there is some motivation to comply and follow the training. It is possible that take-up of training would be lower if offered by a bank or ISP to home users.

Indeed whether or not anti-phishing education can be effective when used, often it is not used. Wilson and Argles (2011) suggest that this is because it is not related to familiar scenarios that users can understand and themselves relate to and conclude that it is of "paramount importance" to find more effective ways of educating large numbers of users (Wilson and Argles, 2011). Kumaraguru, et al. (2009) too state that learning materials are

most effective when related to the real world. Nonetheless users generally manage to successfully navigate other online experiences that do not have direct real life parallels for them, such as fantasy warfare games.

Writing about security training in a corporate context, Parsons, McCormac, Butavicius and Ferguson (2010) write that in order to be successful training has to be:

“personal, meaningful and contextualised, as evidence suggests that programs are more likely to be successful if the users feel that the subject matter and issues are relevant to their own needs.” (Parsons, McCormac, Butavicius, and Ferguson, 2010).

There is no reason to suppose that this is different outwith the corporate context, yet anti-phishing education in general appears in no way personalised.

Parsons et al. (2010) also quote BF Skinner’s work ‘Science and Human Behaviour’ from 1953, which stated that positive reinforcement, in rewarding desired behaviours, was effective in producing the desired outcome. The only positive reward for learning to avoid phishing is avoiding phishing which is effectively staying at neutral rather than receiving any form of positive reinforcement. Virtue may be its own reward but might positive reinforcement be better? However Skinner’s approach, behaviourism, is viewed as somewhat outdated in the workplace (Kohn, 1998) so it is interesting that this is cited uncritically in this context.

Others argue that user training is not effective. Kumaraguru, Sheng et al. (2007) cite web usability expert Nielsen (2004) in arguing that user education about security does not work. Instead, Nielsen stated that technological changes were necessary to protect users because user education was unrealistic in its demands, ineffectual, wrongly supposed that humans were easier to change than technology, and hindered full use of the Internet (Nielsen, 2004). Schneier (2006) in a point/counterpoint with Ranum (2006) argues that attempting to educate users is “largely futile” and would be better replaced by improving technology (Schneier, 2006). Ranum argues implicitly for a behavioural approach, saying that only “pain and humiliation” work as learning tools and that people should be left to learn from their mistakes (Ranum, 2006).

Anandpara, Dingman, Jakobsson, Liu, and Roinestad (2007), asking why, given the amount of anti-phishing education available, phishing continues to claim victims, carried out an experiment, which saw test subjects presented with and asked to identify examples of phishing messages before and after reading anti-phishing education. They concluded that phishing tests measure fear rather than ability to spot phishing messages and that anti-phishing education increased this fear about phishing rather than the ability to recognise it.

They also suggested that anti-phishing tests in particular remove natural context and introduce an artificial context that impacts the test taker’s judgment, making them more likely to identify positives whether they are real or false positives (Anandpara, Dingman, Jakobsson, Liu, and Roinestad, 2007). This point is made by them specifically about anti-phishing tests but may also apply to any experimental or test situation, for example the experiments organised by Kumaraguru et al. (2009) where the users were not aware that they were being assessed for recognising phishing but knew they were being observed, which may have affected their vigilance. However Anandpara et al. (2007), in their experiment presented their subjects with a low number of phishing examples, a total of only five, which might have affected the significance of their results.

Sheng, Kumaraguru, Acquisti, Cranor, and Hong, (2009) on the basis of 31 interviews with phishing experts in 2008 and 2009, which found mixed opinions on the importance of

education in fighting phishing, recommended that academic researchers and industry needed to continue research into making education fun, engaging and up to date in order to make users more likely to engage with it (Sheng, Kumaraguru, Acquisti, Cranor, and Hong, 2009). Amongst other recommendations about topics including law enforcement, governance and technology, they also advised that social networking sites could play a valuable educational role and that education should help users to make trust decisions when they were faced with technology solutions to phishing that required choices (Sheng, Kumaraguru, Acquisti, Cranor, and Hong, 2009).

2.2.3 Conclusions about phishing

It appears then that a major part of the problem with phishing is that users do not experience security as a primary task while online (Dhamija, Tygar, and Hearst, 2006) (Wu, Miller, and Garfinkel, 2006). There is also a suggestion that some do not especially view keeping their financial information safe as important either (Downs, Holbrook, and Crainor, 2007).

Toolbars and warnings appear to have limited impact (Kumaraguru, Sheng, Acquisti, Cranor, and Hong, 2007), (Wu, Miller, and Garfinkel, 2006), (Egelman, Cranor, and Hong, 2008) and users mistakenly focus on site and email content as guidelines (Downs, Holbrook, and Crainor, 2006), (Dhamija, Tygar, and Hearst, 2006), (Furnell, 2007).

There also seems to be a lack of clear consensus about what can reduce vulnerability to phishing amongst online users.

Downs, Holbrook and Crainor (2006) found that more knowledge about phishing and security cues did not protect against phishing whereas a year later the same authors (Downs, Holbrook, and Crainor, 2007) found that it did. The later study did involve people with an existing interest in security, which may have affected how likely they were to retain and act on that knowledge.

Opinions vary too on the efficacy and worth of user education about phishing (Kumaraguru, Sheng, Acquisti, Cranor, and Hong, 2007), (Wilson and Argles, 2011), (Anandpara, Dingman, Jakobsson, Liu, and Roinestad, 2007), (Schneier, 2006). There are also disagreements on what makes education effective (Parsons, McCormac, Butavicius, and Ferguson, 2010), (Ranum, 2006).

However the literature does suggest that aspects of identity and personality may affect how vulnerable users are to phishing, although again there are disagreements for example Pattinson et al.'s findings (2012) about impulsiveness and personality types versus Kumaraguru, Rhee et al.'s findings (2007) about impulsiveness and the research carried out by West Point, cited by Kumaraguru, et al. (2009) which raises questions about how attitudes to authority and social context affect how likely a person is to follow instructions in a phishing communication. Downs, Holbrook and Crainor (2006) touch peripherally on the question of how the user's reaction to phishing may be impacted by how they view their own persona.

This raises a number of questions in relation to protecting against phishing attacks aimed at online banking users, primarily around the questions of attitudes to security risk online and offline, to what extent they really care about security, types of behaviour online and offline, self concepts and how anti-phishing education can be tailored to how people behave online.

These questions will form the basis for the research to be carried out during this project. However they can be further clarified by examining how some of the theory concerning online identity and its relationship to broader identity is currently understood.

2.3 Identity

Identity is defined by the Oxford English Dictionary as “the fact of being who or what a person or thing is” and also as “the characteristics determining who or what a person or thing is”. The definition, particularly as applied to online identity or digital identity, is somewhat nebulous and ‘identity’ is often confused with ‘identifier’ which the OED has as “a person or thing that identifies someone or something”. Alpar, Hoepman, and Siljee (2011) for example say that:

“Identities are therefore only valid within a specific scope.” (Alpar, Hoepman, and Siljee, 2011)

where scope refers to an environment such as work or family. In this particular document, the scope covers online transactions in general and online banking in particular.

2.3.1 A summary of relevant thought about identity in general

Much of the thought about online identity and behaviour appears to derive from work on the nature of identity in modern society in general. Clearly there are fundamental differences between the online and non-online worlds that impact identity and its expression and make anonymity and disguise easier, not least the absence both of physical cues from the corporeal self and a physical setting. Nonetheless the user online is essentially the same person as the user offline and hence considering non-online-specific thought is useful. Castells for example says that:

“Identity is people’s source of meaning and experience.” (Castells, 1997, p6).

“People increasingly organise their meaning, not around what they do but on the basis of what they are, or believe they are.” (Castells, 2000, p3).

He distinguishes between identity and roles, where roles may cover being a mother or a union member or a smoker whereas identity is internalised and used to create meaning. Clearly there may be some overlap as some roles, such as parenthood, may be used for self-definition. Identity may be individual, which is close to the definition used by Erikson who believed that individuals form a coherent sense of identity, in general during adolescence (Amichai-Hamburger, 2007, p193). Alternatively identity may be collective, where it approaches social identity, being based on groups and affiliations and either supports or opposes societal institutions. Therefore, in that it has any connection with collective identity, online identity most closely seems to approach project identity (Castells, 1997, p10) where there is some transformational, cause based aspect, being religion or ideology or some idealistic cause like file sharing or privacy. However that only really seems relevant to online activities devoted to pursuing certain causes and not to activities such as online banking or Facebook, where the user views themselves as an individual.

The act of trying to manage impressions made online corresponds to behaviours in real life around face-to-face interactions. Goffman used the metaphor of a dramatic performance to explain social interaction (Goffman, 1959, p28), where people use props, lines, skills and audiences to create an identity in the eyes of others during interactions. This involves intentional communication (which he calls ‘giving’) and unintentional (‘giving off’). The concept of ‘face’, maintaining and saving it, is also involved, what Goffman describes as:

“the positive social value a person effectively claims for himself by the line others assume he has taken during a particular contact. Face is an image of self delineated in terms of approved social attributes...” (Goffman, 1965, p5).

A modern way of describing this is personal brand management (Gross, 2010, p122). Online this can be reflected in the use of identifiers a person chooses (Gross, 2010, p2).

Those most concerned with managing the impression they present are known as high self monitors and adjust their behaviour according to social cues and reactions they receive. Low self monitors are less responsive and more likely to behave or appear in a way that reflects their internal state.

Goffman in Frame Analysis, his discussion of the organisation of experience (1974), also states that people inhabit a range of different worlds or realities. They understand events within these realities through frameworks, which form a context. In addition, they may not see the reality of what is going – what they see as real may be a deception, a performance or a joke (Goffman, 1974, p10). However ‘keying’ transfers what appears to be one thing into another, for example fighting into play fighting (Goffman, 1974, p45).

2.3.2 Online identity

Discussion of the nature of online identity has tended to focus on topics such as how people segment or disguise real life identities in online environments such as games or chatrooms, showing flexibility and multiplicity, and hence on behaviour in online social settings (Baym, 2010, p106). Baym writes about how Sherry Turkle describes windows on the screen as a metaphor for different aspects of the self as a “multiple, distributed system” (Turkle, 1996). Turkle talks about “eroding boundaries” between the “unitary and the multiple self” (Turkle, 1996, p10). While in the real world people see themselves as unitary, intentional and take responsibility for their actions, online they appear fragmented, multiple and closer to the decentred concepts espoused by thinkers such as Lacan and Foucault (Turkle, 1996, p15).

Early work was largely concerned with identity in anonymous environments (Zhao, Grasmuck, and Martin, 2008) whereas more recent work has focused on non-anonymous or pseudonymous settings such as Facebook or dating sites.

The rise of gaming may be responsible for a move away from the early view that online selves always reflected the offline self. Castells represents this early view (Castells, 2000, p390) for example in quoting a much earlier position from Baym in which she said:

“most users of CMC [computer mediated communication] create on-line selves consistent with their off-line entities.” (Baym, The Emergence of On-line Community, 1998).

Clearly this is not the case in gaming but in social media environments, the digital self generally somewhat reflects the offline self, although there may be enhancements. This similarity increases when it comes to activities online that closely reflect the offline world such as work, banking, e-citizen type activities. According to Zhao, relationships online where there is also an offline component are called ‘anchored relationships’ (Zhao, 2006). Online identities that are tethered to offline ones could perhaps be viewed as anchored identities.

On the other hand, the online world forms a reality separate from the offline world, in other words one of the multiple realities Goffman (1974, p3, discussing Schutz (1945)) says that people experience. It is a different framework, something brought home by the way the monitor provides a frame for an entry into that world. This reinforces the question of whether people behave differently online to offline, something that may potentially be born out by differing attitudes to security in each world.

In addition, in many of these online environments, the digital or online identity of the person is interacting with digital objects or entities that do not necessarily correspond exactly with real life objects, for example a digital object, like a sword, in an online game (Baym, 2010, p107) or avatars of other disguised entities.

At the same time, users are also interacting with the computer itself. McLoughlin describes the effect of computer mediation as making work related activities more definitive and less easy to criticise and quotes Zuboff's assertion 'the computer can't be wrong' (Zuboff, 1988) (McLoughlin, 1999, p108). This could potentially affect the user's attitude to believing phishing emails, although it is questionable whether 24 years on from that statement, with the advantage of greater familiarity with computers, people still believe in their infallibility.

Online, as in real life, there is an aspect of trying to manage impressions one gives of oneself to others (Baym, 2010, p108) by creating and developing a persona. Social identity is important online too, with group affiliations and links to others adding to the online persona created. Inferences about one's identity can be made from the online company one keeps (Baym, 2010, p112).

2.3.3 Implications for understanding identity within online banking

There appears to be a tendency amongst some technologists to view users as a single entity, ignoring differences in personality and identity (Amichai-Hamburger, 2007, p187). Here, the user may consider their identity to be as an individual but in return they are treated in part by the system or by technologists as part of a collective identity, in the Castells sense discussed earlier i.e. a customer, or even less individually as an object.

Yet as expressed by Baym and by Turkle, online identities may be multiple. The professional wiki participant is the same person as the game player and the online dater and the online banking customer but the external representations of online identity are different (Gross, 2010, p122). This corresponds in part with Castells' definition of roles in the real world. It also corresponds to roles in a security sense in that the entity's identity within the system may define what resources it has access to.

In other words, online identity is not absolute but instead describes "an entity... within a specific scope." (Alpar, Hoepman, and Siljee, 2011). In the scope of a particular online bank, an identity describes a customer with a set of associated characteristics (bank account number for example) and identifier (their login name or number). That same entity has different identities elsewhere online and more importantly each identity within the scope is different.

(In practical terms this also imposes a considerable cognitive load on the user, with the cumbersome burden of remembering multiple user accounts and sets of login details (Alpar, Hoepman, and Siljee, 2011), thus potentially increasing the burden that may lead the user to falling for phishing.)

The relationship appears to be many to one – many identities in different scopes map onto one real life person. In practice, it may be many to many – a person may give their partner access to their online bank account or eBay account – to the bank, or eBay though, the entity appears to be one person.

Furthermore, those offline individuals are different from each other in a multitude of ways. At the most fundamental level, differences such as age and gender may have an effect on their online selves. Turkle (1996, p77) states that children (at the time of writing) who grew up with

computers i.e. people born from the early to mid 1980s onwards have fundamentally different attitudes to computers compared to older people. It seems reasonable to assume that that difference could be extended even further by the coming of the Internet. For those children computers are a psychological entity in their own right and they may view them as “alive” (Turkle, 1996, p81-82).

These sorts of differences are widely recognised in most disciplines, for example marketing or design where personas, which are ‘made up’ people or user profiles, created by studying actual user behaviour and classifying it along demographic or behavioural lines (Cooper and Evans, 2006), are used for creating or promoting products and services in a more targeted way. A similar behavioural approach is used to present personalised advertising online by Google. Turkle also discusses personas in the context of MUDs (or MMORPGs) where she refers to them as a mask (Turkle, 1996, p182).

Similarly, some examinations of identity and Internet behaviour may view the Internet as monolithic (Amichai-Hamburger, 2007, p187), which is clearly not the case, even in the simple comparison of Facebook with a banking site. This in turn reinforces how users are not monolithic things.

Indeed earlier studies of behaviour and identity on the Internet found that behaviour differed between anonymous settings such as MUDs/MMORPGs and less anonymous settings such as dating sites, where there was the anticipation that a real life meeting might result (Ellison, Heino and Gibbs, 2006). Nonetheless the idea of creating embellished personas online seems irrelevant to interacting with an online bank where avatars are not in use and there is no facility for individualisation or displaying personality except perhaps in password choice. Identity is not disguised. The figures being dealt with correspond with real money or assets. Indeed it seems probable that the user of an online banking service views themselves as playing a ‘role’ in the Castells sense of role rather than as adopting an identity as an online banking customer. There is no option of managed anonymity or pseudonymity – the expectation is that the user interacts with the bank in their true identity. In return, there is an expectation that the online banking site too is a true representation of the bank. There is a lack of interaction with other users, meaning that the aspect of performance and managing impressions is lacking, except in the communication with the bank. But even that is lacking – there is nothing of the experience of visiting a physical bank branch where the customer recognises and interacts with tellers.

On the other hand if the user continues to understand online interaction as a performance, as described by Goffman, then not responding to a phishing email, where the visual presentation and format of the email is the front or framework for the performance and the written content the dramatisation, could potentially be viewed by the user as a performance disruption (Goffman, 1959, p23).

Indeed, this does raise the question of whether in responding to phishing emails, online banking users consider what the author of the email, supposedly a banking executive, actually a phisher, might think of them, whether they are concerned about being seen as foolish for not reacting to an alarm.

In the offline world as in the online, the motivation for impression management is driven by wanting to achieve certain goals (Chester and Bretherton, 2007, p225). If the user has the desire to represent themselves as a responsible manager of their money then responding to a phishing email rather than ignoring what might be a genuine warning does not seem irrational.

So while there appears a seeming assumption that Internet banking users react in a uniform way to phishing activities, perhaps because of the lack of the overt display of identity on social networking sites, the studies discussed show that this is not true.

On that basis, one might expect that the use of avatars as a mutual authentication tool, for example the Sitekey system, by adding a degree of individualisation and recognition to the interaction, would greatly enhance the certainty of the user that they are interacting with the genuine bank. Yet the study from Schechter, Dhamija, Osment and Fischer (2007) suggested that that is not the case.

This also touches an issue discussed by Alpar, Hoepman, and Siljee (2011) – the distinction between membership of a resource and ownership of a resource. In the latter case, which corresponds to the online banking scenario, as opposed to the former which might for example correspond to an online subscription to a newspaper, the trust relationships are not just about the user entity authenticating themselves and their identity to the system. The onus is also on the system owner, to whom the user has entrusted their money, to authenticate themselves to the user (Alpar, Hoepman, and Siljee, 2011). Placing the burden on the user of having to recognise and understand security cues in order to know that they are on a genuine site as opposed to a phishing site could be seen as abrogating that responsibility on the part of the system owner. Is it then the responsibility of the bank, not the user, to ensure that users do not visit phishing sites by ensuring that their sites cannot be spoofed? Or is it the responsibility of the user not to be fooled?

Finally, computers also impose a degree of abstraction from the activity (McLoughlin, 1999, p108-109), an abstraction that removes reliance on social cues and on impressions given and given off (Goffman, 1959, p28) may also affect attitudes to security.

2.4 Summary and research questions

To summarise, this review has surveyed literature covering both what makes users fall for phishing and how effective the measures taken by banks and other service providers to combat it seem to be. It has also briefly discussed the fundamentals of theory concerning online identity that could be applied to enhance understanding of how to beat phishing. There appears to be no clear consensus amongst researchers about most of these topics except perhaps that users tend to ignore toolbars and that there are inherent problems with security studies around reproduction of genuine online interaction.

Points of particular interest identified include that of whether impulsiveness affects propensity to fall for phishing, the relationship between online and offline security behaviours and who is responsible for online security.

It appears that the way that the user experiences him or herself as an online entity is very different to the technologist's view of the user in a digital identity system. Can this broader understanding of the user as an individual online help service providers to find ways to stop users falling for phishing attacks?

For the purposes of this study, these issues are distilled down to the following research questions, as shown in the previous chapter:

- Why do users fall for phishing?
- Do personality factors have any effect on how people deal with phishing?
- What is the relationship between online and offline behaviour and how does it impact the response to phishing?

- How do users react to existing anti-phishing methods?
- How can existing anti-phishing methods be improved?
- Whose responsibility is it to protect the user against phishing?

If these issues cannot be resolved, the alternative may be to give up on relying on the user entirely, either accepting a high rate of false positives from site blocking systems or attempting to prevent users from supplying useful information to phishers at all.

3 Research methodology

3.1 Introduction

The purpose of this chapter is to describe and justify the chosen research process for this project.

The original impetus for the research was a desire to investigate why, despite the amount of effort that appears to have gone into educating users about phishing, people still fall victim to phishing attacks and whether this is due to a fundamental misunderstanding of how users understand themselves and their online identity. The process started with a literature review in order to clarify the research questions. Expert user interviews were then carried out, followed by a user survey/questionnaire in order to discover expert and user opinion about phishing. While there was some time overlap with these two latter stages, due to a tight time schedule, the intention was to conduct them sequentially, not concurrently, with the earlier interviews influencing the questions asked during the survey.

The data gathered from the interviews and the survey was then analysed and findings considered, in part through the perspective of theory about online identity.

3.2 Literature search methods and results

The research started by a survey of research done into reactions to phishing and to anti-phishing materials such as toolbars. The research that is most frequently cited into this area appears to have been done between 2005 and 2009 although earlier and later studies are also considered in the review. Literature was accessed through Google Scholar and publisher databases such as IEEE, Gale Academic and Elsevier Science Direct.

The findings of the literature review, presented in chapter two of the dissertation, were condensed (see appendix 3) with the objective of extracting themes to use as codes in interpreting further research.

3.3 Research data required

In order to further investigate the questions raised by the survey of the literature, it was decided that experience and opinion from both users and experts within the field would be gathered. Users were asked about their opinions on why people succumb to phishing attacks and what is and should be done to mitigate this. Users were asked about their experiences of phishing, how they deal with mutual authentication and preferred sources of information about avoiding phishing.

This was intended to illuminate both sides of the research – why users behave as they do and how best to help them not to fall victim to phishing. It also seemed that it would be interesting to contrast user experience and opinion with expert comment about that experience and opinion – any noticeable difference between the two might generate insights

into why anti-phishing methods have had limited success to date as explained in the literature review.

3.4 Methodology chosen

3.4.1 Philosophical assumptions

While social research has historically used a wide range of research perspectives and methodologies, the range used in computing and information science research has been somewhat narrower and more normally focused on quantitative methods, perhaps reflecting the scientific, physics and mathematical basis of computer systems development but ignoring the social science aspects of their use.

As in social science, paradigms vary according to source. In this report, the three types of paradigm identified by Orlikowski and Baroudi (1991), positivism, interpretivism and critical studies, will be used.

Using Chua's (1986) classification of positivist, interpretive and critical studies, Orlikowski and Baroudi (1991) examined a sample of published research over 5 years between 1983 and 1988 and found that although the three classifications could all offer insight into the use of information systems, positivism was the dominant paradigm (Orlikowski and Baroudi, 1991).

- They defined positivist studies as either serving to test theory in order to increase predictive understanding of phenomena or to describe events in an 'objective' and 'factual' way (Orlikowski and Baroudi, 1991). Positivism very often corresponds with quantitative methods and defines theory as something that can be empirically falsified (Straub, Gefen, and Boudreau, 2004).
- Interpretive studies reject the idea of a factual or objective reality and instead attempt to understand phenomena through the meaning that participants assign to them (Orlikowski and Baroudi, 1991).
- Critical studies aim to expose and critique assumptions that are taken for granted about systems and organisations and to highlight deep seated contradictions (Orlikowski and Baroudi, 1991). They contain an ethical intention and are emancipatory in nature (Stahl, 2008, p. 8).

While Orlikowski and Baroudi found that the majority of the research from the 1980s surveyed fell into the positivist camp, they felt that the value neutral and independent nature of positivist research lay counter to the goal of information systems research, which was to have a positive impact on information systems practice (Orlikowski and Baroudi, 1991). There has indeed been a move over the past few decades towards accepting qualitative approaches within the information systems field (Avison, Lau, Myers, and Nielsen, 1999), although non-positivist approaches still attract a degree of hostility from some practitioners (McLoughlin, 1999, p. 117).

Since the overall aim of this research is to understand and improve anti-phishing practice rather than to test theories about phishing or online identity, the approach taken will not overall be positivist in nature. Although aspects of the user research will involve questions derived from the literature review and expert interviews, it is not assumed that these will form observable and measurable theories. Nor will the phishing data be used to test the theories about online identity. It also places the user rather than the technology at the centre of the discussion, again a step away from the positivist paradigm (McLoughlin, 1999, p. 142).

In general, in seeking to examine how individuals interact with phishing attacks and anti-phishing materials and in exposing assumptions with the intention of improving current practice and changing the status quo, the approach will be primarily critical in nature, as this also allows for a degree of causality that interpretive studies would not without looking to test causal links in the way that a positivist approach would. In addition, as there is some discussion as to whether the three paradigms, while philosophically distinct, can overlap somewhat in practice (Myers, 2011), (Stahl, 2008, p. 9) the approach may also have interpretive aspects in order to better understand the user experience. Indeed Stahl (2008, p80) reports the use of 'critical interpretivism' as a term.

However, one key part of the critical approach is the intention to overturn oppression (Stahl, 2008, pp. 10-11). That is not appropriate with this dissertation but it could be argued that approaches to phishing that focus either on educational approaches that are overtly technical in content or technical approaches that control the user experience exclude the user from the discourse and disempower them (Stahl, 2008, p23). This reflects the view of Habermas, as cited by Stahl, one of the key thinkers behind critical realism, in stating that affected parties should be able to participate in discourses. In seeking therefore to better understand the user experience and to provide information about phishing that includes rather than excludes, the effect is in one sense emancipatory. It does therefore also allow for a practical intention, although a broader one than simply improving management efficiencies or saving banks money.

This approach will also fall within an anti-foundationalist worldview, given the belief that it is not possible to prove or disprove anything absolute about phishing independent of user experience but only to understand because the problem is primarily one about people that is produced through social interaction and how they react and change (Grix, 2004, p. 61). This reinforces the decision to omit consideration of malware based phishing attacks from the research as in that case cause and effect are more predictable.

3.4.2 Methods

Based on these discussions, and in particular because one goal was to produce recommendations as a result of the research, enlarging the body of knowledge and contributing to meeting practical concerns around phishing (Myers, 2011), a survey and interview based approach was chosen, using mixed methods. There is also potential for considering the overall approach, including the secondary research conducted on the literature, as grounded theory based, where the grounded theory approach is defined as developing theory grounded in the gathering and analysis of data (Myers, 2011) from different groups (Creswell, 2009, p. 13). It should be noted that the objective is not to further develop theory about online identity, nor to test that existing theory, as in a traditional, positivist view of theory, but to use that existing theory as a potential means of understanding the data with a view to making recommendations about phishing (Birley and Moreland, 1998, p. 29).

Mixed methods combine qualitative and quantitative research and aims to gather data from both experts and users. In part this also reflects some of the approaches taken by studies in the literature review. Many of these were quantitative and positivist in nature, measuring and analysing a set number of possible reactions to phishing situations within laboratory conditions, for example choosing one of four different ways of dealing with a phishing email (Pattinson, Jerram, Parsons, McCormac, and Butavicius, 2012) or noticing or not noticing a security indicator (Dhamija, Tygar, and Hearst, 2006). The emphasis was on numerical outputs and deriving meaning from them and on working with theories that could be confirmed or refuted by the data (Straub, Gefen, and Boudreau, 2004).

Nonetheless some of them also included a qualitative aspect, providing explanations of user thoughts and motivations (Downs, Holbrook, and Crainor, 2006) that generated insights useful for this project.

There were a number of primary reasons to use a mixed or triangulated approach (Blaxter, Hughes, and Tight, 2006, pp. 84-86). These were to use qualitative expert interviews to confirm and further examine key issues identified during the literature search, to introduce further issues not identified by the researcher and to facilitate surveying users and to use mixed quantitative and qualitative research with users to confirm expert views and to allow for users to help interpret the quantitative findings.

In addition there may be further factors that influence why a research approach may get chosen, one of which is the context within which the researcher has been trained and worked (Orlikowski and Baroudi, 1991) – in this case journalism, which is highly qualitative in nature.

The approach chosen does not use data collected to test and revise theory about identity but instead uses the theory to illuminate the data. This meant that the approach taken to questioning, both in the interview and the questionnaire, was primarily inductive in nature with evidence leading to theory, rather than deductive where the theory would shape the questions (Grix, 2004, p. 113). This was also seen as advisable to avoid using overly theoretical language during the research process to subjects that might not be familiar with it.

3.5 Expert opinion

In order to maintain a degree of consistency that would make analysing data more straightforward, while still allowing for new issues to be considered, semi structured interviews were used to gather expert opinion. The grounded theory approach meant that there was the option to update or change the questions to cover topics that arose as a result of previous interviews (Dawson, 2007, p. 30).

The tight time schedule for the project and the sensitivity of the nature of the topic meant that potential interviewees were chosen from existing professional contacts of the researcher and experts with links to Edinburgh Napier University. It is not necessarily the case that their views can be extrapolated to the broader population of people working in online banking (Dawson, 2007, p. 49) but it was felt nevertheless that they were generally representative and their expert status would give them a good overview of current thought and opinion in the field. In addition, it was felt that it was important to interview people actually working and consulting in the field in order to both expand on and to provide a counterpoint to the academic opinion obtained from the literature review.

Eight interview invitations were issued with a view to securing five to six interviews. Five interviews were conducted by phone (although the third interview featured two interviewees, who although colleagues offered differing views on a number of topics and so their responses were analysed separately) and a further one by email. In line with Edinburgh Napier University ethics guidelines, the interviewees were promised anonymity. Without identifying either them individually or their institutions, the interviewees comprised one security consultant, one digital transactions consultant, two industry body representatives, a technology company representative and two bank representatives.

3.5.1 Interview content

The interview questions were broken down into three main categories: general, user education and attitudes to phishing. The interviews began and ended with general questions to ensure that topics not foreseen by the researcher could also be raised.

The questions as they stood after several revisions in draft form but before the first interview can be found in appendix 4. They were in part taken from issues which arose from the literature review, as shown in tabular form in appendix 3, and were in part designed to enlarge on the question of how the online identity of users in the context of phishing is understood.

Interviewees were initially asked about their stereotypes of people who fall for phishing attacks and why people fall for phishing attacks – these questions were intended to flag up any prejudices or preconceptions that might inform subsequent answers. They were then asked how responsibility for protecting users should be shared and the balance between technology and education as an ideal approach. The idea here was to investigate the tension between technological and education based solutions explored in the literature review and also to provide some context for the tendency of users, shown in the literature to ignore security information.

Interviewees were then asked what they thought users look out for and think about when making security decisions, in order to see whether this corresponded in any way with the types of security indicators tested in studies such as Dhamija, Tygar and Hearst (2006). User thinking about their online identity was also examined with questions comparing online to real world security, how personality affects propensity to fall for phishing and whether there are any correlations with non-ideal banking behaviours.

The expert interviewees were then asked about educational initiatives, in order to see how these matched with the types of approaches tested during the literature, for example by Kumaraguru, Sheng, Acquisti, Cranor, and Hong (2007) and to see how useful the experts thought industry initiatives were. These topics were also to be investigated in the user survey with the intention of comparing results.

Finally, experts were asked about what they'd like to know about the user perspective, in part to find out what wasn't currently understood and in part to solicit ideas for the survey. Finally, they were asked to sum up how they saw the situation with phishing evolving.

Each interview was recorded and then transcribed and returned to the interviewee for checking. The full transcriptions were protected by encrypting them for security in accordance with ethics requirements.

3.6 User data

The Smart Survey system at www.smart-survey.co.uk was used to gather user data, primarily for its functionality and reasonable pricing. It also allowed respondents to remain anonymous and did not gather or store user identification (except IP addresses for preventing multiple replies), which was thought important given that users were being asked to reply honestly about their behaviour and about their experience of crime. Users were given the option to provide their email address for the chance to win an Amazon voucher as an incentive but a significant number (around a third) chose not to. The offer of a voucher was designed to increase respondent numbers and also to attract respondents who did not necessarily have expert and deeply thought out views on the topic, as it was thought important to represent both expert and non-expert opinion via the survey.

3.6.1 Survey content

The user perspective was surveyed using an online survey containing a mixture of closed ended and open ended questions (Dawson, 2007, pp. 32, 91). The questions were influenced by the research questions identified during the literature review and by the expert opinion gathered during the first few interviews, with a view to comparing user and expert opinion on specific topics. Specifically, the following research questions were examined: how users are currently responding to phishing, their experience of anti-phishing education, how impulsive behaviour correlates with phishing susceptibility, online versus offline security attitudes and who is responsible for protecting against phishing.

The first draft of the survey, which contained 20 questions, some multi-part in nature, was judged too long and the scope was too wide ranging. There was a concern that the length of the survey might deter some respondents from completing it. Although all of the questions derived from the literature search and expert interviews, some of the questions were, it was decided, more appropriate for possible further work and some were considered better examined in a different format to an online survey.

A shortened second draft of the survey was tested on a contact who specialises in designing user experience surveys for a large corporation and was further revised as a result of her input.

The final survey, which contains 22 single part questions, can be found in appendix 5, along with a summary of the results.

3.6.2 Sampling used

It was decided that obtaining a truly representative probability sample of computer users for the survey was impractical within the constraints of the project and instead purposive sampling was used (Dawson, 2007, p. 51). The approach taken was a combination of convenience and snowball sampling where friends were approached in real life and online to take the survey and to recommend it to people within their network and links to the survey were posted on Internet chat forums for women, blogs, Twitter, Linked In, a technical forum and message groups frequented by the researcher and also circulated to other students at Edinburgh Napier University.

This raises the possibility of sampling bias, particularly as participants were to a certain extent self selected. It also means that it will be difficult to extrapolate the results to the broader population and there is a risk that not all sections of the population are properly represented, although the range of locations used to advertise the survey (at one extreme feminist discussion boards, at the other a technical forum) means that the sample should not be too homogenous. However, the survey was advertised only as being about Internet use, to avoid limiting respondents to those who had strong opinions about phishing from the outset and as discussed the chance to win an Amazon voucher may have increased the range as well as number of participants.

3.7 Disadvantages of chosen methods

All methods have disadvantages. For example, in questionnaires or surveys, open and closed survey questions both have advantages and disadvantages. While open questions may lead to a richer response and allow respondents to raise new topics, they also can be harder to interpret and respondents may find them too much like hard work. Closed questions on the other hand may be easier to administer and analyse but may not offer an option that accurately reflects the respondent's experience and hence may miss the

opportunity to discover factors not already considered by the researcher (Dawson, 2007, p. 92).

The online survey method selected, while appropriate for gathering a large number of responses, had the disadvantage that it was too cursory for some of the questions identified in earlier parts of the research. Some questions had to be omitted, partly to make the survey shorter and hence more attractive to potential respondents and some because their seeming relevance would have required too much explanation. It was, even so, difficult to express some concepts in survey question form in a way that would be understandable to respondents without lengthy explanations.

It also proved difficult, due to the topic, to formulate questions without using emotive words or without prestige bias (Dawson, 2007, p. 93). However the anonymous and online nature of the survey may have reduced that factor. Correct formulation of questions is vital, and a skill in itself which requires proper training (Grix, 2004, p. 129), not something that was possible during the time available for this dissertation.

Nor was the survey fully tested on a representative sample of the eventual audience and as such proved ambiguous with respect to several of the questions. For example some people either did not read or did not understand the definition of phishing given in the survey. A couple did not understand what 'bank security messages' referred to. There was a failure to specifically ask for comments about how to improve educational materials, expecting instead that people might volunteer that information in the general comments questions (they didn't).

It also had the disadvantage that answers were self reported and that it is therefore difficult to consider the answers as objectively true in any sense other than about the participant's perception of themselves. Participants may also have been influenced by taking part in the process (Dawson, 2007, p115). It also makes answers to questions where the answers lie on a scale of low to high difficult to analyse as participants may understand the scale differently. In addition, it is not really possible to tell if all respondent have understood the questions in the same way (Grix, 2004, p. 129), making it hard to compare the answers.

In that way, the survey cannot be viewed as containing truly quantitative aspects and its value is largely qualitative in terms of what can be inferred from the answers given.

The timescale for the project also caused problems in that questions for the survey had to be designed before analysis of the interviews started. It would have been better to be able to design the survey questions after completing analysis of the interviews. Had this been done, there would have been the opportunity to ask, for example, about users felt about banks removing their agency with some of the technological measures proposed or to ask about the use of mobile phones for two factor authentication.

The potential problems with the semi-structured interview method chosen for the expert interviews was that it potentially could be too restrictive – while less restrictive than a fully structured interview, which is often viewed as more appropriate for quantitative approaches, it still involved asking each expert the same questions initially (Dawson, 2007, p. 29), even though some questions may not have been fully relevant to each individual. Equally that reduced the opportunity to completely tailor the interview to the individual, especially as interviews were fixed in duration (35-40 minutes) to avoid impinging too much on the schedule of busy professionals. On at least one occasion, the impression was given that the individual could have talked for longer, when the interview closed on schedule after 40 minutes. Transcribing also provided practical challenges for the researcher who is disabled,

creating the temptation to stop the interviews from becoming too long by not further investigating themes.

In addition, some interviewees, agreed to be interviewed but then failed to finalise times for the interview or cancelled their interviews. This appears to be a hazard of academic interviewing, where the interviewee may not identify any publicity benefit to themselves in participating or conversely may worry about anonymity being breached.

3.7.1 Alternative methods

Alternative methods that could have been used but were deemed too problematic or inappropriate for this study included observation and experiments. As discussed during the literature review, there are problems with these methods relating to role play and the primary/secondary activity dichotomy that make it difficult to be sure that the data gathered during these activities is truly reflective of how users behave online.

Any longer term observation type studies of user behaviour were ruled out due to the tight time scale available for the dissertation.

One possible alternative approach might have been to take a semi-structured, unstructured or oral history interviewing approach to gathering user experience. This was ruled out primarily because of the practical issues experienced with transcribing the expert interviews but also because there was some concern about how much users might have to say about a process that the literature review and expert perceptions suggest is largely unthinking. It might also have been difficult to find an adequate number of participants willing to talk, especially participants that had been victims of phishing. Instead, users were given the opportunity during the online survey to discuss their thought processes in free form essay style questions. Nonetheless, as discussed above, some of the questions that arose from the literature review might be better explored in this format in further work.

3.8 Data analysis process

3.8.1 Expert opinions

After all the expert interviews were complete, the transcripts were then coded. The initial codes were extracted from the literature findings and then refined. However further codes were also derived from in depth reading of interview transcripts (Rubin and Rubin, 2005, p. 210) and so stray beyond the findings of the literature review. The codes used are presented in chapter four as subheadings for the analysis of the expert interviews.

3.8.2 User survey

The questions in the survey were either closed questions where respondents were given a choice of possible answers or a scale or they were open questions where they were invited to write brief text answers without prompts beyond the question.

The answers to the closed questions were first considered individually. The open answers were then analysed to extract anti-phishing strategies and to present user opinion. Finally both closed and open answers were filtered by factors such as age and knowledge of computers. More information is given in chapter five where the results are presented.

Because the approach of this dissertation is primarily qualitative, limited amounts of statistical analysis were employed. However descriptive statistics i.e. describing and

presenting the data (Fink, 2006, p. 70) were used as was the chi square test which tests for significance via the null hypothesis that proportions are the same (Fink, 2006, p. 71).

3.9 Evaluation framework

The aim of the project was to shed light on the question of phishing and anti-phishing education through primary research and application of theory, with a view to making recommendations that may improve anti-phishing practice. It was not intended to prove or disprove specific theories and the methods used were primarily qualitative, as discussed. The degree to which the project can therefore be viewed as successful depends on how well it fulfils those aims with regards to the research questions through the media of expert opinion, user experience and theoretical input.

A tabular framework was developed which lays out the research questions, what would be expected to be found based on the literature and what is actually found during the user and expert research. The outputs of this process will form the basis of the discussion of results later in the dissertation. The table is presented in appendix 6.

3.10 Chapter conclusion

The purpose of this chapter has been to explain and justify the approach taken to the research and to outline how the success of the research can be assessed. This approach could be described as critical interpretivism – seeking to explain user reactions to phishing and behaviours around mutual authentication with a view to improving them overall. As such, there is no attempt to prove or disprove existing theories, simply to make recommendations to improve practice. The methods used therefore are mixed i.e. qualitative and quantitative although primarily qualitative i.e. semi structured interviews with experts and a survey of users.

4 Findings from expert interviews

4.1 Introduction

This chapter presents an analysis of the data from the interviews. After a brief discussion of the data analysis process, it presents the data grouped by research question and code. The ethics requirements of the dissertation mean that the interviews will not be reproduced in full, neither in this chapter nor in the appendices but extracts will be quoted as part of the discussion.

The interviews were carried out by phone during March 2012, except for with [6] who chose to answer questions by email instead. The interviews took place before the user survey. Interviewees were later given the chance to comment on the survey results but did not respond.

As Dawson (2007) states, participants may be influenced in their views by taking part in the research process (Dawson, 2007, p114). This seems unlikely with expert interviews, although one of the interviewees, a bank executive, did request a copy of the questions in advance of the interview and the other bank executive completed his answers by email, thus removing the element of spontaneity. There is also the possibility that interviewees may have tailored their answers to fit their corporate position rather than personal perspective – one of the bank interviewees for example had to clear the questions through his press relations department before agreeing to the interview. Several of the interviewees also stated that they had not previously thought about how personality might influence susceptibility to phishing.

The order in which the questions were presented may also have possibly influenced the answers. The questions in the order used are shown in appendix 4 – this order does not correspond exactly with the order in which the answers are discussed below, which was ordered to produce an overall more coherent narrative.

4.2 Interview analysis process

After each phone interview, the interview recordings were fully transcribed and sent to the interviewees for checking. The interviews were then coded, using codes derived from analysing the results of the literature review and from the contents of the interviews themselves. These were mapped as closely as possible onto the research questions. As discussed in the previous chapter, because of the semi structured nature of the interviews these codes do not exactly correspond with all the issues generated by the literature review that were used to produce the interview questions nor with the research questions.

4.3 Interview findings

In this section, the findings of the interviews will be described, organised by research question and code. As discussed, these findings represent what different types of people who are involved in combating phishing think about users, what users do about phishing and how users think about phishing – this may not necessarily correspond with what users themselves do or think. There is some overlap between codes as certain interview extracts may be relevant to more than one code.

4.3.1 What is the relationship between online and offline behaviour and how does it impact the response to phishing?

4.3.1.1 Unreality of online world

If theories of online behaviour and identity suggest that offline and online worlds are different examples of multiple realities (Goffman, 1974, p3), how is that idea reflected in expert opinion on user behaviour? There seemed to be general agreement that the online world is something quite different to the average user, something lacking in the attributes of normal reality.

In particular there is an absence of physical cues that help people to make good judgements in their daily lives.

“...it’s distant and they can’t use those traditional senses of touch...” [3a]

“physicality itself is part of the issue. Things like locks you can see. When you can see things I suppose that does change people’s attitudes a bit.” [2]

“I think it’s got to do with all our senses – it’s sight, smell, sound, touch, you name it. You don’t have that in the cyberworld...” [4]

The result seems to be that being online seems less real.

“It’s almost like a life without responsibility when you go online.” [3a]

“...you’re sitting in a cosy armchair or you’re in your study and it’s just stuff on a screen – there’s the perception that nothing there can hurt me.” [5]

4.3.1.2 Attitudes to online versus offline security

The net result appears to be very different attitudes to safety, according to the experts interviewed. It also reflects discussions in the literature review about risk calculation (Taylor, 2008), (Grix, 2004).

Indeed people seem to act quite differently online to offline, particularly with regards to sharing personal information.

“I personally think people are less aware in the online environment... when people are walking down the street and a bloke comes out of an alley and says ‘do you want to buy a telly’, most people unless they are criminally minded would most likely question it because experience tells them that you wouldn’t buy a TV for cash off a bloke you don’t know in an alley and expect it to be legit but in the online space anyone can set up a website front offering 75% off recommended retail price and people will willingly hand over their card details... [3a]

“I think people take more risks online. They are willing to do things in the online world that they would never do in the offline world. You can stumble across a website that offers designer clothes at 25% of retail and people will quite happily put in their credit card details in the expectation that they will get their designer clothes at 25% of retail yet if there if there was a shop that suddenly appeared on Princes St that said ‘Armani 75% off, we guarantee it’s genuine’, do you think people would go in? No, absolutely not. They’d know it’s a scam a mile off.” [4]

“We’ve almost got two personalities – what we do in the virtual world and what we do in the real world.” [3a]

Part of this different personality seems to involve being more trusting.

“Yes, they hide behind a fancy looking web page and you don’t have that traditional touch and look and feel and previous experience to inform your decision as to whether this is legit or not. You’re in your own home and in a trusted environment – it’s not like when you’re out on the street and you’re a bit more guarded and your instincts kick in. In the comfort of your living room people tend to be a bit more trusting.” [3b]

Not every interviewee agreed about being more trusting though. Instead, the lack of full sensory input discussed above could cause the differences in behaviour.

“I don’t think they are more trusting online, I just think they act differently... I think the risk calculation components of our brain don’t work to the same amount, I’m convinced of it.” [4]

In addition, as discussed, online behaviour just seems less risky, not only because of the lack of financial implications but also for more fundamental reasons that form part of human risk calculations.

“There is no physical threat to online security. Overall the perception of threat differs between the two and phishing is largely immaterial when compared to the threats arising from being caught up in other physical risk based scenarios (fight or flight).” [6]

4.3.2 Why do users fall for phishing?

Having established that the interviewees in general think that people behave differently online compared to offline and possibly appear to be more trusting or at least less untrusting, the interviews then investigated reasons why people might fall for phishing. Therefore the next set of codes considers what sort of people fall for phishing and looks at reasons, extrinsic and intrinsic, why they might. There may be some overlap between codes, especially given that there are potentially causal relationships between codes.

4.3.2.1 Stereotypical victims

It was thought interesting to ask interviewees as the first question in the interview to come up with a stereotype of a typical victim, without thinking too much, as that might shed light on subsequent answers and on industry attitudes to phishing victims and hence on ways of protecting victims of phishing crime.

In fact the majority of the interviewees felt that there was no stereotypical victim, with [1] linking his answer to his views about how victims are too busy to stop and think about phishing risk. [5] added that it can be difficult to form a clear view of who falls victim because people are not necessarily honest, perhaps through embarrassment, about what happened. In addition, even experts can fall for scams.

“It’s anybody. The classic type would be someone more elderly or less computer literate but actually it applies to people who are not just computer literate but also security aware, just in a moment of distraction falling prey to a phishing attack.” [1]

“I can’t think of a particular type and I say that because from what I’ve seen it’s quite varied... I don’t think there is a normal profile or a standard user because I think everyone is susceptible. If you hit them at the right point then they become a victim.” [3a]

“... I know some very smart people in the industry who consider themselves security experts and I’d agree that they are security experts and I know for a fact that they have fallen victim.” [4]

Nonetheless the interviewees with the most technical roles did flag up the stereotype of people who do not understand computers.

“I think there is that category who have no mental picture, even though they understand there are hackers and viruses, of what is going on behind the screen.” [2]

“Uneducated and by uneducated I mean that they have not been properly warned about the risks of responding to these types of emails. Further also I would say that they typically are not computer savvy so they are unable to instantly respond or detect phishing attacks. Your stereotypical victim is an old age pensioner...” [4]

4.3.2.2 User ignorance

Ignorance, or to be more precise, lack of awareness (Yu, Nargundkar, and Tiruthani, 2008) and lack of technical expertise (Anandpara, Dingman, Jakobsson, Liu, and Roinestad, 2007) were both flagged up in the literature review as reasons to fall for phishing.

There appeared to be reluctance amongst the interviewees to describe phishing victims as ‘stupid’, which is consistent with their comments about stereotypes, although [2] did use the word with regards to 419 scam victims.

“If you’re stupid enough to believe there’s \$25m waiting to be airfreighted out of Switzerland if you send \$25k frankly you deserve whatever you get.” [2]

However he also related it back into the lack of a mental framework about phishing.

“We’re in a situation where – it’s the same as saying to the kids ‘how do you know that’s right just because you saw it on Wikipedia?’ What are you using to cross reference it? What are the mental clues? The thing is that they don’t have any because they’ve not been taught that.” [2]

“There are people like my dad who really just don’t understand and have no mental model of computers or the Internet. When they get an email that purports to come from Microsoft telling them that for only \$24 they can have their system upgraded, they’ll happily type in their card details because it never occurs to them it’s anything other.” [2]

He also made the point that the lack of awareness or knowledge may also extend beyond computing.

“You know they have this Race Online thing with Martha Lane Fox so that everyone is going to be online by 2012 – since a fifth of the population is functionally illiterate what does it mean to put them online when you haven’t taught them to read? Half the population is innumerate. Looking at something online when they can’t read a bus timetable – well they won’t read it when it’s on a web page either. How are you going to stop those people being vulnerable to phishing? It’s really difficult. You’ve got to find some way of protecting them.” [2]

While the answer to this may in part be education, some people appear unaware of the education that already exists about phishing, both topics that will be explored further later.

“Simple attacks – education is key, people who fail to spot an obviously dodgy or unprofessional looking attack need to be continually educated.” [6]

“They’re not aware of it [anti-phishing education]. If I’m not aware of it, your average consumer will be utterly unaware of it.” [1]

4.3.2.3 Positive belief

Although the interviewees were reluctant to be too damning about ignorance, they did question the way in which users believed they had protected themselves against phishing and online crime. For example anti-virus packages are not intended to protect against phishing.

“I’d like an understanding of what the average person thinks the risks they are exposed to are. Do you believe you are protected? Do you believe you are protected if you use an anti-virus product?” [1]

Users may believe that what the computer tells them is true, either like [3a]’s 18-24 year olds or [2]’s elderly father.

4.3.2.4 Irresponsibility/carelessness

On the other hand, as Downs, Holbrook, and Crainor (2007) found, some users just don’t especially care about protecting their personal data, something that will also be covered below in detail in 4.3.3. This may be exacerbated by different attitudes to the online world, as discussed in 4.3.1. This manifests itself in carelessness that may leave users vulnerable.

“It’s ultimately the person that’s causing their own downfall.” [3a]

The threat appears remote to them, if they perceive it at all.

“I think people have yet to get their heads around how insecure the Internet really is. It’s only when you’ve got hit for a bit of card fraud or for a phishing email that you might start to accept it a little bit more but I think because it is remote people accept the threat as being remote.” [3a]

Nor do they feel it is their responsibility or liability, a topic which will be further explored later.

“Coming back to the economic situation, the consumer feels little pain. If you have anecdotally spoken to someone in your personal life that has had a small amount of money taken out of their bank account and they don’t understand why – for example the architect who was working on my house a couple of years ago had £3000 lifted out of his business account. He was very lackadaisical – he wasn’t worried about it as the bank was going to reimburse it.” [1]

4.3.2.5 Security as a secondary task

Some of that carelessness may come from security being seen as subsidiary to the main task in hand, something that was discussed in the literature review (Anandpara, Dingman, Jakobsson, Liu, and Roinestad, 2007). Users may also get into an automatic routine with their tasks that detracts from their awareness.

“You’re on a mission – if you think about how somebody goes through their inbox there are a lot of emails. If I go to mine there are 100s and you are rattling through them going what do I need to do? Do I need to ditch it, respond, hold it for later? Something comes up, you’re making a snap judgment and that judgment could be wrong... So there’s probably something about the busyness of everyday life and the way that people process email and the whole HCI piece around email.” [1]

“At the end of the day the users are so used to typing in usernames and passwords that they respond to a request for username and password in such a way that they will just give it over. If you are walking down Princes St and someone says ‘hey, I need to see your credit card’ you aren’t going to pull your credit card out but if you were browsing the web and a prompt comes

up asking for user name and password you will quite happily type it in, especially in the corporate world.” [4]

4.3.2.6 Extrinsic factors

For some of the interviewees, users were playing with loaded dice with both technology and Internet services and even banks conspiring to make avoiding phishing harder and more confusing than it needed to be. Security interfaces can be inconsistent (ed: Roessler and Saldhana, 2010) and even misleading (Grover, Berghel, and Cobb, 2011). In addition even though a major part of bank anti-phishing education is intended to inform users that they will never receive emails asking them to reset their security details, in reality sometimes banks or other Internet services do request this or otherwise contradict their own guidelines (Anderson, 2007).

“The waters are slightly muddled by the sheer volume of other online services – you can start with Facebook although they are getting better – but any Internet forum that will do things like send you an email asking you to reset your password. From an end user perspective they probably are having problems differentiating with what a bank does which should be at a different level to what is more to do with your online social presence.” [1]

“So the banks have long said ‘we will never ask you for your PIN number, never type your PIN in’ except Citibank, one of the banks I used to use until very recently, asked me for my PIN number as a security identifier in some online transactions.” [4]

The security indicators that users are told to look out for may even not be that helpful in avoiding phishing.

“For example you bring up websites and we’ve said ‘make sure you see the little padlock icon there’. The reality is that the padlock icon means absolutely nothing. It says there’s an SSL channel established between you and the other website but it doesn’t guarantee the identity of the other website.” [4]

Fraudsters may even be able to use security indicators to their own advantage.

“The whole certificate authority industry has a lot to answer for in terms of issuing credentials and certificates to people who have then been able to run imposter websites and capture user data.” [4]

These problems combine to mislead even users who are educated about what to look out for.

“Why is everything not encrypted by default? And even then if it is encrypted how do we guarantee the identity of the remote website we are talking to? At that point you are talking about things such as DNS security which is an underlying technology that is well understood and has been available through standards for several years now and yet major operating systems manufacturers including Microsoft still don’t fully support it. So users themselves, they gut check when they go to a website, they rely on the underlying technology to take them to where they want to go. They say ‘I want to go to my bank.’ They assume that when they do a DNS look up it’s going to return the IP address of the bank’s website. They go there and see a padlock because we told them to look for a padlock, they assume it’s a secure session and they can type in their user name and password but there’s no guarantee that that really is the bank’s website because the PKI industry has fallen down. They’ve issued certificates to fraudulent users or someone with access to a root certificate has been able to create another certificate for an imposter of the bank’s website or they’ve been able to tamper with the DNS or any of a number of attacks. So we’ve trained users to look out for these visual cues that at the end of the day mean nothing.” [4]

The solution may have to be legislation and governance (Wilson and Argles, 2011), but as yet that has not happened.

“Regulation and governance - not enough is done here to regulate the Internet content and service providers, but while this may come one day it is littered with legal complexity.” [6]

4.3.2.7 Skill of the phisher

As well as contending with lack of awareness or being too busy or personality factors that may reduce caution, users also have to deal with some phishing attempts being both skilful and convincing (Anandpara, Dingman, Jakobsson, Liu, and Roinestad, 2007).

“When you look at some of the sites they are pretty good. It’s only when you’re a security professional that you know what you are looking for but that’s because you are looking for it. If you didn’t know you’d just accept that that website that’s put before you is a genuine site.” [3a]

Like a well crafted marketing message, phishing messages are designed to make the user act.

“Phishing emails are never a simple notification – their motivation is to drive somebody to a site so they can capture something, a credential, whatever. They always say your account has been subject to something, there’s always an information action thing going on.” [1]

“It’s a call to action connected to getting a refund or keeping their online banking going – something that actually is important to them.” [5]

Phishers also update their activities and techniques to keep abreast of changes in the fight against them.

“...[banks] put warnings out there to say look out for a padlock, don’t click on a link you’ve not seen before. And the fraudsters then leave that same message in their next evolution of phishing attack so they obviously realise that people do take on board what the banks tell them. So they are quite savvy from that perspective.” [3a]

“...fraudsters are continually evolving their sites and making them look more sophisticated and look more and more genuine so it becomes more and more difficult for the consumer to differentiate between a legitimate email or site and a fraudulent one. It’s like an arms race. We might have a new piece of technology or software and the fraudsters will evolve it and change the messaging so it appears again that it’s coming from the bank. It can be difficult – even people in our industry aren’t sure sometimes when they see an email whether it’s from the bank or a legitimate agency or otherwise. It’s difficult. Unless you are working in that space and are IT literate, it’s not going to be easy.” [3b]

There is also a move towards attacks that cannot be detected simply by visual inspection.

“Advanced attacks – these make it difficult for many people to spot the difference. They are also the pest for fraud departments (man in browser/session/mobile, parallel sessions, velocity attacks).” [6]

4.3.3 Do personality factors have any effect on how people deal with phishing?

4.3.3.1 Personality and other intrinsic factors

Age is a factor that was mentioned, although not in great depth, in the literature. Dhamija, Tygar and Hearst (2006) found no correlation in terms of ability to identify phishing sites with

age, whereas Kumaraguru, et al. (2009) found that there was a correlation, with younger people more likely to be deceived. Of the interviewees, colleagues [3a] and [3b] seemed to have thought most about age with [3a] who seemed to be the older of the two by around 20 years arguing that the young were most likely to be deceived because of their acceptance of what the computer tells them, a view that closely reflects Turkle (1996). In contrast the younger [3b] argued that this was not the case and the old were more likely to be deceived because of their lack of understanding of computers.

“Part of me looks at it as a middle aged male over 50 responding to an email that has come to them out of the blue because their knowledge of computing and what is real and isn’t real is somewhat limited. We’ve certainly seen this in things like boiler room scams. But actually from some of the work I’ve heard of, that group tends to be a little more savvy because they naturally don’t trust the computers. We’re seeing more of the 16-24 demographic who would respond to an email because they accept it as real because computer says it’s real.” [3a]

“As you get new generations coming into this space, new users are familiar with social media, twitter etc and are more aware of issues online than those in the older community. The new users around this environment are more aware of the issues.” [3b]

Yet age is just one intrinsic factor and one interesting issue that did seem arise from the literature review but seems little studied is the question of how personality affects behaviours around phishing and in particular impulsiveness (Pattinson, Jerram, Parsons, McCormac, and Butavicius, 2012). None of the interviewees admitted to having considered this in depth before but both the banking representatives, [5] and [6] commented that it was interesting.

“I wouldn’t say I have any evidence to support that – it’s not a specific area we’ve looked at. It’s an interesting area – you’d think there might be some correlation between people who loosely manage their affairs.” [5]

“No, but you could be onto something – this is worth exploring in more than a phishing sense, from a consumer psychology perspective I find the question very interesting.” [6]

[6] did however add that all personality types ought to be able to benefit from anti-phishing education. [5] linked the question into that of responsibility, which is explored in a different code.

“What we have done is studies with user groups with customers to test their attitudes towards security and there is a lot of evidence to suggest that customers think that security is the bank’s problem. Anecdotally you could see that people think that they should just be able to overdraw their accounts and if they are a little bit flippant about that sort of thing they may not securely manage their affairs in general either securely or safely.” [5]

[2] also questioned whether people with more deferential personalities would be more likely to do what they are told by phishing emails, something that could link back to the discussion about the West Point Academy phishing trial cited by Wu, Miller and Garfinkel (2006).

“It’s plausible. I don’t know if it’s enough to explain everything. Clearly people who are deferential do fall for that sort of thing.” [2]

[3a] also questioned whether phishing victims are more likely to also be victims of other types of crime, something that will be investigated during the user survey.

4.3.4 Whose responsibility is it to protect the user against phishing?

4.3.4.1 Is security a technical or social issue?

Before deciding on the most effective way of tackling phishing, it seems important to consider whether successful phishing is more than a purely technical failure. The outcome of that decision may in turn guide the discussion of whose responsibility it is to tackle it. If it is a technical issue at heart then perhaps those users who don't especially care about phishing risk (Downs, Holbrook, and Crainor, 2007) may be justified in passing on the responsibility. If it is primarily social, then regulation and governance may help (Wilson and Argles, 2011) (Anderson 2007).

In fact several of the interviewees were keen to stress that phishing is just another manifestation of fraud.

“...it's the same idea as this guy knocking on the door of a little old lady and charging her £10k to fix her roof.” [2]

“I see phishing just as another form of criminals duping humans into doing things...” [3a]

In a sense, the technology is not the issue – the role of the human is.

“In all of these situations in all fraud the human is going to be the weakest point in the chain. Technology will only take you so far...” [3a]

“You've got to put phishing in the context of what it actually is and at the moment it's the weak point in the online world and I think while you still have humans interacting with a bank account and using emails there's still the opportunity for the fraudsters to exploit that interface. I don't think it will ever go away.” [3a]

Even if phishing is overcome, fraudsters will then move onto other types of fraud. The impression given is of the, if not 'stupid', certainly powerless user, either hiding behind technical solutions, which may or may not be effective, or at the mercy of clever fraudsters. As a result society as a whole may have a responsibility to protect users.

“This is where libertarianism meets the black ice of the Internet. Part of me says 'tough, this is what happens'. If you're stupid enough to believe there's \$25m waiting to be airfreighted out of Switzerland if you send \$25k frankly you deserve whatever you get. I'm sure there were the same problems when phones were introduced – it takes a while for mores to settle. But it's the same idea as this guy knocking on the door of a little old lady and charging her £10k to fix her roof. It's all very well for people like me to say caveat emptor but that's not good enough if we want a more civil society. So it's quite a difficult question but I suppose ultimately the answer is education but what actually should be the answer, a working identity infrastructure, is about as remote as it was a decade ago.” [2]

[2] was also quoted earlier about general rates of illiteracy and innumeracy contributing to people falling for phishing – again a failing of society in general.

Yet the discussions in 4.3.2 suggest that user factors are not irrelevant.

4.3.4.2 User responsibility versus bank responsibility

As discussed before, users, in the UK at least, are largely sheltered from the aftermath of phishing, which contributes to the sense that it is not their responsibility to combat it. This is not a legal requirement in the way that the banks are obliged to refund customers hit by credit card fraud (but not debit card fraud) under Section 75 of the Consumer Credit Act 1974

unless they have been grossly negligent (Consumer Direct, 2012) but many of the banks nonetheless do refund customers. There may be a political aspect to this – in the more individualistic North America banks appear less willing to assume responsibility and refund losses.

“I do feel the banks have a responsibility to their customers – they realise that customers are not as able as the banks themselves to recognise fraudulent emails and such like. The way it works in Britain today is that the banks take the hit from the fraud which means that, and in particular in the UK where you have a relatively small number of relatively large banks that are pretty well organised, they’re doing a very good job of watching for phishing emails – there’s been site takedowns and so on. If you compare that to the States where the industry is much more fragmented and you have many more tiny banks, the liability is less clear about who bears the cost of the fraud. I don’t think the consumer is as well protected in the States as opposed to over here.” [1]

In contrast to this, [4] who is based in the US said,

“At the end of the day, it’s a harsh thing to say but it really is the user’s responsibility to be cognizant of what they are doing online. Now yes there is a lot more the industry could be doing in terms of educating and developing technology but you are starting to see some banks have what we call a one strike rule. Royal Bank of Canada was one of the leaders – if you responded to a phishing attack and lost funds from your bank account they would restore them one time only. The second time – tough, you’ve lost your money. That’s because they were unable to manage the loss of funds at the rate they were occurring from their customers’ banks accounts. They felt they had adequately warned the users to not ever give out their PIN numbers or account details and so on in response to email messages. So at the end of the day it’s a tough thing to say but ultimately it is the responsibility of the end user.” [4]

However if phishing is a social problem or even a business problem for banks, then it possibly makes sense to tackle it in the most effective way.

“I do think that having a few well organised, well resourced entities trying to solve this problem is better than trying to distribute the risk.” [1]

In addition it may be difficult to prove that the consumer was negligent.

“The problem there is that the bank does not have the forensic capability of saying that you were daft. Liability is very difficult to track.” [1]

Several of the interviewees pointed out that it made good business sense for banks to assume liability, given that they want to move customers from branch banking to the cheaper online channel.

“I guess at the moment we’re more in a position where we are happy to bear the losses because we want customers to bank with us online, we need to show we have a degree of integrity and therefore we don’t want to be too concerned about the losses as long as they are under an acceptable limit because otherwise online banking and online transactions kind of die in the ditch really.” [3a]

“However there certainly is a lot more the industry could be doing and should be doing and why today you are finding banks and other organisations making restitutions for lost funds because ultimately they understand that they have a role to play. And at the end of the day if you lose all faith and confidence in doing business online and transacting your banking online and your shopping online then at that point a lot of commerce models start to break down and you start to lose business. So I think a lot of the financial institutions and retailers are willing to tolerate some amount of loss online because that loss can be factored into their P and L.” [4]

Interviewees were keen to point out that that didn't let users entirely off the hook.

"But there is an element on the user's part – like if they drive a car, potentially they might cause harm if they don't know what they are doing. There's got to be an element of that. The responsibility on the part of the user can't be just that oh nobody told me there are criminals out there sending emails." [3a]

In fact the general view was that the responsibility should be shared between users and institutions such as banks, with regulators and ISPs also assuming more responsibility.

"...there comes a point where the customer has to have some responsibility as well. If they sign up for online banking we give them all this information about 'we won't ask you for this for type of data in this kind of form, always protect your security credentials, these are your responsibilities.' So in essence it needs to be a bit of a contract between us and the customer – a shared responsibility." [5]

"The consumer has the responsibility in a general sense, but, where the consumer is using a service provided by others then the responsibility shifts more to the service provider. In the case of financial services, companies trade-off between the tolerance of financial loss versus the investment in tooling and other methods such as marketing and education. Regulators and service providers have some accountability here but not enough is happening in this domain.

The consumer has an obligation for basic security and should accept liability for some things, and organisations providing services actually do three things - accept the negligence of consumers, accept a level of loss, and provide extra security defences.

This has to change to a more balanced set of responsibilities. Technical controls for the consumer need to advance and be simplified, the social awareness needs to rise, and to deliver improved regulation of Internet service providers/content ownership. Education clearly raises awareness, and could have a significant impact without such rapid advancements in technology. [6]

[3b] also indicated that ISPs could be more active, even if they leave the ultimate decision to the user.

"...making sure that if the ISPs are aware that the site is malicious they do inform the consumer that the site they are going to link on is potentially malicious and then leaving the decision up to the consumer." [3b]

He did however make the point that currently, that is not the responsibility of the ISP although this may change, particularly if current government plans in the draft Communications Bill for ISPs to monitor all traffic come to fruition (BBC, 2012).

"We know that ISPs are in a bit of a predicament – they don't necessarily monitor the traffic because that's not really their responsibility, they are just responsible for providing the infrastructure but if going forward they are going to be expected to monitor the traffic then there are resource implications." [3b]

4.3.5 How do users react to existing anti-phishing methods?

4.3.5.1 Attitude to security

It seems reasonable to assume users who care about remaining safe online and protecting their financial data may behave differently to those who don't. Some research discussed in the literature review suggests that users don't actually care that much about their online

security (Downs, Holbrook, and Crainor, 2007). The interviewees also seemed to think that people find it hard to take online security seriously, a topic that will be further explored in a separate code.

“Clearly the threat is less real in the cyberworld for the average consumer. I think people are much more casual.” [1]

Potentially this could be explained by a lack of real world consequences for the users as, in the UK at least, most banks will refund losses incurred through phishing, even though the Consumer Credit Act only obliges them to refund credit card losses.

Not only do they not feel pain but some users resent protective measures that may get in the way of them carrying out tasks online.

“...when Barclays introduced its 2FA device, there was vitriol aimed at them on money saving forums for doing the right thing. There was a complete lack of comprehension that it was designed to protect them rather than make their life difficult.” [1]

Indeed, without user interest in protecting themselves, technical protection measures may achieve little.

“Technology will only take you so far – for example you can build an antivirus to protect your computer but if like most people when once a month it says ‘do you want to update your antivirus’ you click the remind me later button because you don’t want to be hindered by it going through its process. It’s ultimately the person that’s causing their own downfall.” [3a]

Although some but not all of the experts felt that younger users might be more aware of risks, there was also the feeling that younger users did not care about privacy online in any real sense, something that could create vulnerability to phishers.

“I also get very concerned about how people treat their personal information on things like social websites. I’ve got my kids absolutely locked down and heavily monitored. I’ve shown them what sort of information is almost available to the public and talked to them about what that information can be used for. It’s a powerful message. And I don’t think that these sites do enough – their security settings are kind of hidden and they don’t talk at a high level about security at all.” [5]

“Their privacy bar is set much lower than mine so we need to give them the tools so they understand that their privacy and security is important and they actually apply it because their automatic mode of operation will be not to.” [1]

There was nevertheless general agreement that educating users while they were young about the dangers of phishing would be a good thing, a topic that was further explored in education related codes.

“Stuff like that needs to be injected into our psyche at an early age. We probably need to forget about trying to train people like you and me and just make sure that the kids that come out of school have a better awareness of online security, particularly because they are living so much more of their lives online.” [1]

Sometimes however attitudes swing from not caring to over-concern, a switch which could also be based on a lack of understanding of the risks or might be a result of media coverage.

“Then they hear the horror stories that are put out on the media about this or that site and they automatically clam up and start questioning everything. It’s not unusual for us to get questions from members of the public saying ‘we’ve just been told about this particular product they’re offering me – I don’t believe it actually exists. Is it not a bit of scam software?’ Well no, it’s legitimate so they’ve gone completely the other way. To add on top of that fraudsters capitalise on this by using things like scareware.” [3a]

4.3.5.2 How users decide whether sites or emails are genuine or not

Some of the research cited in the literature review examined what users looked out for when trying to determine whether a website or email was genuine or not, i.e. the process of mutual authentication (Furnell, 2007). As the previous discussion of code 4.3.3.1 suggests, in fact users may not be aware enough or care enough or just be too focused on their main task to carry out that process at all.

At most they depend on gut feeling, or at best obvious giveaways like spelling mistakes, particularly since, as discussed above, there is little to lose from being wrong.

“I don’t believe people consider this unless a site is so obviously a fake. When it is obvious, the level of understanding to know what to check is very thinly spread across the consumer base.” [6]

“How do I know if it’s real or not? I don’t. Do I care? Not especially as I use my credit card to buy things so if they do turn out to be mountebanks of the first order, it doesn’t really matter – it’s Barclays’ problem, not mine.” [2]

In addition, as will be discussed later, some phishers are becoming more skilled in avoiding obvious giveaways.

“Traditionally they’ve been told to look out for bad graphics and bad language. Basically anything dodgy. I think that’s not so much the case now. I’ve seen some very good quality sites and phishing sites just basically scrape images and text off ours, with a small change to direct the customer to give the information the fraudster wants. So it’s difficult.” [5]

When users don’t know what to look out for, often they depend on the purported source of the email or the certificate to decide whether to proceed. Unfortunately that can mean little to some users.

“That would suggest the solution isn’t finding a way of verifying who [...] is, it’s finding a set of trusted intermediaries the customer can understand and right now that doesn’t work because the trusted intermediaries at the moment are meaningless to the customer. It’s things like Verisign and look for this little tick. Probably in the longer term it has to be consumer facing. That sort of points towards people like retailers – people who have brands that customers understand.” [2]

In the absence of a proper mental framework for deciding what to do, they tend to believe what they are told.

“I think they genuinely believe what is being said to them. People are so busy and we can give them as much information and advice as possible about looking for secure browsers, checking urls, and people don’t, they just barge straight on through.” [3a]

New technology may even make things worse. Although, as will be discussed later, the mobile phone may present a partial solution to the phishing problem, it can also make things harder for the user.

“More and more customers are using different types of pad devices or mobiles to access our sites and if you look at the browser bar on that it’s a very small space so it’s getting easier on the mobile platform for a fraudster to spoof our web address. There is actually evidence to suggest that customers are more likely to respond to a phishing email on their mobile device than they are on their desktop.” [5]

4.3.5.3 Technical means of combating phishing

The prior work identified in the literature review largely focused on technical solutions to phishing that in some way involve the user i.e. filtering systems linked to toolbars of various sorts (Wilson and Argles, 2011) (Wu, Miller, and Garfinkel, 2006). In fact the technical solutions discussed by the interviewees cut the user out of the equation either by insuring they don’t receive the emails at all or through site take-downs.

“I think today that technology is saving everybody from a lot of pain. There’s immediate response to emails on behalf of the large retail banks – they put a stop to that instantly.” [1]

In the UK in particular, this sort of approach is facilitated by the structure of the banking sector. As mentioned in 4.3.4 the industry is structured somewhat differently in North America.

“...in the UK where you have a relatively small number of relatively large banks that are pretty well organised, they’re doing a very good job of watching for phishing emails – there’s been site take-downs and so on.” [1]

“We take a very strong line on that and we’ve been quite aggressive in detection of phishing sites – we spend quite a lot of money on it, through different technologies – logo matching, keyword matching and a number of different feeds. We work with an external partner on that. We’ve got one of the industry leading performances on speed to take down phishing sites.” [5]

Two of the interviewees, [2] and [4], were very much in favour of working on technology solutions as a priority.

“I’m a technological optimist around these sorts of things so I imagine that we can.” [2]

“I candidly have no interest in the average user’s perspective on phishing [laughs]. It’s a problem that can be solved with technology. Ironically it can be solved by technology that is available today.” [4]

“My personal belief is that the challenges we see are not insurmountable... All the building blocks are available today. I want to stress that. There’s no new technology required. Educational awareness itself will not suffice. We need to rely on technology. It’s just a matter of getting on, knocking some heads together and solving the problem. [4]

Both of them mentioned an identity infrastructure as the solution, although neither of them saw it happening in the short term.

“...there are people who are out there who are smart enough to realise that identity is the next big thing. It’s not just people like me banging on about how identity is the new money. It is actually real.” [2]

“...what actually should be the answer, a working identity infrastructure, is about as remote as it was a decade ago.” [2]

“The reality is that should all the major players come together, they could come up with an online identity system which is used by everyone which would drastically reduce the likelihood that attacks would take place. However commercial interests will prevent that from happening and to a certain extent legislative interests as well. You would find it difficult to roll out a single worldwide identity system or metasystem without legislators from different countries weighing in and saying ‘whoah, we’ve got to define identity with national legislation, we make it look like this’. However from a purely technical standpoint it could be solved very quickly, very fast and you would dramatically reduce the likelihood that phishing attacks would be successful, especially when you combine it with two factor authentication. If the industry and government were willing to make the investment and if you were willing to overcome certain civil liberty issues you could virtually eliminate phishing along with a significant amount of identity fraud.” [4]

Even that might not fully deter phishers though.

“You still have a point of entry somewhere and I’ve seen the most sophisticated authentication and verification systems just being social engineered so I don’t think that that gets round the problem completely.” [5]

Another potential technical solution is using mobile phones, although as has been explained by [5] they can cause problems of their own. Two factor authentication could also help although it is not always clear that banks really understand what this is.

“I would say lots of people are looking towards the mobile phone for the way forward as a way of breaking the logjam. It’s going to be easier to secure the mobile handset. You’ll get used to that – you’ll go to log in to the bank and a little message will pop up on your phone or you go to buy something online and you get a message on your phone or you want to access the intranet at work and a little code appears on your phone.” [2]

“I think that with respect to the user or consumer, the increasing processing power of smart-phones means you will start to see solutions that are smart-phone based so as long as you’ve got your phone, you can prove that you own that phone, that phone becomes an authentication token of one form or another.” [4]

“Banks have to move away from usernames and passwords and Bank of Scotland – 2FA is something you have and something you know, or have and are, or know and are – out of the three types of credential – they ask me to type in username and password and then another password. That’s not 2FA and the chances are that the user has written down that information and put it in their wallet and that means that if the wallet is stolen someone has access to the bank account.” [4]

Technology can however only do so much, as will be discussed in the next code section.

“There’s already different pieces of technology in use by banks and other stakeholders designed to stop users falling prey to phishing attacks and other online fraud but it all hinges on the user’s susceptibility to being tricked and social engineered. The technology can only do so much and if the user’s online attitude isn’t sufficient, they will fall victim.” [3b]

In the end, technology might need to be combined with a risk management based approach to the Internet. [4] felt that some activities simply carry too much risk to be done online.

“You’ve also got to move to a more risk based approach, and I hate to say that because I don’t think anyone manages risk appropriately but a risk based approach means you don’t let people do certain things online. For example just last week I sold a whole bunch of stock by typing into my brokerage account just a username and password then I cashed the proceeds from my brokerage account and transferred them to my bank account again just using my username and password. Had that been stolen I could sold any stock and sent it anywhere in

the world and I would have lost out. We're talking a significant amount of money here, not just a few hundred dollars yet there are no protections in place to guarantee I was who I said I was other than a username and password. Had I lost that or I'd been phished someone could have taken a significant amount of money from me." [4]

4.3.5.4 Anti-phishing education

There are clearly questions outstanding about the efficacy of anti-phishing education (Kumaraguru, Sheng, Acquisti, Cranor, and Hong, 2007), (Wilson and Argles, 2011), (Anandpara, Dingman, Jakobsson, Liu, and Roinestad, 2007), (Schneier, 2006) and some of these questions were echoed by the interviewees.

Despite the technical measures discussed above, education is still seen as important.

"The user problem isn't going to away overnight so it's important to educate the end user and give them as many tools as you possibly think they can mentally consume." [1]

Several of the interviewees stressed that anti-phishing education should start at a young age. This could fit well with teaching in schools about online security and privacy and avoiding cyber-bullying.

"Stuff like that needs to be injected into our psyche at an early age." [1]

"...if you look at the curriculum in schools we're seeing more and more that the national curriculum is touching on how to use online environments and being more comfortable using the Internet and social media... that's the way forward really, educating the new generation." [3b]

"At the end of the day you've got to have an informed and educated user base and a lot more can be done through primary and secondary education." [4]

Educational materials also need to be accessible and easy to understand although that can be somewhat counterproductive in the view of [3b]. [3a] mentions a promotional video from a consultancy security practice. Other similar materials include those in the SANS Securing the Human programme, aimed at corporate security awareness programmes (Security Awareness for the 21st Century).

"Also, when I was younger we had the Green Cross Code on TV and quaint public information films – something like that might work? There's a Deloitte's video promoting their security practice, it's basically like an episode of Spooks, not tech heavy, just a story of how an organisation gets compromised and lose customer information and it really gets the message over. Something dramatised like that would resonate much better than warnings about checking mutual authentication – people don't get that or understand it." [1]

"One of the things we've done when we've done our campaigns is trying to strike a balance between the messaging and the trying to get the message across so people understand what we are trying to say and how comprehensive message is at the same time. So to really make people understand what they are getting themselves into you need to give them some technical messages ... There's always more we want to say but we know certain parts of the community or consumers won't understand that." [3b]

One of the studies reviewed in the literature review found that social context affected how likely people were to open phishing emails (Jagatic, Johnson, Jakobsson, and Menczer, 2007). Social context also seems to come into play with regards to disseminating anti-phishing messages.

“In my experience though people are becoming more and more aware of the dangers of the online environment and people are sharing that information with their friends. We run a consumer awareness website where members of the public are able to email in any queries that they have around phishing and malware and a lot of the time we get emails that say a friend told them that this could be a scam and I just wanted to confirm it with yourselves. Or is this a 419 scam? A friend has convinced me it is and I thought that it isn't or that type of things. Yeah certainly we are aware that people do shared that type of information with each other and do sometimes look to their peers whether something they get involved with is legit or not.” [3b]

“I think word of mouth is very powerful. If one person gets a message and they tell two – that viral spread is the most powerful thing you can get. I would say we're still in the exploration phase of engaging customers with social media. It's still too new to see how that picks up. We've got Twitter accounts and things and we're on Facebook – to see how we can use those as channels for fielding customer concerns and feeding educational messages to them. Again it's hard because banking is pretty boring but it's about a means to an end.” [5]

[5] also described an example of an embedded education method (Kumaraguru, Rhee et al., 2007).

“One of the things we do is that when we take down a site, at the point at which the customer clicks through to a point that we have taken down we redirect them to the APWG¹ education page so they can see what they've done wrong.” [5]

Other initiatives from his bank included information over different channels and free software.

“There's general information – in hard copy in branches, information on our website about how to stay safe online. Some of the technology we use, we give away to the customer to protect against phishing. We give away a product called Trusteer Rapport and we let customers install that. It's able to know as well when a customer is on our genuine site and if they try and put their credentials into a phishing site they get a warning. [5]

Rival [6] also described different channels.

“The majority of education is via the postal route, product documentation, helpdesks and support operations.” [6]

On the other hand [5] did warn that the business reasoning discussed in the section on responsibility could affect educational efforts.

“...our business proposition people are treading that fine line between keeping people secure and not scaring them off the channel. You are statistically very, very unlikely to suffer online fraud despite all the hype around it. It's a tiny minority of our customers that ever experience it. So there is an argument that says don't go too over the top about some of the negative side of it.” [5]

[5] also felt that more industry co-operation would make education efforts more effective.

“It's really hard getting things co-ordinated but I still think we could do more at industry level. It's a problem that has persisted for years and it's not going away. It spikes around organisations, sometimes we get hit more, sometimes [other bank] gets hit more but the general levels are still increasing. There is an argument that it is just such a pain in the neck

¹ Anti Phishing Working Group

that if we all came together and did some TV advertising or just something higher profile – you know, this is the stuff that can go wrong.” [5]

“I think we work as an industry. It would be hard to measure so we work as an industry against fraud. It’s not a competitive thing and if we started getting into that kind of space then we’d be closing our doors on conversations with each other. And part of fighting it is sharing some of the M.O.s – sharing what we know about fraudsters. I still think it’s better to work together than separately.” [5]

4.3.5.5 User reaction to anti-phishing education

While some studies, such as those from the research group at Carnegie Mellon quoted extensively in the literature review, found that anti-phishing education was effective, the interviewees were less certain. Even measuring effectiveness was seen as problematic.

“It’s quite difficult to measure really. How do you measure whether – it takes time to tell whether a user’s attitudes have changed. We know that from our experience although the number of phishing attacks has increased the number of users falling victim to them hasn’t necessarily followed that trend. Attributing that to education campaigns or to better technology is difficult to say. It’s probably a combination of both – better technology from the ISPs, from the banks and from online infrastructure providers and educational awareness from the industry over a number of years that you see slowly seeping into people’s mindsets. A combination of both but it’s hard to find a scientific measurement for it really...” [3b]

Others saw it as ineffectual, and not even something users were aware of.

“Candidly, I think people are most likely to learn from having a bad experience, having something bad happen to them. I think that research would show that if you target all of your customers with an anti-phishing campaign the number of people who would fall victim to phishing over the next 12 months would remain roughly the same as if you had never even conducted the campaign. That’s been borne out by the internal work we’ve done at [large technology employer] where we did the anti-phishing campaign and yet the number of people who fell victim were roughly the same as the year before when we didn’t do a campaign.” [4]

“Unless it’s happening to you... You’re going to log into your bank account or you’re going to a website and there’s a message saying ‘report phishing here’ or ‘latest scams’ or something like that and you want to pay for your gas bill, you aren’t going to stop and look at any of that because you are just going to get in there, do what you need to do and get on with your life.” [5]

“Unless they’ve suffered previous losses, I don’t think they are bothered unless there is a genuine interest in the topic.” [6]

“They’re not aware of it. If I’m not aware of it, your average consumer will be utterly unaware of it.” [1]

4.3.5.6 Technical solutions versus user education

The interviewees therefore appeared to think that both technology approaches and educational campaigns had problems, both largely because of user weaknesses but also because likely technology solutions were slow in being taken up.

However education alone could not be enough to beat phishing.

“The user problem isn’t going to away overnight so it’s important to educate the end user and give them as many tools as you possibly think they can mentally consume. I think today that technology is saving everybody from a lot of pain. There’s immediate response to emails on behalf of the large retail banks – they put a stop to that instantly... All the stuff about user education – that’s never going to be a hard, definite, right we’ve stopped that one. You’re always going to have people inadvertently or deliberately clicking, thinking it’s their bank.” [1]

“It’s two pronged but my experience is that you can only go so far in education. We do work at industry level through UK Payments and there’s a viral web campaign going on just now called ‘the devil is in your details’ to try and encourage customers to just think about where and when they give away their information. So we will continue to go on with that but... we set up timers on certain pages to see how long customers spent on them. We found that whenever we were giving them information and it was preventing them getting at the transaction they wanted to do, it was really just how quick they could hit the next button.” [5]

“So education is difficult because it’s hard to grab people’s attention. It’s easy to teach people about fraud and protecting themselves and they listen to you when there’s a teachable point of view and they’ve suffered from fraud but just in the day to day business it’s really hard to get some of those messages through and that’s why we need to have those technical options open to us as well.” [5]

However for at least two of the interviewees technology alone is not enough either, for reasons already explored and because widespread changes are needed.

“So it’s quite a difficult question but I suppose ultimately the answer is education but what actually should be the answer, a working identity infrastructure, is about as remote as it was a decade ago.” [2]

“Whether or not you can actually address that behaviour through email campaigns and educational awareness I’m not sure. I think technology has a large part to play in solving the problem and there are a number of technologies that would help including single sign on. So you sign on once and you never have to sign on again. The industry just has to get together and get its act together...” [4]

The answer therefore seemed to be a combination of the two.

4.3.6 How can existing anti-phishing methods be improved?

4.3.6.1 Problems with technical solutions

In addition to the problems with technology such as false positives flagged up in the literature review (Wilson and Argles, 2011), technical solutions are also hampered by their human interfaces, as [3b]’s comment in the previous code shows. His colleague [3a] agreed with him.

“In all of these situations in all fraud the human is going to be the weakest point in the chain. Technology will only take you so far – for example you can build an antivirus to protect your computer but if like most people when once a month it says ‘do you want to update your antivirus’ you click the remind me later button because you don’t want to be hindered by it going through its process.” [3a]

As [4] described in 4.3.2.7, some of the technical indicators offer more confusion than reassurance.

“So we’ve trained users to look out for these visual cues that at the end of the day mean nothing.” [4]

And as discussed, phishers are continually improving their skills, leaving anti-phishing technology to catch up.

“While innovation in tooling can just about keep up with phishing techniques, the ability for organisations to justify investment and deploy controls will always mean they are at least two steps behind the fraudsters.” [6]

4.3.6.2 Initiatives

In general, the prior work reviewed in the literature review covered controlled experiments about phishing. Although [3a] and [3b] showed some knowledge of academic work in this area, the interviews were designed more to find out about their knowledge of and views on real world initiatives. Given the views expressed above about how phishing should be fought, what initiatives were they actually aware of? Much of this information has been discussed in previous codes but there was also some discussion of co-ordinated efforts.

As previously discussed, the structure of the UK banking industry appears to make co-ordinated efforts more effective than in some other countries.

“Each institution that we work with has their own campaigns and we do joint industry campaigns where you look at working with radio, newspaper, TV and various sorts of media outlets. We work with law enforcement and other sorts of government agencies such as the National Fraud Authority and it’s all about doing campaigns and educating with awareness around what phishing is and looking out for the telltale signs. Each bank has their own security page where you can go and look for information about signs of a phishing attack and what phishing is and what to do if they have fallen victim. So lots of educational awareness campaigns that we do and we do them on a regular basis.

There’s been work done by the academic community about looking at the behaviours of online users or victims of phishing and we use that to inform our strategies for own campaigns. There’s various consumer websites that members of the public can use again to give them very detailed information around phishing and malware, again how do you spot a genuine email from a fraudulent one.” [3b]

[3b] mentioned law enforcement and went on to call for further involvement from them and from government in general.

“It’s government really – that’s where the work needs to be done at a governmental level. Recently we’ve had law enforcement increase their capabilities so you’ve got subject matter experts, you’ve got the Police Central e- Crime Unit, you’ve the Serious Organised Crime Unit, you’ve got various other agencies being set up such as the NFA and they specialise just in the online environment protecting the consumers so that’s made a massive effect... But I think that at a higher level there needs to be more work done from the government to start mandating and start regulating the area a bit more.” [3b]

[4] made the point that in general anti-phishing initiatives tend to concentrate on financial sector attacks and that there are other sectors where there might be risks (although this point is unlikely to apply in the UK), a timely message given the recent attack on Utah Medicaid records (Infosecurity Magazine, 2012).

“Most anti-phishing efforts I’m aware of in the industry in the real world, come from the likes of banks... I’ve never seen an educational awareness campaign by, say, the online healthcare industry. The use of electronic health records is exploding and you are seeing more and more doctors tracking their patients online. Certainly my doctors offer the same. I’ve never seen a circular from my doctor saying ‘don’t type in your user name or password’ or ‘be careful, somebody might be trying to phish for your medical data or commit medical fraud by

impersonating you to receive services they are not otherwise eligible for'. I've only ever seen financial services messages." [4]

[4] also discussed efforts to protect against spearphishing within organisations.

"The sole exception to that is in companies that are themselves likely to be breached as part of economic espionage or because they are a target for one reason or another. So internally we have educational awareness campaigns that say 'you may be subject to a phishing attack because of who you are or what you do with the company. You've got access to source code – be aware that this can access the company. So I've seen these kinds of educational awareness campaigns in [large technology employer]. I'm aware that our counterparts in the industry do it as do some other potentially rich targets such as defence contractors, aerospace manufacturing, computer manufacturing, such as Intel – I know they do something similar. So you do see occasional awareness campaigns but they are tied to the organisation and not to any industry sector or online commerce. I've got to tell you, by the way and I can't go into details, but we had a very prominent campaign internally warning people of the dangers of phishing and then they ran a simulated phishing attack internally and a significant number of people fell victim." [4]

4.3.6.3 Future of phishing

Given these efforts and views, how did the interviewees see phishing and the fight against it developing in the future? Both [2] and [4] mentioned the mobile phone as an authentication device as a way forward, although [5] pointed out that it is also part of the problem.

There was a general view that it would only mutate rather than go away, given that fraud mutates.

"I think we'll continue to see it. You've got to put phishing in the context of what it actually is and at the moment it's the weak point in the online world and I think while you still have humans interacting with a bank account and using emails there's still the opportunity for the fraudsters to exploit that interface. I don't think it will ever go away. I think it will continue to be seen as a route in for the fraudsters. Banks will get better at protecting – and they are actually very good at protecting per se – you may well get better filtering through the ISPs and better education. But I think it will just continue – you will always see humans being lied to by fraudsters." [3a]

His colleague [3b] felt that a change would only occur when the problem became one for the government to tackle.

"...I think that as government puts more focus on the online environment so that as government services such as HMRC, benefit system, NHS records, as they go online that becomes a common way of accessing your public services, that's when you'll see real change. You'll have government influence on what ISPs and what email providers and security – they're going to be informing the strategies..." [3b]

[1] also felt that education and technology would make less of a difference than government and law enforcement tackling the root of the problem.

"My understanding is that a lot of the Serious Organised Crime Agency's efforts were around making it harder to get the sites set up in the first place, trying to get either legislation or common practice frameworks in place so there was a certain bar that had to be passed before you could register a domain. So the long term strategic thing is that that is a good thing to do. In the near term I don't think there is going to be substantive change influenced by anything other than a major gang take down so efforts should be focused on that. I don't think we're going to improve user behaviour, I don't think we're going to improve technology on banking sites or on anti spam products, which went downhill after Google changed their policy recently, so none

of that is going to change... While there is long tail activity, there is probably a small number of highly orchestrated actors and if law enforcement can go after them and take them out then we can see the volume of these attacks dropping by double digits.” [1]

[6] does see a change coming over the long term.

“Changes to the way in which payments are made, and the way in which authentication is performed, over the next 10 years will significantly change the manner in which payments fraud and phishing are executed. I think this will reduce the current fraud in the traditional online channel, and ultimately the relationship between eCommerce and payments will change resulting in traditional phishing becoming proportionally irrelevant. We are all set for the consumerisation of authentication – think Identity Card, BankID, one day passwords become redundant and online person fraud becomes much harder. In that case, what you phish for changes considerably. [6]

In general those changes were seen as a move on the part of the fraudsters towards spearphishing and malware.

“We’ve seen more sophisticated attacks in the online space – really advanced malware and fraudsters attempting to manipulate what the customer sees on-screen and trick them into giving their security away so there’s programs that make transactions in the background and without the customer even knowing. Phishing in itself I don’t see going away any time soon. What we do see is – and there’s a perception across the industry that there’s a lot more compromised credentials out there than the fraudsters have used – so I think they are getting more selective and I think the thing that probably concerns me just as much as the general phishing is the stuff that’s more targeted – spearphishing. So if you take that into the corporate space, we’ve seen examples in general industry – advanced persistent threats and malware being used in unison to get into company networks and things like that. There will always be a technique of tricking customers into opening a link or clicking a pdf – that’s not going away any time soon.” [5]

In general then the overall mood appeared to be pessimistic, apart from ‘technical optimist’ [2], who believed that there would eventually be a technology fix and quoted TS Eliot in support of his views.

“The mobile has changed what’s going on in that space and delivered some new possibilities. You’ll get different responses from other people. I’m a technological optimist around these sorts of things so I imagine that we can.
As TS Eliot said once, “They constantly try to escape
From the darkness outside and within
By dreaming of systems so perfect that no one will need to be good” [2]

4.3.6.4 Improved responses – interviewee recommendations

The interviews did generate a list of suggestions about how phishing could be better tackled. These should not be viewed as endorsed by all the interviewees, nor as a formal outcome of the dissertation. They are presented for reference.

- Anti phishing education should be started early and should be engaging and easy to understand.
- Industry co-operation on educational efforts is beneficial.
- There is a need for more government and law enforcement involvement with an emphasis on arrests.
- Users could be liable for a fine or excess payment as a way of motivating them to take care (another type of nudge).

- Well known consumer brands should act as trusted intermediaries so as to be understandable to the user.
- Banks and other Internet bodies need to be more consistent in following their own security practices when interfacing with customers.
- There needs to be more clarity around what security indicators mean and how reliable they are.
- DNS security could be fully implemented in operating systems.
- PKI certificate authorities should be more careful about who they issue certificates to.
- A major identity infrastructure should be implemented.
- Mobile phones should be used for authentication.
- More effective Internet governance is needed.
- A risk management based approach should be taken to what can be done online.
- Users need to pay more attention to online privacy.
- More responsibility needs to be passed to regulators and ISPs.

Out of these recommendations, the recommendations about DNS security, about security indicators, about law enforcement involvement and about making education more engaging somewhat overlap with recommendations made as a result of the expert interviews carried out in Sheng, Kumaraguru, Acquisti, Cranor, and Hong, (2009) although their study was wider ranging with more interviews, 31 in total, but no user involvement.

4.4 Chapter conclusion

Although some of the interviewees had doubts about how able users are to avoid phishing, they concluded that a combination of education, technical action (from the banking and technology industries, not users) and law enforcement action was the key to beating phishing. They felt that people behave differently online and are more trusting and that they were best educated young if they were to become more aware about online crime. There was a general air of pessimism about ever being able to beat phishing, with fraud sure to mutate elsewhere as soon as it is mitigated in one area.

5 Findings from the user survey

5.1 Introduction

This chapter presents an analysis of the results of the online user survey. The questionnaire remained online for 10 days in March 2012 and was completed 354 times. The system used did not store data relating to visitors who chose not to answer any questions. No question in the survey was compulsory, in order to encourage participation.

The survey contained 22 questions broken down into four thematic sections. It started with four introductory closed questions about demographic factors for filtering purposes. There was then a section of closed questions about participant perceptions of security followed by a section of closed questions about learning to stay safe online and then a final section about attitudes to and strategies for staying safe, which comprised open and closed questions. Each section except the introductory section was followed by an open question to allow the participants to record any thoughts they had about their answers.

The questions map onto the research questions, as listed previously but as discussed in chapter three, some of the more subtle issues had to be omitted for the sake of clarity and accessibility.

This chapter focuses on the most important results and their implications, broken down by theme. A fuller version of the results, along with a full question list, is available in appendix 5. It also filters the results using a selection of user profiles or personas, based on findings from the literature review and expert interviews and will examine how their attitudes and behaviours concerning phishing differ. Where differences are described as significant, this reflects statistical significance, measured using a Chi-square test (Chi-square test, 2005).

5.2 Results of the filtering questions

The questions in this section asked about age, gender, level of knowledge of computing and speed of decision making. Speed of decision making maps onto the research question about personality factors whereas the others were included for filtering purposes.

Age was a factor that was brought up in the expert interviews, although it did not feature in depth in the literature review. The results largely reflect the profile of people to whom the survey was advertised – students and professionals, with more than half of the sample being under 35. Splitting by gender however shows some differences, with women more heavily represented in the 18-25 and 26-35 age groups and men in all the other age groups. The low number of older participants, 26 who were over 55 years old out of the total of 354, made meaningful comparisons between age extremes difficult.

Question 2, about gender, was included primarily for filtering purposes. Neither the expert interviews nor the literature review picked up gender as a significant factor. The lack of balance in replies (nearly 70% female) was unexpected especially given that the forums on which the survey was promoted should have produced on average slightly more male than female replies. Despite this, close analysis of the data in this chapter showed few significant differences between men and women.

Nonetheless other answers are presented in their raw form and adjusted for gender where possible to assume an equal split. For the purposes of simplification and because the number of female respondents was so much larger, anyone identifying as neither male nor female has been analysed with female replies. It was not possible to fully adjust the data for gender balance for answers where cross tabulation was occurring, nor in discussions of answers to open questions.

Question 3 about levels of knowledge was included to allow for examination of whether greater computing knowledge correlates with greater security awareness. There were very few replies from people with little to no knowledge of computing with the proportions reflecting the way in which the survey was advertised online only. The bulk of replies came from people with medium low or medium high levels of knowledge. Around 14% (21% adjusted) were experts. It should be stressed that this information is, as with all the survey questions, self reported and does not necessarily correspond with successful security skills and strategies, as will be shown later in the chapter. Accessing the experience of more people with very low experience of computer use or very restricted usage would require a different form of research.

Question 4, about speed of decision making, related to the question of impulsiveness raised in the literature review (Pattinson, Jerram, Parsons, McCormac, and Butavicius, 2012) and maps onto the research question of personality factors. The result by itself is not of interest, although it is possible that people who are less impulsive may have bookmarked the survey for later and then forgotten about it. It should be noted that self report on decision speed is not a scientific way of measuring impulsiveness but administering Frederick's Cognitive Reflection Test (2005) was not considered practical in the context of this survey and the question was selected as an approximate proxy with the view to investigating further if marked results were obtained.

Overall, the sample skewed female, young, with middling levels of computing knowledge and medium fast decision making.

5.3 Perceptions of security

In this section participants were asked about how concerned they were about online crime and for comparison how concerned they were about physical world crime. They were then asked if they had been phishing victims and for comparison whether they had been victims of real world crime. Finally they were asked if they read security messages from their bank while banking online and they were given a chance to comment about these questions. These questions map onto the research questions about online and offline behaviour and attitudes to anti-phishing methods.

Respondents were neither overwhelmingly very worried nor unworried about online crime although the number of 'very low worried' were more than double the number of 'very high worried'. Gender differences were not statistically significant. Also there was little variation across age groups in levels of concern.

However level of computing knowledge did affect level of concern. As level of knowledge of computing grows, levels of being either 'medium high worried' or 'very high worried' drop and levels of being 'medium low worried' or 'very low worried' rise, reflecting either greater confidence in their ability to spot scams or possibly the point made by Egelman, Cranor, and Hong, (2008) about over confidence. Some of the comments in the open question in this section reflected this.

As a savvy user, I keep a close eye out for scams. This makes me feel relatively secure about avoiding cyber crime. - **female, 26-35, expert**

Don't always read security messages since I have a BSc in computer forensics with a high amount of Security modules so am aware of the threats. – **male, 18-25, medium high expertise**

Others feel protected by industry guarantees to refund losses.

i work in finance and use online banking and other online financial services on a regular basis. i feel that i am protected as a consumer by credit card companies and banks who will take the loss in the event of an unauthorized transaction. – **male, 26-35, medium high expertise**

It was expected that, based on expert interviewee responses, that levels of concern about offline crime would be higher than those about online crime, reflecting the theme of an online life without responsibility and the lack of physical violence in online crime. In fact the reverse was true.

burglary - easy to know I've locked the doors. Computer fraud - less easy to be certain so more concerned – **male, 56-65, medium high expertise**

Level of concern	Online crime	Offline crime
very low	18.61%	22.81%
medium low	40%	48.89%
medium high	32.93%	21.93%
very high	8.45%	6.36%

Table 1 Comparison between levels of concern about online and offline crime (adjusted)

The difference between the two levels of concern is statistically significant. In addition, because most of the respondents who were very worried about physical world crime were also very worried about online crime but the converse was not anywhere near as marked, it seems like online crime worries some people who do not otherwise worry much about crime. Analysis of answers to open questions showed a general lack of understanding of what phishing is, suggesting perhaps that lack of knowledge can breed fear.

At nearly 10% of the population the number of respondents who had lost money through phishing was very much higher than would be expected, perhaps because the survey attracted people with an interest in the topic. Figures from anti-phishing solution provider Trusteer from 2009, based on data gathered over a 3 month period through their anti-phishing plugin Rapport from bank customers in Europe and the US who had installed Rapport, suggest that 0.47% of an average bank's customers become victims every year (Trusteer, 2009). It is possible though that data collected from Rapport users excludes those who lack the concern about phishing necessary to install Rapport and therefore is not fully representative.

Ten out of the 354 respondents of this survey (3%) stated that they had installed Rapport or other bank provided software. Trusteer reports a user base of 28.6 million 'desktops' (Boodaei, 2011). There are approximately 19 million households in the UK (Office for National Statistics, 2011) with Internet access and at least 70 million in the US (Internet World Stats, 2011) and at least 28 million in Canada (Internet World Stats, 2011) giving Trusteer an approximate maximum coverage of 24% of users, assuming a primarily UK and North American user base so the reported figure in this survey is low. This may be partly explicable by the skew towards younger survey participants, however of the respondents

who did download Rapport, 60% were in the 18-25 age group. With one exception they also had medium high or expert levels of knowledge and the gender split reflected the overall sample. It is possible that people without good levels of computing knowledge might not feel confident about successfully installing Rapport.

Not surprisingly people who have lost money to phishing were significantly more concerned about online crime. This suggests that the comment made by two of the expert interviewees, that people learn from experience, may be correct. However previous victims had a reasonably even age spread, not supporting the opposing suppositions from [3a] and [3b] about how age might affect likelihood of being deceived. There was also a slightly higher proportion of self described experts amongst the victims than amongst the general sample.

A very slightly higher proportion of very quick decision makers have fallen victim to phishing compared to other types of decision maker but not statistically significantly so, so there is no support for Pattinson et al.'s (2012) work on impulsiveness at this stage.

The answer to question 9 about whether people stop to read security messages while carrying out online banking tasks may bear out information gathered in the literature review and the expert interviews about security not being viewed as a primary task. Considerably over half of the respondents, 65.95%, sometimes/always do not stop to read security messages. It also bears out the experience of one of the banking interviewees who stated that his bank had carried out research which showed that online banking customers clicked past security messages as quickly as possible.

It is possible there are reasons for this – perhaps people feel that reading a message once or only occasionally is enough. Only 5% claim to never read them. In general propensity to read them declines with levels of concern about online crime but conversely 22.2% of people who never read banking messages have medium high levels of concern about online crime. So this could mean either that non-readers don't care (a much higher proportion took no precautions to protect themselves against phishing than in the general sample) or they feel confident that they know how to protect themselves already (nearly 2/3 of them have medium high or expert levels of knowledge) or that they prefer other channels for education. However cross tabulating with other answers shows that these refuseniks actually prefer to receive anti-phishing messages from banks compared to other channels. It may also suggest that there is something about the way that bank security messages are presented that do not encourage people who may still be interested in their content to read them.

I know that I should read T and Cs but they're never written in an engaging way. I also know the risks of false website but don't really know the warning signs to look out for. – **female, 36-45, medium low expertise, reads messages rarely**

Given that some of the respondents clearly didn't understand what phishing is, perhaps they don't understand the bank messages.

Overall, levels of concern about online crime were higher than expected in the survey sample but that concern does not always translate to reading security messages while carrying out online banking.

5.4 Learning to avoid phishing

In this section respondents were asked whether they had seen anti-phishing educational material, its source, whether they read it, how easy to understand it was and whether they had changed their behaviour because of it. These questions map onto the research questions about attitudes to anti-phishing materials and how to improve them.

Nearly $\frac{3}{4}$ of respondents had seen anti-phishing material. That means that 25.28% of respondents (unadjusted) who are all computer users have no memory of ever seeing any anti-phishing material. While over 73% of people who had seen anti-phishing messages had seen them from their bank, nearly 29% had received them from friends and family, the third most seen source, reinforcing the idea that social context may play a role in promoting anti-phishing education. Women were more than twice as likely as men to have noticed information from friends/family, reflecting popular stereotypes about women being more socially co-operative than men (Balliet, Li, MacFarlan, and van Vugt, 2011). Women were also less likely to have read the material. In fact the percentage of non-readers in both genders was very similar to that of people who never read banking messages but there was actually little overlap with 90% of non-readers of bank messages having read the anti-phishing material and just 6% of non-readers of anti-phishing materials never reading bank messages. The lack of equivalence between the two answers further reinforces the point that many people don't seem to understand what phishing is, reflecting points made by Yu, Nargundkar, and Tiruthani (2008).

However most people (85.75% adjusted) felt that the level of the material was just right and less than 1% found it much too difficult. Yet answers from the open questions suggests that there is a general lack of understanding about what phishing is and how to best protect oneself, so even though people think they find the information easy to understand, it may not be carrying the message across.

Read it lots of places, they all say the same thing, it gets boring! - **male, 56-65, medium high**

Most do not give suitable advice or tips on how to spot or avoid issues. i.e. Checking links go to where the text says...- **male, 26-35, expert**

Yet only 34% of people changed their behaviour as a result of the information, with women statistically significantly more likely to change than men. From the comments, it seems like for many people they were already happy with their existing practices, even when these appear not to be ideal.

I put "no" to 15 because I felt I was already using good online behavior to protect myself. Information i receive advising me on how to protect myself from phishing is never new information for me. – **female, 26-35, expert**

When I said NO reading it didn't change my online behaviour, that is because I was already aware and careful online. – **female, 36-45, medium low expertise**

Information from friends/family was most likely to make people change behaviour whereas information from banks was least likely.

most people do not read any financial documents that arrive at their home or via their online banking. if they hear it from their friend, they will listen. – **male, 26-35, medium high expertise**

Yet when asked about preferred sources of information, official sources like banks were strongly preferred, across all age groups.

I tend to pay more attention to information about phishing/scams from more "trustworthy" sources like the news and my bank. Half of the "scams" one is warned about on social media are urban myths or rare, so I don't think those warnings sink in as well as more serious warnings. – **female, 36-45, medium low expertise**

18-25 year olds were the age group showing the highest level of interest in Facebook and Twitter as channels.

Preferred information source	% of answers adjusted	Men	Women	% of answers not adjusted
Twitter	8.64%	6.93%	10.98%	9.77%
Facebook	24.04%	18.81%	29.27%	26.15%
on my bank website	68.89%	70.30%	67.48%	68.39%
in a letter from my bank	51.58%	49.50%	53.66%	52.59%
in newspapers	32.76%	27.72%	37.80%	35.06%
in magazines	23.63%	18.81%	28.46%	25.86%
Other, please specify:	14.83%	15.84%	13.82%	14.37%

Table 2 Preferred channel for receiving anti-phishing educational material

So, while the majority of respondents had seen anti-phishing materials, and preferred to receive them from official sources, other survey answers suggest that while they thought they understood them, this may not actually be the case and their influence on behaviour is not great.

5.5 Protecting against phishing

In this section, respondents were asked whether they felt they should be refunded by banks for their phishing losses, whether they took measures to protect themselves against phishing, what these were, how they decided whether to click on email links and how they decided if a website was genuine. These map onto the research questions about anti-phishing methods, why people fall for phishing and responsibility.

A statistically significantly large majority of people felt that banks should refund them for phishing losses – this was taken as a proxy for their feelings on whose responsibility it was to protect them. From this, one might expect that a large number of people would take no precautions to protect themselves but only 35% of people claim to take no precautions against phishing and of those a large proportion of people who claimed not to protect themselves against phishing had clear strategies for avoiding phishing emails and fake websites, further pointing to a lack of understanding of what phishing is. This also points to an expectation of shared responsibility.

Many of the answers about bank liability and refunds seem based around the idea that phishing is caused by a breach in bank security. This further implies that not everyone is completely clear exactly what phishing is and how it happens, a point made by some of survey respondents.

On 18, I do think the bank should return the money in some cases if they were at fault, e.g., they had poor security practices that led to the breach. – **female, 26-35, medium low expertise**

Rider on question 18 - I wouldn't expect the bank to refund if I've blatantly broken all the rules of avoiding being phished; it's a different matter, though, if their system has been hacked to email customers and therefore looking legitimate. – **female, 56-65, medium high expertise**

(18) yes for me because I make the effort to thwart phishing attacks.

(18) yes otherwise the banks would be even less secure than they are now.

(18) no for people how have not made an effort to understand phishing attacks.

The banks need to make basic security measures effective eg:

Check the link target in the status bar. If javascript is enabled this is pointless. – **male, 36-45, expert**

There were many other comments of this nature as well as some that somewhat implausibly claimed to have never received a phishing email.

Under-26 year olds are least likely to say they protect themselves of all age groups. People who take precautions against phishing tend to be older, better educated about computing, more concerned about online crime and more likely to read bank security messages. Users of all levels of knowledge except very low are more likely to take precautions against phishing than not, with self described expert users most likely to take precautions. Possibly users with very low knowledge levels do not know how to take precautions, since a majority of users with a very low knowledge of computing were either 'medium high worried' or 'very high worried' about online crime and hence were not complacent about it. This may suggest that they would be more likely to take precautions if they understood how.

The most popular general anti-phishing strategies listed are using trusted sites, looking out for https indicators, not opening unsolicited mail, not clicking on links, typing in urls or using bookmarked links, using spam filters, anti-virus software and firewalls. However even the most popular strategy, anti-virus software, only received 39 mentions out of a possible population of 354. Out of the 217 people who commented, most listed more than one strategy.

One common theme was that sticking to big brand online retailers would help avoid problems. This leaves people open to falling for spoof sites. Some of the respondents had a good idea of what they should be looking out for as indicators of security but even so, only 18 people mentioned https in answer to this question and of the seven who mentioned certificates, not all mentioned checking their validity. A number of respondents thought that avoiding infection would help protect them against phishing. Some clearly understood about the risk from malware but many seemed to confuse phishing risk with viruses.

Never open e-mails from unknown or that look unusual
Run virus software before and after any financial transactions online
Have two different virus checking tools that are used – **male, 46-55, medium low expertise**

Nineteen people felt that a firewall would protect them. Some of the more unusual but effective techniques, such as using a Linux Live CD for banking (one person, male, 56-65, expert) were more aimed at preventing malware than pure phishing.

In total, no more than around 20 people had truly robust anti-phishing strategies, involving a multi-layered and informed approach although a much larger number had one good habit, primarily not clicking on links or entering bank urls manually, or good general but not phishing-specific habits.

There was in general no indication whether people using toolbars for example actually notice or take heed of the warnings and whether people checking certificates for example actually know what to look out for.

336 people answered the question about email strategies. In the literature review Downs, Holbrook, and Crainor (2006) discussed strategies users displayed in working out how to deal with emails, including focusing on content rather than security indicators. Here users were asked specifically about links in emails, something at least 30 of them had said in answers to other questions they never click on. In this question, only nine stated that they never clicked on links, thus displaying an inconsistency.

The most popular ways of deciding whether to click on a link in an email were based around looking to see who the sender was, and whether the respondent knew them or trusted them

or was expecting to hear from them. Well over half of the respondents listed this as a strategy. This can leave users open to threats from malware generated emails.

If I know the sender, it doesn't cross my mind. I don't click the link if the sender is unknown. – **female, under 18, medium low expertise**

Also popular was the purported intention of the email, how well written it was and whether it looked legitimate. Just as with gut feeling and common sense in general, many people depend on whether the email 'looks' right to help them decide whether to click or not. As phishers are increasingly using logos and html formatting in emails, this is not necessarily a good strategy. It was also difficult to understand some of the strategies e.g. whether an email looks 'safe'.

The destination of the link was also important, both ostensible and what was revealed by hovering (although that can be compromised using Javascript). Finally anything that got through the spam filter was generally viewed as genuine. Only around 30 people displayed very good strategies.

In the next question people were asked about their strategies for deciding whether a website was genuine before they entered their payment details. There were 333 responses. People primarily appear to have interpreted the question as being about online shopping.

How well known the site is was very important to respondents, with 149 saying they only use known/trusted sites. As it is often better known sites that are spoofed by phishers, this is not necessarily a good strategy. Some of the comments suggest that respondents are either checking more for information about whether the site is likely to be hacked or whether it ostensibly belongs to a company in good reputation rather than whether it is genuine and not spoofed. In other words they are considering their risk in using the site in a broader sense than avoiding phishing sites. Some users chose to google for known security problems or reviews of the site and two stated that they checked into site ownership using WHOIS.

Many respondents knew that they should look out for signs of security on the site but some were content to be told the site was secure without verifying that for themselves. Phishers could therefore deceive users by including security messages on the site. Sixty eight people mentioned https and 11 certificates, although only five checked the certificate was valid. As discussed in the expert interviews, these are not necessarily an indicator that the site is genuine but they do help protect against payment details being hijacked by man-in-the-middle approaches. Again this suggests a lack of clarity about what phishing is. Again, some users were mainly influenced by gut feeling about visual clues, but this was not that common. Very few people mentioned toolbars or warnings in this context, fewer than those who listed them as strategies in previous questions.

Many of the respondents chose, rather than looking out for security indicators, to minimise potential losses instead by carefully selecting how they pay or by other means of risk minimisation. Many people saw the presence of PayPal as a guarantee of site security. Known payments processors also appear to act as an endorsement, as does 3D Secure even though this requires entering extra data.

Out of the 333 responses, only approximately 13 respondents checked very thoroughly before entering their details.

Overall therefore it seems that while many of the participants felt that they were protecting themselves, few were exhibiting robust protective strategies and there appeared again to be

a degree of confusion about what comprises phishing. For most lay users however, phishing is probably viewed as part of an overall mass of security threats and their focus may be on protecting themselves in general. For more expert users, malware may appear a threat more worth focusing on. It would of course be interesting to find out whether people differentiate those threats and which worry them the most.

5.6 User personae

The answers of different categories of users were then considered as a whole using categories drawn either from the literature review or the interviews – age, knowledge of computing and speed of decision making. Adjusting for gender imbalance showed very few differences of interest and so this will not be further examined. The intention was to see if these different personae – young, expert etc affected online identity in terms of behaviour in this area.

5.6.1 Age

Turkle (1996) stated that attitudes to computers differ between those whose first experience of computers were as a child and those who first encountered them as adults. The answers of those under 35 and over 35 were compared to selected questions from question 5 onwards (i.e. excluding other filter questions).

Younger people are significantly less likely to read bank security messages. There was also a noticeable and significant difference between the age groups concerning noticing anti-phishing materials. Younger people were much less likely to recall having seen anti-phishing materials. Under 35s were also more than twice as likely to pick up information from friends/family as older age groups. This is probably a reflection of how social lives change as people age and settle down. There was little difference between the age groups in terms of how likely they were to read the information but they were twice as likely to find it too simple and also twice as likely to find it too difficult to understand. There were no great differences in whether younger people acted on the information or not.

Question 16 concerned preferred sources of information and here there were noticeable differences.

Preferred source of information	Under 35 by %	Over 35 by %
Twitter	11.84%	5.83%
Facebook	32.46%	14.17%
on my bank website	70.18%	65.00%
in a letter from my bank	54.82%	48.33%
in newspapers	33.77%	37.50%
in magazines	25.44%	26.67%
Other, please specify:	12.72%	17.50%

Table 3 Preferred source of information by age

It is clear that younger age-groups are far more open to receiving information on social media platforms. In fact they scored higher for all sources except newspapers, magazines and other, possibly reflecting general tastes in media consumption (Ofcom figures show under-45s consume less print media than over-45s (Frangi, 2010)).

Under-35s were significantly more likely to think that they should be refunded if they lose money to phishing (77.39% against 65.25%) and they were also significantly less likely to take precautions against phishing (61.57% against 72.13%).

In other words, under-35s appear somewhat less responsible than older age groups about informing themselves and protecting themselves against phishing, corresponding with general stereotypes of how younger people behave with regards to risk and responsibility. However the quality of their strategies was no better or worse than those of older age groups. It is not clear whether this confirms Turkle's theory about differing attitudes to computers and there were in fact fewer under-35s in the 'very low concern about online crime' category than over-35s although this may reflect how concern also drops with computing experience and expertise. Nor were they significantly more likely to be victims of phishing so expert [3a]'s perception that younger people believe what the computer tells them is not borne out.

5.6.2 Knowledge of computing

This exercise compares self described 'expert' users with all the other answers. People who describe themselves as computing experts may of course have a wide range of different areas in which they may be experts and may not necessarily be any more expert with regards to security than other users.

The pattern of concern about online crime differs significantly between the two groups with experts generally less concerned overall but actually more likely to display very high levels of concern, perhaps because of a better understanding of the risks. On the other hand they may also be most able to mitigate those risks so the number of experts in the very high concern category is interesting.

Experts are actually more likely to have lost money to phishing, although not significantly so. However experts are much more likely to always read bank security messages (perhaps from professional interest) and less likely to never read them. They are also much more likely to have seen anti-phishing messages (94% compared to 71.43% of non-experts). They are considerably less likely to listen to information and advice from friends and family than other people. Unsurprisingly, specialist websites were mentioned as 'other' sources more by experts than non-experts. The percentage of experts who read the information was almost exactly the same as the percentage of non-experts. There was also very little difference in how easy to understand they found the information. They were however considerably less likely to act on it (28.26% against 39.22%), perhaps indicating a degree of complacency or perhaps indicating the quality of the information.

While preferences for reading sources were similar (except for Twitter and Facebook, which experts were less in favour of) they were more likely to suggest specialist online sites as an ideal channel for information – these of course would be very much less likely to reach anyone who was not a computing specialist.

Percentages for feeling that banks should refund phishing losses were nearly identical across both groups but experts were much more likely to take precautions to protect themselves (74% for experts against 63.67% for non-experts), a statistically significant difference and despite a few self described experts displaying thoroughly inadequate strategies, in general computing experts protect themselves better against phishing than non-experts.

This does suggest overall that knowledge about and understanding of phishing does make for more effective protection, backing up the studies from Kumaraguru et al (2009) showing that education improves efficacy rather than those from Anandpara, Dingman, Jakobsson, Liu, and Roinestad, (2007) which showed that education increases fear rather than efficacy.

5.6.3 Speed of decision making

Here, following the work of Pattinson et al (2012), very quick decision makers were measured against everyone else.

The answer profile concerning levels of concern about online crime was significantly different with a much higher percentage of people with very low concerns about online crime and a much smaller percentage falling into the medium low concern category that was the most popular for the general population. The very high figure was also higher for fast decision makers. The differences were much less marked with regards to non-online crime.

Fast decision makers were also a little more likely to have lost money in phishing attacks. They are also a lot less likely to read banking security messages.

There was not a great deal of difference in recall of seeing anti-phishing messages and the sources of those messages were similar too, except fast decision makers were less likely to take advice from family and friends.

As a result, it's difficult to say that very fast decision makers have markedly more problems with phishing or to confirm Pattinson et al.'s 2012 findings but the profile has sufficient differences with the general sample that it may be worth investigating further.

5.7 Chapter conclusion

One of the main themes to come out of the survey is that the people who responded to the survey in general do not appear to understand what phishing is or how best to combat it. Perhaps as a result of this, levels of concern about online crime are higher than about real world crime, the opposite of what was expected. Nonetheless the majority of people surveyed do take precautions to protect themselves but those precautions are mixed in quality and often depend on recognising who sent emails or limiting themselves to big brand websites. Although people say that they have seen anti-phishing educational material and found it easy to understand, their strategies suggest otherwise in many cases. In addition there are also people who do fail to protect themselves or to read anti-phishing materials or bank security messages.

There seems to be a general expectation of shared responsibility between banks and users for security – users take precautions to protect themselves but expect the bank to refund any losses. However this appears in part based on the belief that phishing is a result of failings in bank security, further emphasising the lack of understanding about what phishing is.

6 Discussion

6.1 Introduction

In this chapter the findings from the expert interviews and the user survey are compared with the findings from the literature review and with each other and are discussed and analysed. It should be noted that the experts whose comments are reported in chapter 4 were also given the opportunity to comment on the survey data but chose not to.

Contributions to theory and future work will then be discussed in the following, concluding chapter.

6.2 Research questions

In this section, each research question and each point that arose from it as a result of the literature review will be dealt with in turn, tying the points raised in the literature review into the results of the interviews and survey.

6.2.1 Why do users fall for phishing?

6.2.1.1 Users have a lack of awareness and understanding of phishing

In general the interviewees felt that the stereotype of phishing victims with little understanding of computing and phishing was unjust, because all levels of user can fall victim through distraction or highly skilled attacks, although there was some discussion of the uneducated, probably older user with little awareness of computing and online risks.

Yet survey results showed that there was a general lack of understanding about what exactly phishing was at all levels of computing knowledge (and with respondents being self selecting anyone genuinely ignorant or illiterate may have elected not to participate or may never have seen the survey). Only a few survey participants seemed to be well educated on the topic.

Many people appeared to confuse phishing with viruses and hacking and, perhaps more understandably, with malware, bearing out Furnell's findings from 2007 about a lack of knowledge of what phishing is. This confusion guided their strategies in combating it. There also seemed to be a perception that phishing was caused by a failure in bank security.

This suggests that the findings of the literature review are broadly correct – there is a lack of correct understanding of what phishing is and how to combat it and that the industry possibly credits users with more understanding than they actually have. In contrast, the industry perception that people were unaware of anti-phishing education was not correct as nearly 75% of respondents recalled seeing some form of a wide variety of channels.

However it does suggest that educational materials need to be far more explicit about the differences between different types of security threat and the corresponding strategies to combat them. This is particularly so given that respondents describe the material as easy to understand and yet they clearly do not understand it or at least do not retain that understanding. Users may also benefit from having information presented to them on several occasions in line with the findings of Kumaraguru, et al. (2009). Yet both the literature

(ed: Roessler and Saldhana, 2010) and the survey findings suggest that people tend to habituate to and ignore repeated warnings, because they think they know the answer already and hence do not need to change their behaviour.

Overall then, the perception that people are confused about phishing appears to be correct for this sample, something that may have consequences in creating educational materials and strategies.

6.2.1.2 Complacency about ability to combat phishing.

The literature showed that expert users may ignore toolbar warnings (Egelman, Cranor, and Hong, 2008) and that feelings of self efficacy may be counterproductive (Compeau and Higgins, 1995). The interviews did suggest that average users may be deluding themselves about how protected they are, either because they tend to believe computer mediated messages (as with Zuboff's assertion that the computer can't be wrong) or because they have chosen protection mechanisms which while appropriate to some security threats are not appropriate or enough to protect against phishing. Even expert users are taken in.

The survey results bore this out. Nearly 2/3 of respondents took precautions to protect themselves but in general those precautions were not robust and even some of the computing experts displayed poor strategies. Of the people who took no precautions, 2/3 had low or very low levels of concern about online crime. So there appears to be a degree of complacency about the ability to combat phishing at all levels of computing knowledge that bears out the findings in the literature. Equally, the remaining one third who were concerned but take no precautions are an obvious target for more education. In addition, people did tend to believe what they were told online, be it the identity of the person ostensibly sending an email or of the organisation owning a website.

This is not greatly different to how many people behave in the physical world, for example with regards to diet, exercise or contraception, or indeed with regards to computer backups. In addition often people inform themselves about issues but not enough, from failing to carry out full surveys while buying houses to not reading the small print on time share sales. They also fall for scams, pranks and April Fool's jokes.

At all levels of knowledge, respondents seemed to feel they were more protected than they were but there seems to be little about the findings under this heading which contradict how people manage themselves in daily life or which suggest that the online self is greatly different to the offline self in this respect.

6.2.1.3 Carelessness and lack of interest in security and risk

A role play based study carried out by Downs, Holbrook, and Crainor (2007) indicated a general lack of concern about protecting personal information online. Theories such as the Technology Acceptance Model and its successors suggests that users will not be motivated to protect themselves if they don't see the benefits.

While the interviews tended to back up this position, the survey in general did not with users appearing to display a reasonably responsible if often misguided attitude with two pointing out that loss of money is not the only consequence of falling for phishing and substantial inconvenience and embarrassment may also result. Where users did not protect themselves it seemed to largely be as a result of ignorance.

In terms of Castells' sense of organising meaning around who they are and playing roles, users seem in the main to view themselves as responsible online bankers or shoppers,

however mistaken their methods may be. They are trying to behave responsibly, in the main. And clearly this is not an area where they are taking on a different identity to their offline one (unless of course they are themselves trying to defraud the bank or the online shop). There is also an aspect of impression management too if they do not want to be seen as careless about fraud and losing money to phishers. One of the two who commented about the after effects of having been a victim described it as 'embarrassing' so in Goffman's terms he had lost 'face' (Goffman, 1965, p5).

There does therefore appear to be a difference between the literature, expert opinion and user attitudes. It is possible that the role play nature of the study by Downs et al (2007) may have influenced the responses of their participants. It is also possible that survey participants may have been reluctant to be honest about a lack of responsibility.

6.2.1.4 Ignorance of security procedures

Lack of technical knowledge (Anandpara, Dingman, Jakobsson, Liu, and Roinestad, 2007) and misunderstanding security cues (Downs, Holbrook, and Crainor, 2006) were reasons cited in the literature for inability to deal with phishing.

The expert interviewees did indeed feel that many people simply lacked the knowledge and capability to protect themselves and the survey quite clearly suggested a level of confusion about security measures and what they were appropriate for at all levels of knowledge of computing. The expert user quoted saying that she uses a 'firewall' to protect herself is indeed protecting herself against some threats but not necessarily against phishing. The same goes for all the people who depended solely on anti-virus software. It is possible that some of the people who took no precautions at all failed to protect themselves because of a lack of understanding of computers, figuring that it is better to do nothing than to do something that might in itself cause problems. Internet discussions about Trusteer Rapport for example might be enough to deter novice users from installing it (Dhanendran, 2010).

6.2.1.5 Focus on primary task rather than security

Several of the literature sources found that users viewed security as more of a distraction than a prime focus (Anandpara, Dingman, Jakobsson, Liu, and Roinestad, 2007), (Downs, Holbrook, and Crainor, 2007).

Interviewees [1] and [4] certainly seemed to agree, pointing out that habit drives many security responses (entering a password for example) and pressures of work lead people to do some tasks almost on automatic pilot, thus displaying ritualised behaviour (although that phrase was not used by the interviewees). Others resent the demands of security.

On the other hand, some people clearly do think about security choices as their responses to the three strategy questions in the survey show. Nonetheless some of those strategies probably do happen on automatic pilot and 93 people mentioned depending to all or some degree on tools that do it for them - telling them what is and is not safe or blocking threats (anti-virus packages, Trusteer Rapport, anti-malware packages, firewalls) rather than thinking about the risks themselves. One comment from an older male with medium low computing knowledge echoed the point about resenting security, describing bank security practice requirements as failure of customer service. He expected a refund of phishing losses, took virtually no precautions and had medium low concern about online crime.

It is probably inevitable that in many cases security is a secondary task – if only because people can only think about threats that they notice or are aware exist or in some cases because they do not care to think about them at all.

6.2.1.6 Ritual nature of task activity

Riegelsberger and Sasse's (2008) citation of Goffman's (1959) discussion of ritualised familiar behaviour is closely related to the above point and the comments from the experts apply equally. However this was too obscure a point to address in the user survey and none of the comments to the open questions were in any sense relevant to this. Trying to explore this point might be better done with a more ethnographic approach – observation in situ for example. Nonetheless, it could be suggested that security behaviour may become somewhat ritualistic in nature, particularly with regards to entering passwords on demand, with the same strategies followed even when they may not be appropriate. People may also have ritualistic methods of devising passwords which may reduce their strength.

Overall though, this point was not addressed.

6.2.1.7 Social context

Jagatic, Johnson, Jakobsson and Menczer's (2007) study showed that student participants were far more likely to become phishing victims if the email came from someone they knew. The answers to the question in the survey about email strategies strongly bore this out and showed that by far the most popular strategy (and one chosen by more than a third of survey participants and over half the people answering that question) was to trust by default emails appearing to come from people they knew, often as their only strategy. As discussed, this is not necessarily helpful. It may also link into Goffman's points about performance and face (Goffman, 1965, p5) – what would be the consequences of not responding to the email supposedly from a friend asking for money because their credit card had been stolen on holiday, if indeed it were real?

One of the interviewees [3a] felt that users in general tended to believe what they were told online so that if an email appeared to come from a friend, they would accept that. This highlights the unreality of online activity – in reality all one can say is that it appears to come from a known email address and that is not the same as coming from a particular person – and also highlights the difference between online identity and online entity as discussed by Alpar, Hoepman, and Siljee (2011). Interviewee [2] pointed out that the problem wasn't just users not being able to verify that the email came from who it supposedly came from (already a level too complex for most of the survey participants) but also that there was the question of being able to recognise or trust the intermediary purporting to verify the sender. This point from [2] also applies to certificate authorities which have brand names that mean nothing to the average user.

Social context therefore appears to influence how likely someone is to fall for phishing. It also became important when it comes to learning how to combat phishing, something that will be enlarged on below.

6.2.2 Do personality factors have any effect on how people deal with phishing?

6.2.2.1 Personality traits (extraversion)

This was addressed in the literature by Pattinson, Jerram, Parsons, McCormac and Butavicius (2012) where more extraverted people were found to be better at dealing with emails. This was not explored in any depth at all during the interviews and any attempt to discuss personality in general did not produce much discussion, although one banking representative commented that people of all personality types could benefit from anti-phishing education. However it is hard to understand how public educational materials could be targeted or tailored by factors such as Myers Briggs type, of which

extraversion/introversion forms one scale, even though this might be effective. This feeds into the idea, discussed in the literature, from Amichai-Hamburger (2007, p187) about users being viewed as a single entity.

Nor was it addressed in the survey, which considered only one aspect of personality – impulsiveness.

6.2.2.2 Degree of impulsiveness

One of the more interesting findings in Pattinson et al.'s work (2012) was that impulsiveness can affect one's likelihood of falling for phishing. Both bank representatives interviewed agreed that it might be interesting to see whether that translated to general bad banking behaviour correlating with a propensity to fall for phishing and that it might link into ideas about responsibility for phishing losses too. Interviewee [5] suggested that impulsive people were more likely to shun responsibility for phishing losses.

In the survey, speed of decision making was used as a proxy for impulsiveness and there were some differences found between fast decision makers and the general population, especially with regards to how likely they were to read bank security messages. In fact very fast decision makers were least likely to think that banks should refund their losses, with medium fast decision makers most likely.

Overall, the findings were not conclusive but it appears that there could be some potential for examining bank customer records in this area and this would be one feasible way of recognising that all users do not have one amorphous identity.

6.2.2.3 Concern about what sender of email thinks of recipient

This arose from a comment made by a participant in the study run by Downs, Holbrook, and Crainor, 2006. It may also link into what Goffman describes as performance disruption (Goffman, 1959, p23) where not doing what the email requests disrupts the expected trajectory of the interaction.

Interviewee [2] suggested that older users with more deferential personalities might be more likely to respond to phishing attempts purely because they are used to doing what they are told. Yet there was nothing in any of the user comments to suggest that worries about what the email sender thinks is a concern.

Overall, this research question was not investigated to the fullest degree, in part because expert interviewees had not really considered the issue before and in part because of the difficulty of framing suitable survey questions. There is the potential for more research here but there are also questions about whether a practical way of utilising the results for good can be found. It's easy to imagine how phishers might use this. However one could argue that in utilising different sorts of strategies, users are themselves reflecting their differences and there could be merit in further investigating if different types of strategies are more effective for specific personality types.

6.2.3 What is the relationship between online and offline behaviour and how does it impact the response to phishing?

The idea that online behaviour closely reflects offline behaviour is now somewhat dated (Baym, 1998) but there are aspects of the online world where the online self is closely connected to the offline self and banking clearly is one of them.

The interviewees in general agreed that the online world was somewhat less real to users, lacking in particular physical cues that help with judgment. One described it as a life without responsibility. They also felt in the main that people took more risks online and behaved in a more trusting way online although there was some disagreement about whether people were more trusting or just behaved differently. There were several references to how younger people in particular have few concerns about online privacy. Yet at the same time the survey showed that people were more concerned about online crime and do try to act responsibly, although it also showed that many people tended to take things at face value online. It also showed that over 5 times as many people replying had been victims of physical world crime as online crime, suggesting greater caution online (or possibly less crime).

Several of the interviewees made the point that phishing is just another type of fraud and it is true that people do also fall for scams in the physical world or over the phone, from boiler room scams, to fake perfume bought from market stalls to mis-sold income protection plans. With phishing as with these deceptions people think what they see is real but it is not (Goffman, 1974, p10).

Because online banking is simply a more practical replacement for a physical world activity it is closely anchored as a relationship (Zhao, 2006), even when the bank is online only, thanks to the presence of ATMs and physical currency. If money ever becomes purely digital, perhaps that will change.

Even so, it does not appear possible to say that the two areas of behaviour mirror each other closely based purely on this research.

6.2.4 How do users react to anti-phishing methods?

6.2.4.1 Confused by warnings, indicators and education

As was established under the discussions about ignorance, both the interviews and the survey showed that users at all levels of computing knowledge were somewhat confused about the difference between different types of security threat and different means of countering them.

6.2.4.2 Focus on site content, graphics rather than security indicators

A number of authors found that users tend to focus more on content than on security indicators in assessing risks (Downs, Holbrook, and Crainor, 2006), (Dhamija, Tygar, and Hearst, 2006), (Furnell, 2007).

The interviewees strongly felt that users depended either on gut feeling or on advice to look out for bad graphics or writing, something that can be falsely reassuring as phishing attempts become more professional looking. Some of the people surveyed did indeed mention these factors in their strategies – there were mentions of bad grammar as a warning sign and logos and graphics as positive indicators, as well as how professional the email or site looked. Something else mentioned regularly was the tone of emails – whether they sounded like they came from their purported senders. In Goffman's terms, where that is not convincing, the intentional part of the phisher's communication is subverted by unintentional giving off of clues that show it is not real (Goffman, 1959, p28).

However many respondents, nearly 20% of the entire sample, and not just expert users, mentioned looking out for https designations on websites and others listed looking out for unspecified security indicators or the padlock logo (although there was little or no indication as to where on the screen they looked for that). In contrast only 5.6% of the sample listed

'look and feel' with regards to websites. Far fewer people listed email content as an indicator than who the sender was (not by any means a better strategy though).

On the whole then, the literature findings here are borne out, although the user perspective is a little more complex than expected.

6.2.4.3 Education too complex

The perspective in the literature review that user education was too complex came originally from a newspaper article about a House of Commons Science and Technology Report into Cybercrime (Sample, 2012). Other authors certainly felt that educational messages could be made more effective (ed: Roessler and Saldhana, 2010) or clearer.

Interviewees felt that educational materials needed to be engaging but there was concern that dumbing them down could be counterproductive. There were also doubts about how effective they were and whether people were actually even aware of them.

The survey showed however that most people who recalled seeing educational materials felt they were 'just right' in understandability terms. Nonetheless, against that one must set the effectiveness of the anti-phishing strategies displayed. It is hard to judge whether they were indeed too complex and respondents did not want to admit that to save face, or conversely too simple and not explanatory enough, or people thought they understood them but didn't, or whether they were pitched correctly and people simply failed to recall them when needed. It does seem likely that something needs to be done to make them clearer or possibly more detailed and explanatory, although that might help phishers.



Figure 4 Example of an anti-phishing educational message

Despite what the survey respondents said, it seems that there is potential to make phishing education easier to understand and recall.

6.2.4.4 Security indicators are not effective/are ignored

The literature review found that users often have difficulty interpreting or acting on the information provided by toolbars (Kumaraguru, Sheng, Acquisti, Cranor, and Hong, 2007) and may simply ignore them (Downs, Holbrook, and Crainor, 2007). There are also concerns about false positives.

The interviewees had little to say about this type of technology, focusing instead of efforts driven by the banks – site takedowns for example. It seemed though that the interviewees in general felt that tools of this nature that placed the onus on individuals to protect themselves were not sufficient.

From the survey it seems difficult to state either way whether indicators are ignored although it might be possible to argue that in some cases they are not understood or effective. The survey did not give any idea of whether users always noticed warnings and it would be difficult outside of a laboratory environment to measure that. However there could be merit in asking whether users always act on warnings they do see. Nonetheless a good proportion of the respondents appear somewhat dependent on packages of this nature.

It's difficult to say, therefore, whether this finding from the literature is borne out.

6.2.4.5 Banks/website owners cause confusion by not following own guidelines or by having poor security practices

Inconsistency in security user interface design (ed: Roessler and Saldhana, 2010), (Grover, Berghel, and Cobb, 2011) can be problematic for users as can banks ignoring their own security guidelines (Anderson, 2007). This was confirmed by both [1] and [4] who pointed out that some banks do contradict their own guidelines and that other website owners may often do things that banks say they won't (asking for password confirmation for example) meaning that it is hard for users to know what is and is not right. Only one of the survey respondents in any sense picked up on these issues though, an expert user who refuses to bank online until banks improve what he called their "noddy level understanding of security". While many other respondents clearly were confused, it is difficult to know what to attribute that to.

Overall, with regards to this question, there is general confirmation of the findings of the literature review. The interviewees tend towards wanting to resolve problems by avoiding placing responsibility on users, while users do appear for the main part to be trying their best although there is a general level of confusion about what is effective. The W3C work edited by Roessler and Saldhana (2010) is intended to standardise security interfaces on screen – standardised implementation of this and of consistent URLs across the industry could make the job of explaining what to do and what to look out for much easier for users to understand. On the other hand it might also make the job of creating convincing spoofs much easier for phishers.

6.2.5 Means of improving anti-phishing methods

The expert interviews generated a list of recommendations for improving anti-phishing efforts – these were listed in chapter four. At this stage only points arising specifically from the literature review will be considered.

6.2.5.1 Embedded education

Work done by Kumaraguru, Sheng et al., (2007) showed that embedded education is more effective than warning notices and other non-embedded methods. One of the interviewees did cite their own bank's approach of linking customers trying to click on phishing links to the Anti Phishing Working Group's education page about phishing but made no comment about the effect of this. Another said that he felt that people only learnt through experience, which is rather a different sort of embedded learning. This was not a topic that was mentioned by any of the survey participants but it would have been interesting to find out if any of the respondents who admitted to having been victims previously had fallen for phishing a second time. As they tended in general to be very much more concerned about online crime than

other respondents, the experience is likely to have had some effect. Overall, though, this finding was not confirmed.

6.2.5.2 Making education relevant to the real world/more personalised

Some sources suggest that making education relevant to the real world for the user makes it more effective (Kumaraguru, et al. 2009). Others say that the fact that it often is not relevant or relatable to explains why it is ignored (Wilson and Argles, 2011). Pattinson et al.'s 2012 work on personality factors concluded that a better understanding of these could improve security management within a corporate context, something reinforced also with regards to corporate training by Parsons, McCormac, Butavicius, and Ferguson (2010).

While it's easy to understand what more personalised education might be, although perhaps not how it might be managed in an efficient fashion, it's not necessarily clear what more relevant education might be like. In Kumaraguru et al.'s case (2009) it may simply refer to how that particular study was not administered under lab conditions, thus reducing the confusing effect of role play.

Interviewees however agreed that education needed to be engaging, for example dramatised and pitched at a level that people could understand. Banks discussed using a variety of channels, although these are largely currently limited to in-branch leaflets and messages on the website. There was also discussion of using social media channels to encourage viral spread of anti-phishing messages. With spammers and cybercriminals moving over to Facebook and Twitter as a medium (Leyden, 2012), social networks may become an increasingly important channel for education.

Personalisation per se was not discussed although messages received from friends and family become de facto more personalised in a sense. Whether a personalised outreach that might be appropriate within a corporate context is practical over an entire customer base was not discussed but there was discussion about whether a better understanding of individual customer behaviour with regards to banking might help to identify potential phishing victims.

Pitching different types of educational material at different levels of knowledge and understanding might be one feasible approach, although anything pitched at experts should probably contain refresher material, given that as shown here self described experts may overestimate their level of knowledge about security.

Interviewees also felt that education should begin early, in schools and that children would have a better chance of protecting themselves as a result. This echoes another conclusion from Kumaraguru et al. (2009) and also current policy from the Labour Party (Hopkins, 2012).

While survey participants did not explicitly discuss personalised education, there was a strong preference displayed for information from official sources and in official guises, such as bank letters. Nonetheless younger people were more open to receiving information informally from friends and family. Indeed people overall were actually most likely to change their behaviour as a result of information from friends and family. Industry generated anti-phishing messages are after all not laboratory trials so by their very nature are 'real world'. It's easier to understand how a message might be made more 'relatable to' by means of language and examples for instance than more 'real'. 'Relatability' could also be tested reasonably easily using randomised controlled trials. True personalisation of public information however may not be so easy to achieve.

Overall, though, as long as information is seen to be reputable and from an official source, making it more relevant seems as if it could be beneficial.

6.2.5.3 Use of positive and negative reinforcement

The question of positive reinforcement was also raised by Parsons, McCormac, Butavicius, and Ferguson (2010) because of its general applicability to training, although as mentioned behavioural approaches of this nature are seen as somewhat outdated by some. Yet for at least one interviewee, negative reinforcement was seen as more effective, as he stated that people only learnt about phishing from losing money to it.

Indeed those survey participants who had already been victims of phishing were significantly more worried about online crime, showing that the point about negative reinforcement might be correct. However their strategies for beating phishing were not noticeably more robust and multi-layered than those of the entire group, suggesting that caution is not enough unless coupled with knowledge. And as discussed above, further investigation into whether they had been victims more than once was not undertaken.

There was no mention of positive reinforcement and it is difficult to know what this might comprise, although a game based component could be added to education for younger people, such as Kumaraguru et al.'s game Phishguru (2007 (with Rhee et al) and 2009) and banks could possibly add a good account management premium or bonus to interest rates, for example for agreeing to download Trusteer Rapport.

This point could also be seen as relevant to making education more relevant and 'real'.

6.2.5.4 Use of active warnings that cannot be ignored

(Wu, Miller, and Garfinkel, 2006) suggested that phishing warnings from toolbars and other software should be designed so they cannot be ignored but must be engaged with, in other words nudges or choice architectures that do not allow users to make wrong choices by default (Pieters and Coles-Kemp, 2011). Yet as Wilson and Argles (2011) point out, such tools often have problems with false positives which could be irritating for the user.

Toolbars and warnings were not technology topics that the interviewees really discussed, although [3a] did point out that users often do not get the best out of systems they have, failing to update anti-virus systems and other software for example. In addition, people operating on auto-pilot as discussed by [1] may well click OK on warnings without reading them. None of the survey participants admitted to ignoring warnings but some of the few participants who mentioned looking out for certificates did not mention reading and checking them so it certainly seems possible that people may well just click through warnings and indicators even though they are ostensibly looking out for them.

However in that case active warnings might not help if people don't bother to read them – just clicking OK on something that pops up in the centre of the screen is not much better than ignoring something flashing at the top, making this literature finding something that isn't necessarily borne out or contradicted by the research.

6.2.5.5 Consistent interfaces

Inconsistency in security user interface design (ed: Roessler and Saldhana, 2010), (Grover, Berghel, and Cobb, 2011) has already been discussed in this chapter with little specifically being said either by interviewees or users. It is worth mentioning though that with current sign on systems imposing a hard to manage cognitive load because of multiple usernames

and passwords to remember, as discussed by Alpar, Hoepman, and Siljee (2011), anything that reduces that by adding consistency might be helpful to users (although also to phishers). On the other hand if every sign on interface is the same, might that conceivably lead users to be even less vigilant and even more prone to click OK without extra thought?

6.2.5.6 Role of mobile authentication

For a number of authors, such as Mannan and van Oorschot (2010) mobile or other personal devices could be the answer to phishing by adding an additional layer of authentication to logging in (i.e. two factor authentication). Yet both interviewees and survey participants pointed out that mobile devices also introduce new problems, particularly because of their small screens. This is therefore a possible area for user education, both about minimising the dangers arising from small screens and also about how mobile communications are more secure than unencrypted Internet traffic.

6.2.5.7 Helpfulness or otherwise of site authentication images

While there was mention in the literature of this technology (Iliev and Sun, 2010) and how it could be strengthened to ensure users did not fail to benefit from it, it was not mentioned at all by the interviewees and only in passing by one user who presumably banks with a Sitekey customer. It could however be viewed as a means of allowing the user to personalise the security experience.

Overall, there was little overt input from the survey respondents in this area, other than about preferred sources for information, as discussed above, and a few comments from self described expert users about enhancing bank website security, for example by avoiding the use of Javascript.

6.2.6 Responsibility for protecting user against phishing

6.2.6.1 Users don't believe they have responsibility for protecting themselves and do not care about risk

This finding came from the Downs, Holbrook, and Crainor, 2007 study which involved role play. In real life, are things different?

The interviewees talked about a 'life without responsibility' online and how the knowledge that (most) banks would refund their losses made users reluctant to protect themselves. This perspective is similar to the one espoused in the recent suggestion by the Labour Party in the UK that failing to take care online should be viewed as equivalent to drink driving (Hopkins, 2012). Yet there was also recognition from the interviewees that banks have a responsibility to protect their customers and that offering protection is in fact a business decision that protects their investment in the online channel. Overall, they felt, the responsibility should be shared and one suggested an insurance liability charge type of measure where a small financial fine might concentrate the mind. Alternatively, a different type of business decision might involve selling insurance against phishing to customers.

Strangely though, the interviewees who were most in favour of a technological response that would most disempower users, [2] and [4] and who were least confident of the user's ability to protect themselves, were also those that thought that the responsibility in liability terms lay entirely with the user, a seeming contradiction and arguably unfair.

A majority of survey respondents however felt that banks should be responsible, or should at least refund their losses. This view reduced somewhat with age and degree of computing

knowledge but also seemed to be based in part at least on the view that phishing was caused by bank websites getting hacked, which again indicates confusion about phishing. On the other hand a majority (a slightly smaller one) did take action (of varying levels of effectiveness) to protect themselves against phishing. So as with the interviewee views, there seems to be a willingness to share aspects of responsibility and a level of contradiction.

Overall though, given that many users seem to have severely restricted or mistaken understandings of what phishing is and how to combat it, whose responsibility is that? That of the person who mistakenly thinks they are doing the right thing or that of the banks that have tried to explain what the right thing is and presumably failed up to now?

In addition Alpar, Hoepman, and Siljee's point (2011) about the distinction between membership of a resource and ownership of a resource seems relevant here. Phishing losses presumably come from accounts that have the ability to make payments i.e. current accounts. The customer may be either paying the bank for the facility or at least enabling the bank either to earn interest on their balance or to contribute to the bank's regulatory capital requirements. The move to online banking is not just about the (undoubted) added convenience to the customer, it's also about cost savings from closing branches. Both parties derive benefits from the bank customer relationship.

As discussed in the literature review, it is not just about the customer having to reliably authenticate themselves to the bank. The bank also has an obligation to authenticate themselves to the customer, i.e. to provide an online banking experience that allows the customer to reliably distinguish between the genuine bank website and phishing spoofs. This is the basis of mutual authentication. Survey responses suggest that banks are not doing that in an adequate fashion. Again, it seems as if the responsibility is a shared one and if that is the case, the situations where either the bank or the user alone take liability for phishing losses seems unfair.

In summary, this particular finding from the literature produced some interesting tensions and some of the most significant research findings.

6.3 Chapter conclusion

If this chapter has one major outcome, it seems to be that the responsibility for combating phishing and improving mutual authentication should be shared. There were many areas where interviewee and user opinions coincided and a few where they did not, primarily the expert view that users see the online world as a world without responsibility and do not care about online risks and hence are careless about security. In fact the opposite is true – users worry more about online risks than physical world ones and take precautions to protect themselves. Unfortunately, due to misconceptions about what phishing is, those protective precautions and mutual authentication approaches are poor. Experts also thought that users either did not understand or were unaware of anti-phishing education – this was not explicitly borne out by the survey results but despite saying that the information they had read was easy to understand, many users did not display good protection strategies. There seems to be a basic lack of understanding and knowledge about phishing, something for which the responsibility again should be shared.

The next chapter uses these findings and interpretations to go on to develop conclusions to the dissertation.

7 Conclusion and future work

7.1 Aim of the dissertation

The aim of this dissertation was to gain a better understanding of how users carry out mutual authentication and protect themselves from phishing with the intention of enabling the banking industry to offer better educational and technical responses to phishing. It achieved this through answering the following research questions.

- How are users responding to phishing?
- Do personality factors have any effect on how people deal with phishing?
- What is the relationship between online and offline behaviour and how does it impact the response to phishing?
- How do users react to existing anti-phishing methods?
- How can existing anti-phishing methods be improved?
- Whose responsibility is it to protect the user against phishing?

7.1.1 How are users responding to phishing?

The study suggests that contrary to some of the established literature in this area and to the views of the expert interviewees, most of the users surveyed do care about doing the responsible thing about protecting themselves against phishing. However many of them are clearly confused about phishing, what it is and how to protect themselves. This confusion was the clearest outcome of the survey. Some of them are able to admit to that confusion, others are complacent about their knowledge and strategies. Very few of them display a fully robust understanding and approach, an issue which manifests at all levels of computing knowledge. Part of the confusion lies with what phishing is and how it differs from other security threats – there appeared to be some confusion about the difference between phishing and hacking for example with some people thinking that phishers obtained their details by hacking bank systems. Others seemed to have a basic understanding about malware but not about the social engineering aspect of phishing.

Possibly as a result of this there were quite high levels of concern about online crime, higher than about crime offline.

Most of the users surveyed both took protective measures and read anti-phishing material and bank security messages. However a hard core of users did not and there were some who rated themselves very concerned about phishing but did not take steps to protect themselves. This again suggests a fundamental lack of understanding that could usefully be addressed by better targeted and designed anti-phishing education campaigns.

Social context mattered with users both prone to believing that emails coming from the email addresses of known individuals or companies were inherently trustworthy and also in varying degrees open to learning about the dangers of phishing from friends and family.

There were some differences identified between different types of people. Younger users were in general less responsible although those who did protect themselves had just as good

strategies as other age groups. Expert users (self described) who felt they had a better understanding of the risks as a whole were less concerned about online risks but also contained a sub group who were very much more concerned than the general population. This suggests that some self described experts perhaps need a reality check about how good their understanding really is. Impulsive people were slightly more likely to become phishing victims than the general population.

Overall, users turned out to be more concerned and more responsible (albeit with varying levels of effectiveness) than they were expected to be by industry experts but no better educated or aware than the experts expected. This suggests that with the right educational approach users might become better at protecting themselves against phishing.

It was felt that this research question, which was fundamental to the other questions, was investigated thoroughly and successfully.

7.1.2 Do personality factors have any effect on how people deal with phishing?

This topic was mentioned only in passing in the literature and proved difficult to investigate. Expert interviewees had not really considered it as a topic and it was difficult to deal with in an online survey. Nonetheless the factor of impulsiveness was examined through the proxy of a question about speed of decision making and it did seem that there were some differences between fast decision makers and others, mainly in how likely they were to read bank security messages and how concerned they were about online crime. Given that how people behave online is by its very nature a behavioural issue, it seems likely further investigation into how personality affects behaviour would be fruitful in this area but there are questions about how this could be achieved and what kind of practical benefit could arise from any results given the public education nature of the issue.

7.1.3 What is the relationship between online and offline behaviour and how does it impact the response to phishing?

While the expert interviewees expected users to treat their online activities as a life without responsibility, this was not borne out by the findings of the survey. Users did appear to try to act responsibly. Nonetheless certain aspects of unreality in the online world did show up. For a start, users were prone to judge the trustworthiness of emails by who appeared to send them. Not many checked that the ostensible sender was reflected by information shown in the source data of the email. In other words people did appear quite trusting online and there was a tendency to judge by appearances.

The survey did not allow the discovery in any real sense of how people behaved offline, but it did show that more people had been victims of offline crime than online crime and that there was a correlation between being a victim of online crime and being a victim of offline crime suggesting a possible relationship between online and offline behaviour. Users were also more worried about online crime than offline, the reverse of what was expected by the expert interviewees. This added level of worry did in general result in users taking precautions (although not in all cases) albeit not necessarily effective ones.

Given that only two questions in the survey dealt with offline topics, a broader ranging enquiry could probably have answered this question more effectively.

7.1.4 How do users react to existing anti-phishing methods?

The results of this research question largely speaking confirmed literature findings – that many users find security indicators confusing and are reliant on content, look and feel and branding for cues, something that phishers are increasingly taking advantage of. Yet given the expert interviewee contention that more recognised indicators such as the https designation and certificates cannot necessarily be relied on to guarantee veracity, and that banks are sometimes guilty of contravening their own guidelines, users are left in a difficult position and perhaps cannot be blamed for their confusion. Perhaps aware of these contradictions, users displayed a strong preference for educational material and security guidance from official sources like banks, although younger people were more open to less orthodox channels.

They confounded expectations however in claiming to find existing user education easy to understand but this was not necessarily as it seems if their strategies are anything to go by because the indications are that even if they think they do, many do not understand or retain the information they have read.

Again, it would have been possible to investigate this question in greater depth but the results obtained provide a reasonably clear answer.

7.1.5 How can anti-phishing methods be improved?

The expert interviews generated a list of suggestions about how to improve anti-phishing which are listed in chapter four. These overlapped in part with similar recommendations drawn up after a similar but much wider ranging expert interview effort at Carnegie Mellon University. These could form the basis for further work, for example testing the recommendations, extending them or gathering further support.

One of the main findings in the literature was that educational efforts should be more 'relevant'. This is an ill defined concept. One way of understanding it is to segment and target the information better, taking into account age differences, different levels of computer knowledge and different types of approach. There are challenges to doing this but a broader range of channels, for example social media, something banks are already considering, is one way. Another, which was widely recommended by the interviewees, is to start education early, in schools.

The users did not have much to say on this topic although in general they expressed a preference for receiving educational material through official channels, suspicious perhaps that less official outlets could be used by phishers to trick them. Apart from channel preferences however they were not canvassed on their views about improving what they read so this could form the basis for extending this research, as could examining the expert recommendations with a broader panel of experts.

7.1.6 Whose responsibility is it to protect the user against phishing?

This research question was thoroughly examined and showed up quite a few interesting tensions. For example, some experts felt simultaneously that users were completely liable for their own safety online but could not be trusted with the agency to create that safety. Many users felt responsible for their own safety but at the same time expected the bank to refund any losses. The latter view appeared based on a lack of understanding about phishing, the former was harder to parse but not untypical of how technologists view users. The issue of ownership versus use of resources was relevant as was the question of which assignment of responsibilities made best business sense for banks.

7.2 Critical reflection

As the discussion under aims and objectives shows, the enquiry to a great extent answered the research questions. However there are areas where further enquiry is possible – these will be discussed in the appropriate section below.

7.2.1 Methodological issues

The biggest methodological flaw associated with the research was that the sampling techniques used to gather survey participants, convenience and snowball sampling, did not result in a truly representative sample which makes extrapolation of the results to the general population difficult. The sampling method was chosen for reasons of practicality and cost and was the best method given the constraints of the project but nonetheless it was not ideal. It also resulted in a sample that was somewhat skewed in both gender and age terms and, because all recruitment for the survey was done online, could not truly represent users who rarely used computers.

While the gender skew did not appear to impact the results greatly as adjusting for gender made little difference, the other two factors may have had an effect. Examining how under-35s differed with older age groups did show some differences as discussed in chapter five. In addition there were not enough participants with very little or no knowledge of computing to be able to form a judgment about how they would have changed the overall results in larger numbers but it seems likely that they would have.

In retrospect, while the choice of a survey had the benefit of accessing a large number of users (354), it also had some failings as a tool for gathering information about users. It was difficult to access anything other than high level opinion and comment. Following up with discussion groups and interviews, had time and resources allowed, would have produced more finely grained data. Users may also have been tempted to present a better picture of how they behave than might really be true in order to save face. This already appeared to be the case with respect to some of the self described computing experts and may well have extended to exaggerating how often they carried out various precautionary measures. This is not something that would have necessarily been remedied by the use of discussion groups and only observation in situ or some form of online monitoring might have produced more verifiable data.

Despite best efforts, there may have been prestige bias in some of the wording – for example in asking people how easy educational material was to understand. The answer was overwhelmingly ‘just right’, something that clearly was not the case given some of the other answers.

Finally, it would have been beneficial to have received feedback from the expert interviewees about the survey findings for purposes of triangulation but despite being given the opportunity, none of the interviewees chose to, feeling no doubt that they had given up enough time for free already.

7.2.2 Limitations

The main limitations of this work, as discussed, were time and resource. While there was enough agreement between experts to assume that further investigation might have produced similar findings, it is not necessarily the case that further user investigation would have produced similar findings, particularly if there had been more representation from computing novices or phobics. In the further work section, there will be a recommendation that data mining techniques could be used to find out whether becoming a phishing victim

correlates with other clearly identifiable types of banking behaviour. Access to bank customer databases would be required for that work and its lack at this point formed a limitation.

7.3 Future work

As well as generating the findings discussed, the research also produced some inconsistencies and topics that would merit further study. Some of the findings also merit further examination. These are examined in turn below.

7.3.1 Inconsistencies between findings

As discussed above, the major area of inconsistency was between the findings that users found educational material easy to understand and their actual reported behaviours. Despite already discussed reservations about the role of role play exercises in this area, this is something that could potentially be better examined in such a setting.

There were of course also inconsistencies between expert opinion and user opinion on certain topics. Identifying these was part of the point of the research, particularly given the tension identified in the literature review about how technically users are only considered individual in terms of unique identifiers but in reality are all individuals from a behavioural perspective. These have been discussed at length in the findings chapter and resolving this dichotomy may be an important part of the answer to resolving the issue of identity online.

7.3.2 Building on findings

Areas for possible future work split into two types – issues about users and issues concerning possible solutions. These topics arise from findings from the survey and interviews and also from findings from the literature review that were not satisfactorily answered by the survey and interviews.

One of the major findings of the study was that the users surveyed appeared to confuse phishing with other types of security threat. One direction for further study would be to investigate this further, finding out what types of threats they were aware of and how they ranked them in severity and further clarifying how they distinguish between them. It would also be interesting to discover, presumably by means other than a survey, how honest users are about their behaviour around and experience of security threats, particularly given that malware is often found on porn and gambling sites.

The study also generated some tentative evidence that Pattinson et al.'s work (2012), which covered the impact of personality factors on phishing management had some merit with regards to impulsiveness– very fast decision makers were slightly more prone to becoming phishing victims. Other factors such as extraversion were not studied for this dissertation but could be studied in future, for example in focus groups or further surveys, although it is unclear how this could then be leveraged in practical terms.

As mentioned above, one way of further investigating the findings on impulsiveness would be to work in co-operation with a bank, where feasible within the requirements of data protection regulations, to see whether impulsive banking behaviours like incurring unauthorised overdrafts do correlate with falling prey to phishing attacks. If this did find a correlation, banks might then be able to predict who is likely to become a phishing victim and target them with specially designed educational materials accordingly. Given that one of the basic premises of the work is that technology does not account for the individuality of and differences between users, work that further individualises users and finds correlations between different approaches to security and different types of activity could potentially result in differentiated

types of technology solution, for example different types or layers of authentication processes for different types of user. This reflects customer differentiation in banking in general where based on different behavioural profiles, customers may have different credit limits, overdraft limits, bank fees and even different EMV online and offline authorisation floor limits for card use.

There were a number of topics relating to how users experience phishing that were touched on only peripherally or not at all and could form the basis for further work. For example there was some discussion of standardisation of security interface design but the research did not investigate how different approaches to interface design might affect how easy users found mutual authentication. Nor did they investigate whether the work carried out by W3C (ed: Roessler and Saldhana, 2010) had in fact improved matters for users.

There was also in the end, primarily because of time factors, limited use of the behavioural theory in the analysis of the data, although it did generate some insights. However, much of the reading done in this area seemed far more applicable to less prosaic areas of online activity than banking, for example social networks or gaming, so there is the potential for further work here.

A more solutions focused direction would be to compare different bank strategies on customer education for effectiveness. Again, this would require access to bank customer records. There was a little evidence from the expert interviews about different bank approaches with regards to refunds, but it was not possible to draw any conclusions about their relative impact on phishing.

It might also be possible to test different types of educational or warning messages in randomised tests across bank customer lists, subject of course to suitable ethical controls.

It might also be possible to examine the risk to single sign on solutions posed by phishing.

In addition, mobile phones may have a role to play in two factor authentication which could greatly reduce the risk of phishing attacks. While a technical investigation of this is a study of a completely different scope, it would be interesting to investigate user opinions and experiences of mobile phone use in banking to find out whether such a measure would be welcome and effective. On the one hand, mobile phone usage for a multitude of app based purposes is seemingly very popular, on the other the expert interviews did present anecdotal evidence that many users do not like having to take extra steps using extra equipment to access bank or payment services.

Another area raised by the literature review that was not really addressed was design of educational materials, a separate discipline in itself, and in particular how some of the insights generated in the study could be incorporated into educational material. This is another area that could be usefully studied as a separate topic.

Finally, one interviewee spoke about the role of trust and trusted intermediaries online. While trust was touched on peripherally in the project, this is a related area which would bear considerable investigation. While some users did speak about checking certificates, there was little evidence that most of them knew what this meant and what the significance of the issuing name on the certificate was. As he said, would a certificate issued by a known retailer such as Tesco carry more weight than one issued by Verisign? Given the way that some users relied on known brands for authenticating websites, there is a temptation to say yes. This is something that could be usefully investigated.

7.4 Contributions to body of knowledge and relationship to larger area of study

The main contribution of this work is to suggest that it is likely that users are more concerned about online crime and more responsible about how they protect themselves than expected but that they remain confused about what phishing is and that confusion reduces the impact and effectiveness of their precautions. Concern levels about online crime are higher than those about offline crime. The work also showed that there may be differences in approach according to age group, level of computing knowledge and degree of impulsiveness in the personality.

With regards to the broader area of digital identity, it reinforces the importance of an anti-foundationalist approach in this area. There is no one size fits all answer. Thus it highlights the dichotomy between the technologist's view of the user and the user's experience of themselves and poses the possibility of layered approaches to user authentication that recognise the difference between user attitudes, personality, levels of knowledge and levels of responsibility. Instead of removing user agency with broad brush approaches like a global identity management system, which the expert interviewees admit pose almost insurmountable commercial and political difficulties and also potentially increase the gains for phishers, it suggests a layered and complex approach, building on user individuality.

7.5 Recommendations

One of the objectives of this work, as mentioned in chapter 3, was to generate recommendations for countering phishing. The unrepresentative nature of the sampling used in the research makes it difficult to form any definitive recommendations for the banking industry as a result of the work but section 7.1.5 does contain comments about improving anti-phishing techniques and section 7.3.2 contains recommendations for further work. Chapter 4 closed on a list of suggestions from the experts – these could be further investigated as opposed to implemented immediately. The only recommendation that it appears safe to make as a result of the research is that the confusion about what phishing is and thus how to counter it needs to be further investigated and if verified, acted on.

7.6 Conclusion

In conclusion, the dissertation produced some interesting answers to the research questions posed in the introduction and throughout the work about user attitudes, behaviours, and reactions to phishing and anti-phishing efforts. Some of the findings may even go some distance towards reducing the cost of phishing set out in the introduction to this work.

It has also left the potential for interesting further work into individual responses in this area, particularly into how the propensity to fall for phishing may relate to other types of banking behaviour and into layered authentication responses.

8 Bibliography

About UK Payments. (2010). Retrieved June 22, 2012, from UK Payments: http://www.ukpayments.org.uk/about_ukpayments/

Alpar, G., Hoepman, J.-H., and Siljee, J. (2011, January 2). *The Identity Crisis. Security, Privacy and Usability Issues in Identity Management*. Retrieved January 19, 2012, from Cornell University Library: <http://arxiv.org/abs/1101.0427>

Amichai-Hamburger, Y. (2007). Personality, Individual Differences and Internet Use. In A. Joinson, K. McKenna, T. Postmes, and U.-D. Reips, *The Oxford Handbook of Internet Psychology* (pp. 187-204). Oxford: Oxford University Press.

Anandpara, V., Dingman, A., Jakobsson, M., Liu, D., and Roinestad, H. (2007). Phishing IQ Tests Measure Fear, Not Ability. *Lecture Notes in Computer Science*, 362-366.

Anderson, R. (2007). Closing the Phishing Hole: Fraud, Risk and Non-banks. *Nonbanks in the Payments System*. Kansas: Federal Reserve Bank of Kansas City.

Anti Phishing Working Group. (2011). *Phishing Activity Trends Report 1st Half 2011*. APWG.

Avison, D., Lau, F., Myers, M., and Nielsen, P. A. (1999). Action Research. *Communications of the ACM*, 94-97.

Balliet, D., Li, N., MacFarlan, S., and van Vugt, M. (2011). Sex Differences in Co-operation: A Meta-Analytic Review of Social Co-operation. *Psychological Bulletin*, pp. 881-909.

Baym, N. (2010). *Personal Connections in the Digital Age*. Cambridge: Polity Press.

Baym, N. (1998). The Emergence of On-line Community. In S. (. Jones, *Cybersociety: communication and community* (pp. 35-68). Newbury Park: Sage.

BBC. (2012, May 9). *Queen's Speech: Internet monitoring plan to have 'strict safeguards'*. Retrieved May 13, 2012, from BBC: <http://www.bbc.co.uk/news/uk-politics-18003315>

Birley, G., and Moreland, N. (1998). *A Practical Guide to Academic Research*. London: Kogan Page.

Blaxter, L., Hughes, C., and Tight, M. (2006). *How to Research*. Maidenhead: McGraw Hill Education.

Boodaiei, M. (2011, August 3). *What a Difference a Year Makes*. Retrieved May 7, 2012, from Trusteer: <http://www.trusteer.com/blog/what-difference-year-makes>

Castells, M. (1997). *The Power of Identity*. Oxford: Blackwell Publishers.

Castells, M. (2000). *The Rise of the Network Society, 2nd ed*. Oxford: Blackwell Publishers.

Chester, A., and Bretherton, D. (2007). Impression Management and Identity Online. In A. Joinson, K. McKenna, T. Postmes, and U.-D. Reips, *The Oxford Handbook of Internet Psychology* (pp. 224-236). Oxford: Oxford University Press.

Chi square test. (2005). Retrieved April 12, 2012, from Graphpad software:
<http://www.graphpad.com/quickcalcs/chisquared2.cfm>

Compeau, D., and Higgins, C. (1995, June). *Computer self-efficacy: development of a measure and initial test*. Retrieved March 3, 2012, from Gale Expanded Academic ASAP (MIS Quarterly): http://go.galegroup.com/ps/retrieve.do?sgHitCountType=None&sort=DA-ASC-SORTandinPS=true&prodId=GPSanduserGroupName=napier&tabID=T002andsearchId=R1andresultListType=RESULT_LISTandcontentSegment=andsearchType=BasicSearchFormandcurrentPosition=7andcontentSet=GALE|A17380216and

Consumer Direct. (2012). *Fraudulent Websites: Police Operation*. Retrieved April 22, 2012, from FindLaw: http://findlaw.co.uk/law/consumer/consumer_protection/22284.html

Cooper, R., and Evans, M. (2006, Winter). Breaking from Tradition: Market Research, Consumer Needs, and Design Futures. *Design Management Review*, pp. 68-74.

Creswell, J. (2009). *Research Design*. Thousand Oaks, CA: Sage Publications.

Davis, F., Bagozzi, R., and Warshaw, P. (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Management Science*, 982-1003.

Dawson, C. (2007). *A Practical Guide to Research Methods*. Oxford: How To Books.

Dhamija, R., and Dusseault, L. (2008). The Seven Flaws of Identity Management. *IEEE Security and Privacy*, 24-29.

Dhamija, R., Tygar, J., and Hearst, M. (2006). Why Phishing Works. *Computer Human Interaction*. Montreal: ACM.

Dhanendran, A. (2010, February 18). *Trusteer Rapport*. Retrieved May 14, 2012, from Computer Active: <http://www.computeractive.co.uk/ca/review/1915381/trusteer-rapport>

Downs, J., Holbrook, M., and Crainor, L. F. (2007). *Behavioural Response to Phishing Risk*. Pittsburgh: Institute for Software Research, Carnegie Mellon University.

Downs, J., Holbrook, M., and Crainor, L. F. (2006). *Decision Strategies and Susceptibility to Phishing*. Pittsburgh: Institute for Software Research, Carnegie Mellon University.

ed: Roessler, T., and Saldhana, A. (2010, August 12). *Web Security Context: User Interface Guidelines*. Retrieved January 28, 2012, from W3C: <http://www.w3.org/TR/wsc-ui/>

Egelman, S., Cranor, L. F., and Hong, J. (2008). You've Been WARNed: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings. *CHI 2008*. Florence: ACM.

Ellison, N., Heino, R., and Gibbs, J. (2006). Managing Impressions Online: Self-Presentation Processes in the Online Dating Environment. *Journal of Computer Mediated Communication*, 415-441.

Financial Fraud Action UK. (2012, March 7). *2011 Fraud Losses Continue Downward Trend*. Retrieved March 25, 2012, from UK Payments Administration: <http://www.financialfraudaction.org.uk/cms/assets/1/end%20of%20year%20fraud%20figures%20final.pdf>

Fink, A. (2006). *How to Conduct Surveys*. London: Sage.

Finread. (2009). Retrieved March 1, 2012, from CEN - European Committee for Standardisation: <http://www.cen.eu/cen/Sectors/Sectors/ISSS/CEN%20Workshop%20Agreements/Pages/FINREAD.aspx>

Frangi, L. (2010, August 24). *The UK's Media Consumption Habits*. Retrieved May 5, 2012, from We are social: <http://wearesocial.net/blog/2010/08/uks-media-consumption-habits/>

FraudWatch International. (2012). *Phishing Web Site Methods*. Retrieved April 30, 2102, from FraudWatch International: <http://www.fraudwatchinternational.com/phishing-fraud/phishing-web-site-methods/>

Frederick, S. (2005). Cognitive Reflection and Decision Making. *Journal of Economic Perspectives* , 25-42.

Furnell, S. (2007, March). Phishing: Can we spot the signs? *Computer Fraud and Security* , pp. 10-15.

Goffman, E. (1974). *Frame Analysis*. London: Peregrine Books.

Goffman, E. (1965). On Face-Work. In E. Goffman, and J. Best, *Interaction Ritual: Essays in Face to Face Behaviour*. Chicago: Aldine Publishing Co.

Goffman, E. (1959). *The Presentation of Self in Everyday Life*. Harmondsworth: Penguin.

Grix, J. (2004). *The Foundations of Research*. Basingstoke: Palgrave Macmillan.

Gross, B. (2010). Online identifiers in everyday life. Urbana : University of Illinois.

Grover, A., Berghel, H., and Cobb, D. (2011). The State of the Art in identity Theft. In M. Zelkowitz, *Advances in Computers vol 83* (pp. 2-47). London: Elsevier.

Hopkins, N. (2012, May 15). *Cyber security should be promoted with hard-hitting ad campaign, says Labour*. Retrieved May 15, 2012, from Guardian Online: <http://www.guardian.co.uk/technology/2012/may/15/cyber-security-ad-campaign-labour>

Iliev, D., and Sun, Y. B. (2010). *Website forgery prevention*. IEEE.

Infosecurity Magazine. (2012, April 9). Hack compromises personal data of Utah Medicaid recipients. *Infosecurity Magazine* .

Internet World Stats. (2011, July 12). *Canada*. Retrieved May 7, 2012, from Internet World Stats: <http://www.Internetworldstats.com/am/ca.htm>

Internet World Stats. (2011, February 14). *North American Internet Stats*. Retrieved May 7, 2012, from Internet World Stats: <http://www.Internetworldstats.com/am/us.htm>

Jagatic, T., Johnson, N., Jakobsson, M., and Menczer, F. (2007). Social Phishing. *Communications of the ACM* .

Kohn, A. (1998). Challenging Behaviorist Dogma: Myths About Money and Motivation. *Compensation and Benefits Review* , 27-37.

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., et al. (2009). *School of Phish: A Real-World Evaluation of Anti-Phishing Training*. Pittsburgh: Cylab.

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F., et al. (2007). Getting Users to Pay Attention to Anti-Phishing Education: Evaluation of Retention and Transfer. *APWG eCrime Researchers Summit*. Pittsburgh: Institute for Software Research, Carnegie Mellon University.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., and Hong, J. (2007). *Teaching Johnny Not to Fall for Phish*. Pittsburgh: CyLab.

Leyden, J. (2012, May 6). *Cybercrims dump email for irresistible Facebook, Twitter spam*. Retrieved May 6, 2012, from The Register: http://www.theregister.co.uk/2012/05/06/social_network_spam/

Mannan, M., and van Oorschot, P. (2010, August 12). Leveraging Personal Devices for Stronger Password Authentication from Untrusted Computers. *Journal of Computer Security* , 703-750.

McLoughlin, I. (1999). *Creative Technological Change*. London: Routledge.

Myers, M. (2011, November 12). *Qualitative Research in Information Systems*. Retrieved March 6, 2012, from Association for Information Systems: <http://www.qual.auckland.ac.nz/>

National Fraud Authority. (2012). Retrieved June 22, 2012, from Home Office: <http://www.homeoffice.gov.uk/agencies-public-bodies/nfa/>

Nielsen, J. (2004, October 25). *User Education is Not the Answer to Security Problems*. Retrieved February 23, 2012, from Alertbox: <http://www.useit.com/alertbox/20041025.html>

Office for National Statistics. (2011, August 31). *Household Internet Access*. Retrieved May 7, 2012, from Office for National Statistics: <http://www.ons.gov.uk/ons/rel/rdit2/Internet-access---households-and-individuals/2011/stb-Internet-access-2011.html#tab-Household-Internet-Access>

Orlikowski, W., and Baroudi, J. (1991). Studying Information Technology in Organisations: Research Approaches and Assumptions. *Information Systems Research* .

Parno, B., Kuo, C., and Perrig, A. (2006). *Phoolproof Phishing Prevention*. Retrieved March 1, 2012, from Carnegie Mellon University: <http://sparrow.ece.cmu.edu/~parno/phishing/>

Parsons, K., McCormac, A., Butavicius, M., and Ferguson, L. (2010). *Human Factors and Information Security: Individual, Culture and Security Environment*. Edinburgh, Southern Australia: Australian Government Department of Defence.

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., and Butavicius, M. (2012). Why do some people manage phishing emails better than others? *HAISA 2011*. London: Emerald Group Publishing.

Phishing Attack Trends Report 1H 2011. (2011, December 23). Retrieved January 30, 2012, from APWG: <http://www.antiphishing.org/phishReportsArchive.html>

Pieters, W., and Coles-Kemp, L. (2011). Reducing Normative Conflicts in Information Security. *New Security Paradigms Workshop*. Marin County: ACM.

Police Central e-Crime Unit. (2012). Retrieved June 22, 2012, from Metropolitan Police: <http://www.met.police.uk/pceu/>

Ranum, M. (2006). *User Education*. Retrieved March 2, 2012, from Ranum.com: http://www.ranum.com/security/computer_security/editorials/point-counterpoint/users.html

Research Methods Knowledge Base. (2006, October 20). *The t-test*. Retrieved April 12, 2012, from Web Center for Social Research Methods: http://www.socialresearchmethods.net/kb/stat_t.php

Riegelsberger, J., and Sasse, M. A. (2008). *Ignore These At Your Peril: Ten principles for trust design*. Retrieved March 3, 2012, from ucl.ac.uk: http://hornbeam.cs.ucl.ac.uk/hcs/publications/Riegelsberger+Sasse_Ignore%20These%20At%20Your%20Peril_Ten%20principles%20for%20trust%20design_TRUST2010.pdf

Rouse, M. (2005, September). *Domain Name System*. Retrieved June 22, 2012, from searchnetworking: <http://searchnetworking.techtarget.com/definition/domain-name-system>

Rubin, H., and Rubin, I. (2005). *Qualitative Interviewing - the Art of Hearing Data*. London: Sage Publications.

Sample, I. (2012, February 2). *MPs call for media campaign to raise awareness of cybercrime*. Retrieved February 2, 2012, from The Guardian Online: <http://www.guardian.co.uk/technology/2012/feb/02/mps-media-campaign-awareness-cybercrime>

Schechter, S., Rachna, D., Ozment, A., and Fischer, I. (2007). The Emperor's New Security Indicators. *The 2007 IEEE Symposium on Security and Privacy*. Oakland: IEEE.

Schneier, B. (2006, August 22). *Educating Users*. Retrieved March 2, 2012, from Schneier on Security: http://www.schneier.com/blog/archives/2006/08/educating_users.html

Security Awareness for the 21st Century. (n.d.). Retrieved April 22, 2012, from SANS Securing the Human: <http://www.securingthehuman.org/>

Sheng, S., Kumaraguru, P., Acquisti, A., Cranor, L., and Hong, J. (2009). Improving Phishing Countermeasures: An Analysis of Expert Interviews. *eCRIME '09* (pp. 1-15). Tacoma: IEEE.

SOCA. (2012). Retrieved June 22, 2012, from SOCA: <http://www.soca.gov.uk/>

Soghoian, C., and Jakobsson, M. (2007, April 10). *A Deceit-Augmented Man In The Middle Attack Against Bank of America's SiteKey® Service*. Retrieved February 26, 2012, from slight paranoia: <http://paranoia.dubfire.net/2007/04/deceit-augmented-man-in-middle-attack.html>

Stahl, B. C. (2008). *Information Systems Critical Perspectives*. Abingdon: Routledge.

Straub, D., Gefen, D., and Boudreau, M.-C. (2004). *Quantitative, Positivist Research Methods in Information Systems*. Retrieved March 4, 2012, from The ISWorld Quantitative, Positivist Research Methods Website: <http://dstraub.cis.gsu.edu:88/quant/>

Sun, B., Wen, Q., and Liang, X. (2010). A DNS based Anti-Phishing Approach. *Second International Conference on Networks Security, Wireless Communications and Trusted Computing* (pp. 262-265). Wuhan: IEEE Computer Society.

Table of critical values of t. (n.d.). Retrieved April 12, 2012, from Sussex University: <http://www.sussex.ac.uk/Users/grahamh/RM1web/t-testcriticalvalues.pdf>

Taylor, R. (2008). The Social Side of Security. In T. Kidd, and I. Chen, *Social Information Technology* (pp. 140-150). London: IGI Global.

Tetard, F., and Collan, M. (2009). Lazy User Theory: A Dynamic Model to Understand User Selection of Products and Services. *Proceedings of the 42nd Hawaii International Conference on System Sciences - 2009*. Hawaii: IEEE.

Trusteer. (2009, December 2). *Measuring the Effectiveness of In-the-wild Phishing Attacks*. Retrieved April 12, 2012, from Trusteer.com: <http://www.trusteer.com/sites/default/files/Phishing-Statistics-Dec-2009-FIN.pdf>

Turkle, S. (1996). *Life on the Screen: Identity in the Age of the Internet*. New York: Simon and Schuster.

Ventakesh, Viswanath, Morris, M., Davis, G., and Davis, F. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly* , 425-478.

Verisign. (2012). Retrieved June 22, 2012, from Verisign: <https://www.verisign.co.uk/>

Weigold, T., and Hiltgen, A. (2011). Secure Confirmation of Sensitive Transaction Data in Modern Internet Banking Services. *World Congress on Internet Security 2011*. London: IEEE.

Whitman, M. E., and Mattord, H. J. (2012). *Principles of Information Security*. Andover: Cengage Learning.

Wilson, C., and Argles, D. (2011). The Fight against Phishing: Technology, the End User and Legislation. *i-Society 2011* (pp. 501-504). London: IEEE.

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology* , 662-674.

Wu, M., Miller, R., and Garfinkel, S. (2006). Do Security Toolbars Actually Prevent Phishing Attacks? *CHI 2006* (pp. 601-610). Montreal: ACM.

Yu, W., Nargundkar, S., and Tiruthani, N. (2008). A Phishing Vulnerability Analysis of Web Based Systems. *Symposium on Computers and Communications* (pp. 326-331). Marrakech: IEEE.

Zhao, S. (2006). Cyber-gathering places and online-embedded relationships. *presented at Annual Meeting of the Eastern Sociological Society* . Boston.

Zhao, S., Grasmuck, S., and Martin, J. (2008). Identity construction on Facebook: Digital empowerment in anchored relationships. *Computers in Human Behaviour* , 1816-1836.

Appendices

9 A1 - Glossary

2FA – two factor authentication, authentication using two out of three authentication types - something you know, something you have and something you are. Often refers in banking to use of card reader devices with a numeric keypad that generate one time authentication codes based on the card pin and transaction data.

419 scams – scams where people are asked to supply an amount of money to facilitate the release of a larger amount of money currently frozen in a bank account. Typically operated by Nigerian fraudsters and named after a part of the Nigerian penal code.

Anti-foundationalism – an approach that rejects the idea of a fundamental or founding belief or principle (Grix, 2004, p. 61).

Authentication – the process of ensuring an individual or process is who he/she claims to be (Whitman and Mattord, 2012, p582).

Authorisation – the process of ensuring an authenticated individual has access rights to a particular service (Whitman and Mattord, 2012, p582).

AV – anti-virus software.

Digital identity – a set of data that uniquely identifies a person or thing online. Not to be confused with online identity, which is the online persona that an individual creates from their online activities.

DNS – Domain Name System – naming system for computers and other resources connected to the Internet (Rouse, 2005).

EMV – interoperable smart card based credit and debit payments standard created by Visa, MasterCard and Europay, widely used except in US.

Hand held authentication devices – devices that generate a one-time passcode to authenticate logins or transactions (see 2FA)

MUD/MMORPG – multi-player online virtual environment, now more commonly referred to massively multi-player online role playing game.

Mutual authentication – the process or ways in which a user ensures that they are on the correct website.

NFA – National Fraud Authority – UK Home Office Executive Agency fighting fraud (National Fraud Authority, 2012).

Phisher-controlled proxies – a man in the middle attack where consumer to bank communications are passed through a proxy system that collects data.

Phishing - the act of tricking individuals online into revealing sensitive information, for example passwords or PINs and other banking details.

PKI – public key infrastructure

Police Central e-crime Unit – Metropolitan Police unit investigating computer crime (Police Central e-Crime Unit, 2012)

SANS – online computer security information resource at www.sans.org.

Single sign-on – access control system that allows user to access multiple systems while logging in once (Alpar, Hoepman, and Siljee, 2011).

Social engineering – techniques used to trick people into disclosing information.

SOCA – UK Serious Organised Crime Agency – national police agency fighting organised crime (SOCA, 2012).

Spearphishing – a highly personalised phishing attack aimed at a single individual, often intended to obtain access to corporate resources such as trade secrets or source code.

SSL – Secure Sockets Layer - Transport Layer cryptographic protocol providing secure communications online.

UK Payments Administration – UK banking industry trade body (About UK Payments, 2010).

Verisign – authentication services provider and certificate authority (Verisign, 2012).

10 A2 - Project management

10.1 Discussion

The project was managed by creating a schedule of major and interim milestones, detailed in the table below. An agenda was prepared for each supervisor meeting and tasks were agreed and diaried during each meeting. Progress was tracked and as the project developed, target dates were either met or revised as necessary.

However management of the project suffered from a number of issues that would have ideally been avoided. Topic choice would have been better made during the term preceding the dissertation but thanks to the academic demands of the preceding term was not finalised until shortly before the proposal deadline, reducing the amount of time available for focused exploratory reading and producing a level of doubt about the topic that continued throughout the project and somewhat hindered progress at times. Nonetheless, the initial topic choice deadline was met.

Academic research methodology turned out to be very much more complex (and interesting) than expected and reading about this was not started early enough. The qualitative social sciences aspect of the project, which was somewhat outside the norm for projects associated with the Advanced Security and Digital Forensics course, meant that this involved gaining rapid knowledge of topics and approaches that had not been encountered before.

Similarly, questionnaire design also turned out to be a more complicated area of endeavour than expected and more time to study this skill would have led to a better designed and better tested survey.

In general, the short time scale of the project made it challenging to build in contingency planning for delays. Earlier delays caused by a slightly higher number of interviews than originally planned for were compensated for and the major deadline of the survey closing date was met. However the much higher than expected number of survey responses meant that the initial submission deadline of 30th April was not possible without cutting down considerably on the amount of data analysis possible. At this point, the decision was taken, in agreement with the project supervisor, to analyse the data thoroughly and so to aim for the August completion deadline rather than the original April one. In addition the large amount of data meant that early drafts of the survey findings chapter had to be rewritten and reduced several times to produce a chapter of acceptable length. In the end however, the survey analysis produced was of a higher standard than would have been possible had the April deadline been met. Unexpected health issues also caused scheduling delays.

Overall, the experience of managing this project provided useful learning that could be used to avoid similar issues in any future research projects of a similar or larger nature.

10.2 Project Plan

Full revision 27/2/12

Major milestones highlighted

Milestone	Comment about any changes to deadline	Deadline	Revised deadline	Actual
Literature review first draft complete		2/3/12		3/3/12
Deliver initial report to supervisor and 2nd marker		4/3/12		3/3/12
Reading about methodology	Despite extensive commercial experience of conducting research, many academic research methodology concepts were new to me – reading was more challenging and took longer than expected.	2/3/12	6/3/12	6/3/12
Identify expert interview targets		24/2/12		24/2/12
Request interviews	Felt it important to formulate firmer research questions from literature review first. Interviewees also suggested further interview targets meaning that further invitations were extended.	2/3/12	6/3/12	12/3/12
Conduct interviews	Changed due to decision to conduct interviews and questionnaire sequentially and not concurrently	30/3/12	23/3/12	23/3/12
Transcribe interviews		30/3/12		24/3/12
Devise online user questionnaire	This was a much harder task than initially expected.	16/3/12		21/3/12
Launch questionnaire	Delayed due to delay in finalising questions	19/3/12	21/3/12	21/3/12
Promote questionnaire		23/3/12		23/3/12
Questionnaire closing date		30/3/12		30/3/12
Complete analysis of interviews and	Devising the codes for the interviews took	13/4/12	29/4/12	1/5/12

questionnaire	longer than expected. The far greater number of survey replies and the need to adjust the data for gender balance also meant that far more time was needed for questionnaire analysis than initially expected.			
Final write up	Impacted by extra time needed for analysis and by unexpected health problems.	23/4/12	11/5/12	29/6/12
Print and bind	Work and other commitments in May mean there will be a gap between concluding and final edits. Ill health caused further delays.	27/4/12	13/7/12	10/8/12
Final submission of report		30/4/12	13/7/12	10/8/12

11 A3 - Summary of literature review findings in chart form

Research question	Breakdown of issues	Major references
Why do users fall for phishing?	Skill of the phisher	Yu, Nargundkar, and Tiruthani, 2008 Anandpara, Dingman, Jakobsson, Liu, and Roinestad, 2007 Jagatic, Johnson, Jakobsson, and Menczer, 2007 Dhamija, Tygar, and Hearst, 2006
	Lack of awareness and understanding of phishing	Yu, Nargundkar, and Tiruthani, 2008 Anandpara, Dingman, Jakobsson, Liu, and Roinestad, 2007 Kumaraguru, Sheng, Acquisti, Cranor, and Hong, 2007 Furnell, 2007
	Complacency about existing knowledge and protection	ed: Roessler and Saldhana, 2010 Egelman, Cranor, and Hong, 2008 Taylor 2008
	Carelessness and lack of interest	Downs, Holbrook, and Crainor, 2006 Downs, Holbrook, and Crainor, 2007
	Focus on site content, graphics rather than security indicators	Downs, Holbrook, and Crainor, 2006 Dhamija, Tygar, and Hearst, 2006 Furnell, 2007 Schechter, Rachna, Ozment, and Fischer, 2007 Egelman, Cranor, and Hong, 2008
	Ignorance of security procedures	ed: Roessler and Saldhana, 2010 Dhamija, Tygar, and Hearst, 2006
	Focus on primary task	Dhamija, Tygar, and Hearst, 2006 Wu, Miller, and Garfinkel, 2006 ed: Roessler and Saldhana, 2010 Anandpara, Dingman, Jakobsson, Liu, and Roinestad, 2007
	Ritual nature of task activity	Riegelsberger and Sasse, 2008
	Banks/website owners cause confusion by not following own guidelines or by having poor security practices	Wu, Miller, and Garfinkel, 2006
	Social context	Jagatic, Johnson, Jakobsson and Menczer, 2007

	Whether security is viewed as a primary or secondary task	Dhamija, Tygar, and Hearst, 2006 Wu, Miller, and Garfinkel, 2006
	Amount of effort required to protect self	Ventakesh, Viswanath, Morris, Davis, and Davis, 2003 Tetard and Collan, 2009
	Perceived severity of the risk (no impact)	Downs, Holbrook, and Crainor, 2007
How do users react to existing anti-phishing methods?	Education too complex	Sample, 2012
	Security indicators are not effective/are ignored	ed: Roessler and Saldhana, 2010 Schechter, Rachna, Ozment, and Fischer, 2007 Wu, Miller, and Garfinkel, 2006
	Confused by warnings, indicators and education	Kumaraguru, Sheng, Acquisti, Cranor, and Hong, 2007 Wu, Miller, and Garfinkel, 2006 Egelman, Cranor, and Hong, 2008
	Effectiveness of education – is it effective or not?	Downs, Holbrook and Crainor 2006 Downs, Holbrook, and Crainor, 2007 Yu, Nargundkar, and Tiruthani, 2008 Kumaraguru, Sheng, Acquisti, Cranor, and Hong, 2007 Nielsen, 2004 Schneier, 2006
	Does education increase fear rather than efficacy?	Anandpara, Dingman, Jakobsson, Liu, and Roinestad, 2007
Do personality factors have any effect on how people deal with phishing?	Personality traits (extraversion)	Pattinson, Jerram, Parsons, McCormac and Butavicius 2012
	Degree of impulsiveness	Pattinson, Jerram, Parsons, McCormac and Butavicius 2012 Kumaraguru, Rhee, Sheng, Hasan, Acquisti, Cranor and Hong, 2007
	Concern about what send of email thinks of recipient	Downs, Holbrook, and Crainor, 2006
	Attitudes to authority	Personal deduction Wu, Miller, and Garfinkel, 2006
	Age – does/does not	Dhamija, Tygar, and Hearst, 2006 Kumaraguru, et al., 2009
How can existing anti-phishing methods be improved?	Use of active warnings that cannot be ignored	Wu, Miller, and Garfinkel, 2006 Egelman, Cranor, and Hong, 2008 ed: Roessler and Saldhana, 2010
	Consistent interfaces	Dhamija and Dusseault, 2008 ed: Roessler and Saldhana, 2010
	Use of site authentication message not helpful	Schechter, Rachna, Ozment, and Fischer, 2007

	Role of mobile devices in authentication	Mannan and van Oorschot, 2010
	Embedded education	Wu, Miller, and Garfinkel, 2006 Kumaraguru, et al., 2009 Kumaraguru, et al., 2007
	Making education relevant to the real world/more personalised	Wilson and Argles, 2011 Kumaraguru, et al., 2009 Parsons, McCormac, Butavicius, and Ferguson, 2010
	Use of positive reinforcement	Parsons, McCormac, Butavicius, and Ferguson, 2010
	Use of negative reinforcement	Ranum, 2006
	Understanding the web environment and URLs	Downs, Holbrook, and Crainor, 2007
	Understanding anti-phishing education messages	Kumaraguru, et al., 2009
	Receiving more frequent/regular education	Pattinson, Jerram, Parsons, McCormac and Butavicius 2012 Kumaraguru, et al., 2009
What is the relationship between online and offline behaviour and how does it impact the response to phishing?		Baym 2010 Turkle 1996 Zhao 2006
Whose responsibility is it to protect the user against phishing?	Is it a social or technical issue?	Taylor, 2008 Wilson and Argles, 2011 Schneier, 2006

12 A4 - Expert interview questions

Thank you for agreeing to talk to me. During this interview I will be asking questions about user experiences of phishing and industry approaches to preventing phishing being successful. I have a set list of questions but if there are any points I do not raise that you feel are worth discussing, please do let me know. I will be recording the interview and providing you with a transcript afterwards.

These are some general introductory questions to start off with about phishing.

- 1 What is your stereotype of someone who falls for phishing?
- 2 Why do people fall for phishing?
- 3 How should responsibility for protecting users against phishing be shared?
- 4 How would you balance people issues against technology issues in combating phishing?

Now I am going to ask some questions about how people's attitudes and reactions to phishing. Previous academic research in this area raises a wide variety of perspectives – I am interested to see how these fit in with the industry view.

- 5 What do you think that people look out for and what do they think about when they are trying to decide whether a website or email is genuine or not?
- 6 How do people's attitudes to online security compare to their attitudes to offline security and why?
- 7 Do personality types and attitudes to authority make a difference to how people react to phishing and has anyone ever investigated this in a non-academic sense?
- 8 Have you or do you know anyone who has done work to discover whether propensity to fall for phishing correlate with other non-ideal banking behaviours, for example incurring unauthorised overdrafts?

Now I am going to ask about anti-phishing education.

- 9 What sort of anti-phishing education initiatives are you aware of and how effective do you think they are?
- 10 What would improve them?
- 11 What do you think that users think of anti-phishing education?

A final couple of questions.

12 What would you like to know about the user's perspective of phishing?

13 How do you think that the current situation will evolve?

14 Is there anything we've not discussed you'd like to add?

Thank you very much for your help. I will transcribe your answers and send them to you for checking and changing if you wish.

Can you suggest anyone else with an expert knowledge of this area who you think might be willing to help?

13 A5 - Data and questions from the user survey

13.1 Answers to survey questions

This chapter presents the results of the online user survey. Because the gender split of the respondents was not even, with a 5:2 ratio in favour of women and because on first sight there appears to be differences in response between the genders, the data as it stands cannot be extrapolated to the general population (although the self selected nature of the sample means that is the case anyhow). Therefore the answers will be presented firstly as drawn from the raw data and then split by gender. For the purposes of simplification and because the number of female respondents was so much larger, anyone identifying as neither male nor female has been added to the female replies. The coloured charts are produced by the Smart Survey software and as they are self explanatory are not captioned.

www.smart-survey.co.uk/v.asp?i=49296baiff

Google

Staying safe online

17%

Introductory questions

These questions will help me better understand your other answers.

Page 2 of

1) How old are you?








- ☐ under 18
- ☐ 18-25
- ☐ 26-35
- ☐ 36-45
- ☐ 46-55
- ☐ 56-65
- ☐ older than 65

2) What is your gender?

Figure 5 Introductory questions of the survey

Introductory questions

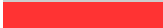


1) How old are you?

			Response Percent	Response Total
1	under 18		0.57%	2
2	18-25		39.38%	139
3	26-35		25.50%	90
4	36-45		12.75%	45
5	46-55		14.45%	51
6	56-65		6.80%	24
7	older than 65		0.57%	2
			answered	353
			skipped	1

Age	% of answers adjusted	Men	Women	% of answers unadjusted
under 18	0.4%	0.00%	0.80%	0.57%
18-25	34.27%	22.55%	46.00%	39.38%
26-35	23.80%	19.61%	28.00%	25.50%
36-45	15.38%	21.57%	9.20%	12.75%
46-55	16.00%	19.61%	12.40%	14.45%
56-65	9.15%	14.71%	3.60%	6.80%
older than 65	0.98%	1.96%	0.00%	0.57%

Table 4 Age of respondents

2) What is your gender?

			Response Percent	Response Total
1	male		28.98%	102
2	female		69.89%	246
3	other/prefer not to answer		1.14%	4
			answered	352
			skipped	2

3) How great is your knowledge of computing?				
			Response Percent	Response Total
1	very low		1.99%	7
2	medium low		38.64%	136
3	medium high		45.17%	159
4	expert		14.20%	50
			answered	352
			skipped	2

Knowledge of computing	% of answers adjusted	Men	Women	% of answers unadjusted
very low	1.4%	0.00%	2.81%	1.99%
medium low	32.52%	17.65%	47.39%	38.64%
medium high	45.24%	45.10%	45.38%	45.17%
expert	20.96%	37.25%	4.42%	14.20%

Table 5 Computing knowledge of respondents

4) In everyday life, how quickly do you make decisions?				
			Response Percent	Response Total
1	very quickly		14.45%	51
2	medium quickly		57.22%	202
3	medium slowly		26.06%	92
4	very slowly		2.27%	8
			answered	353
			skipped	1

Decision speed	% of answers adjusted	Men	Women	% of answers unadjusted
very quickly	14.84%	15.69%	14.00%	14.45%
medium quickly	55%	50.00%	60.00%	57.22%
medium slowly	27.39%	30.39%	24.40%	26.06%
very slowly	2.76%	3.92%	1.60%	2.27%

Table 6 Decision speed of respondents

Questions about your views on security

5) How great is your level of concern about becoming a victim of computer crime – phishing for example?				
			Response Percent	Response Total
1	very low		17.33%	61
2	medium low		40.91%	144
3	medium high		32.67%	115
4	very high		9.09%	32
			answered	352
			skipped	2



Level of concern - online	% of answers adjusted	Men	Women	% of answers unadjusted
very low	18.61%	21.57%	15.66%	17.33%
medium low	40%	38.24%	41.77%	40.91%
medium high	32.93%	33.33%	32.53%	32.67%
very high	8.45%	6.86%	10.04%	9.09%

Table 7 Level of concern about online crime

6) How great is your level of concern about becoming a victim of non-computer crime – mugging or burglary/home invasion for example?				
			Response Percent	Response Total
1	very low		20.68%	73
2	medium low		47.88%	169
3	medium high		24.08%	85
4	very high		7.37%	26
			answered	353
			skipped	1


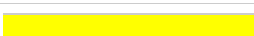
Level of concern - offline	% of answers adjusted	Men	Women	% of answers unadjusted
very low	22.81%	28.43%	17.20%	20.68%
medium low	48.89%	50.98%	46.80%	47.88%
medium high	21.93%	16.67%	27.20%	24.08%
very high	6.36%	3.92%	8.80%	7.37%

Table 8 Level of concern about offline crime

7) Have you ever entered your financial details into a website and as a result later lost money through fraud?				
			Response Percent	Response Total
1	yes		9.97%	35
2	no		90.03%	316
			answered	351
			skipped	3





Online fraud victims	% of answers adjusted	% of answers unadjusted
yes	9.97%	9.97%
no	90.03%	90.03%

Table 9 Victims of online crime

8) Have you ever been the victim of any other form of crime?				
			Response Percent	Response Total
1	yes		55.11%	194
2	no		44.89%	158
			answered	352
			skipped	2

Other crime victim	% of answers adjusted	Men	Women	% of answers not adjusted
yes	58.86%	67.33%	50.40%	55.11%
no	41.14%	32.67%	49.60%	44.89%

Table 10 Victims of other forms of crime

9) When you are carrying out online banking tasks, do you read the security messages on the banking website?				
			Response Percent	Response Total
1	always		25.50%	90
2	sometimes		44.48%	157
3	rarely		17.00%	60
4	never		5.10%	18
5	I don't bank online		7.93%	28
			answered	353
			skipped	1

Reading security messages	% of answers adjusted	Men	Women	% of answers not adjusted
always	24.96%	23.53%	26.40%	25.50%
sometimes	43.1%	40.20%	46.00%	44.48%
rarely	17.8%	19.61%	16.00%	17.00%
never	5.05%	4.90%	5.20%	5.10%
I don't bank online	9.08%	11.76%	6.40%	7.93%

Table 11 How often bank security messages are read



Question 10 asked for comments about answers on the preceding page: selected comments are listed here:

- The crime case was my credit card being cloned - possibly through on-line activity, but I do not know for sure how details were obtained.
- I do a lot of online shopping for my mother, with her card so am vigilant to not expose her to credit card fraud.
- As a savvy user, I keep a close eye out for scams. This makes me feel relatively secure about avoiding cyber crime.
- Identify theft happened one time while purchasing tickets through ticketmaster, and then through our credit card we purchased an identify theft protection plan; which later helped me sort out a fraudulent charge from amazon.com - both issues were rectified quickly.
- i work in finance and use online banking and other online financial services on a regular basis. i feel that i am protected as a consumer by credit card companies and banks who will take the loss in the event of an unauthorized transaction.
- for 8 - was a victim of fraudulent use of CC online, but never found out how details were shared - careful with online shopping, check certificates, use well known, reputable shopping sites etc.
- I am more concerned about physical action against me than any online crime
- <https://halifax.co.uk/> a bank
<https://halifax-online.co.uk/> who knows?
 Requires javascript = pointless vulnerabilities
 I will not bank online until my bank demonstrates at least noddy level understanding of security.

- Not all loss is financial, even if you do recover funds it can take a lot of time and effort to do so.
- burglary - easy to know I've locked the doors. Computer fraud - less easy to be certain so more concerned
- off-line crime was a phishing telephone claiming to be my mobile phone company - i fell for it and was fleeced for almost £1000
- Don't always read security messages since I have a BSc in computer forensics with a high amount of Security modules so am aware of the threats.
- My concern is low because I approach any kind of email, phone call or letter that supposedly comes from a bank with the greatest scepticism. The phishing attempts are usually easy to spot because they aren't addressed specifically to me and generally they are very unsophisticated.
- I don't feel concern about phishing/ hacking/ online fraud because I have all my emails and Internet security settings at maximum. Usually I can't access things I KNOW are safe!
- I think banks make it far too cumbersome for consumers in their security protocols, especially in regard to telephone banking; I detest banks' lack of customer service.
- mostly, i use paypal or online banking to do transactions and trust these systems to work well. Otherwise I'd use my credit card to pay which offers me fraud protection...
- I was reimbursed by the bank but it was very embarrassing to have been duped and very inconvenient to have to change bank account numbers etc

Questions about learning to avoid phishing

11) Have you ever seen any information about how to avoid phishing? If you answer yes to this question, please continue to question 12. If you answer no, please skip to question 16.

			Response Percent	Response Total
1	yes		74.72%	263
2	no		25.28%	89
			answered	352
			skipped	2

Has seen information about phishing	% of answers adjusted	Men	Women	% of answers not adjusted
yes	77.21%	83.33%	71.08%	74.72%
no	22.79%	16.67%	28.92%	25.28%



Table 12 Whether respondents have seen information about phishing

12) Who provided it? Please tick all that apply.				
			Response Percent	Response Total
1	bank		75.29%	198
2	Internet provider		31.94%	84
3	ebay		26.62%	70
4	paypal		40.68%	107
5	government		13.31%	35
6	newspaper		28.52%	75
7	television		22.81%	60
8	radio		8.37%	22
9	friends/family		33.08%	87
10	law enforcement body		4.94%	13
11	I can't remember		7.98%	21
12	Other, please specify:		23.57%	62
			answered	263
			skipped	91

The other sources of information, mentioned by 62 people in total were, in order of popularity: University – 12, online media – 12, workplace – 11, email provider (mainly gmail) – 7, social networking and media – 6, gaming sites – 2, tech sites – 2, general word of mouth – 2, antiphishing or security sites – 2, personal finance website – 2, Electronic Frontier Foundation – 1, colleague advice – 1, browser toolbar – 1, googled it – 1, 'myself' – 1, business club – 1, as part of degree course – 1.





Source of information	% of answers adjusted	Men	Women	% of answers unadjusted
bank	73.21%	67.44%	78.98%	75.29%
Internet provider	31.89%	31.40%	32.39%	31.94%
ebay	27.63%	31.40%	23.86%	26.62%
paypal	41.11%	43.02%	39.20%	40.68%
government	13.21%	12.79%	13.64%	13.31%
newspaper	28.45%	29.07%	27.84%	28.52%
television	21.5%	17.44%	25.57%	22.81%
radio	7.73%	5.81%	9.66%	8.37%
friends/family	28.89%	17.44%	40.34%	33.08%
law enforcement body	4.88%	4.65%	5.11%	4.94%
I can't remember	9.23%	12.79%	5.68%	7.98%
Other, please specify:	23.86%	24.42%	23.30%	23.57%

Table 13 Source of information seen about phishing

13) Did you read it? If you answer yes to this question, please continue to question 14. If you answer no, please skip to question 16.				
			Response Percent	Response Total
1	yes		93.54%	246
2	no		6.46%	17
			answered	263
			skipped	91



Did you read it?	% of answers adjusted	Men	Women	% of answers unadjusted
yes	94.28%	96.47%	92.09%	93.54%
no	5.72%	3.53%	7.91%	6.46%

Table 14 Whether information seen was read

14) How easy was the information to understand?				
			Response Percent	Response Total
1	too simple		8.91%	22
2	about right		87.04%	215
3	a bit too difficult		3.64%	9
4	much too difficult		0.40%	1
			answered	247
			skipped	107

Easy to understand	% of answers adjusted	Men	Women	% of answers unadjusted
too simple	10.59%	15.66%	5.52%	8.91%
about right	85.75%	81.93%	89.57%	87.04%
a bit too difficult	3.05%	1.20%	4.91%	3.64%
much too difficult	0.6%	1.20%	0.00%	0.40%

Table 15 How easy the information was to understand








15) Did you change your online behaviour because of it?				
			Response Percent	Response Total
1	yes		37.05%	93
2	no		62.95%	158
			answered	251
			skipped	103

Change of behaviour	% of answers adjusted	Men	Women	% of answers not adjusted
yes	34.26%	26.83%	41.67%	37.05%
no	65.75%	73.17%	58.33%	62.95%

Table 16 Whether behaviour changed as a result of seeing information

Source of information	% of people who changed behaviour - adjusted	Men	Women
bank	30.95%	24.1%	37.8%
Internet provider	36.3%	30.8%	41.8%
ebay	35.95%	23.1%	48.8%
paypal	31.25%	22.2%	40.3%
government	33.75%	30%	37.5%
newspaper	40.2%	30.4%	50%
television	34.75%	28.6%	40.9%
radio	32.5%	40%	25%
friends/family	43.9%	40%	47.8%
law enforcement body	36.1%	50%	22.2%
I can't remember	52.8%	50%	55.6%
Other, please specify:	30.8%	23.8%	37.8%

Table 17 Behaviour change by gender and source of information

16) Where would you be most willing to read information about protecting yourself from phishing? Please tick all that apply.				
			Response Percent	Response Total
1	Twitter		9.77%	34
2	Facebook		26.15%	91
3	on my bank website		68.39%	238
4	in a letter from my bank		52.59%	183
5	in newspapers		35.06%	122
6	in magazines		25.86%	90
7	Other, please specify:		14.37%	50
			answered	348
			skipped	6

Preferred information source	% of answers adjusted	Men	Women	% of answers not adjusted
Twitter	8.64%	6.93%	10.98%	9.77%
Facebook	24.04%	18.81%	29.27%	26.15%
on my bank website	68.89%	70.30%	67.48%	68.39%
in a letter from my bank	51.58%	49.50%	53.66%	52.59%
in newspapers	32.76%	27.72%	37.80%	35.06%
in magazines	23.63%	18.81%	28.46%	25.86%
Other, please specify:	14.83%	15.84%	13.82%	14.37%

Table 18 Preferred source of information about phishing



The 'other' channels suggested, in order of preference, were:

Trusted technology sites – 4, speciality anti-phishing advisory websites – 3, radio – 3, TV – 3, email provider – 2, speciality anti-phishing blog – 2, online media – 2, TV advertising – 2, work – 2, by email, source not specified – 2, government – 1, university – 1, Electronic Frontier Foundation – 1, word of mouth – 1, personal finance websites – 1, book – 1, from colleagues – 1, from a specialist security product provider – 1, from ISP – 1, PayPal – 1, online retailer sites – 1, from spouse – 1, email from bank – 1, magazines – 1, poster – 1, in classroom – 1, government – 1, 'on website where you might be a victim' – 1.

Question 17 asked for comments about answers on preceding page: selected comments are reproduced below:



- I am more willing to read about protecting myself from phishing if it's from an official, rather than news, source
- I chose "no" I did not change my behaviors because I generally think that anti-phishing strategies are common sense things that I was already following before I received formal information about it.
- I didn't change my behavior because I was already following the guidelines (e.g. never give out your private info).

- The only behavior that I have modified was the length of time between changing/updating bank/email/paypal/amazon passwords.
- It's just something you know, as a result of techy discussions etc
- I tend to pay more attention to information about phishing/scams from more "trustworthy" sources like the news and my bank. Half of the "scams" one is warned about on social media are urban myths or rare, so I don't think those warnings sink in as well as more serious warnings.
- I put "no" to 15 because I felt I was already using good online behavior to protect myself. Information i receive advising me on how to protect myself from phishing is never new information for me.
- I regularly receive emails to my hotmail account, purportedly from banks that I hold no accounts with, with a subject line stating that it's important information about my account. I wouldn't even click on an email that appeared to come from my own bank, so I wonder how people can be so daft as to fall for such scams.
To a certain extent, warnings about Internet scams and phishing are good, but ultimately you can't save people from their own stupidity.
- I feel cautious / aware enough that I don't need more info.
- I didn't change my online behaviour because I was already wary
- I think that a fake bank website used for phishing could also have misleading info about how to protect yourself. It seems like an ironic source to trust.
- most people do not read any financial documents that arrive at their home or via their online banking. if they hear it from their friend, they will listen.
- When I said NO reading it didn't change my online behaviour, that is because I was already aware and careful online.
- Been on the web since Compuserve - seen phishing since it was in short pants.
- Read it lots of places, they all say the same thing, it gets boring!
- I didn't actually change my behaviour because my husband has always warned me about potential phishing attempts and I've always been on the lookout for them - but I did understand better the various things to watch out for.
- Didn't change my behaviour as quite suspicious of emails like that anyway...
- letters from bank which are not fliers would be hav more weight than anything online
- I would most likely trust non computer based forms of information to protect myself from phishing mainly as you could trust whether they wer authentic or not. Online info could in theory be a phishing scam...
- I've always been suspicious of the Internet even though I use it regularly and never understand why people fall for the obvious phishing tactics. My partner is my main source of information
- I don't know what phishing is!
- I think there is a common misunderstanding of phishing as opposed to hacking.
- For question 15) I didn't change my behaviour because I was already doing everything the info suggested
- I can not remember the information I read about phishing and whether or not it was simple.
- Information needs to be widely avaiable, such as on dedicated websites so that it is easily found. Many people who could be the victims of phishing may not use f-book or twitter, e.g. the older age groups.

18) Do you think your bank should refund you if you lose money because of a phishing attack?				
			Response Percent	Response Total
1	yes		73.28%	255
2	no		26.72%	93
			answered	348
			skipped	6

Should banks refund losses?	% of answers adjusted	Men	Women	% of answers unadjusted
yes	71.95%	69.00%	74.90%	73.28%
no	28.05%	31.00%	25.10%	26.72%

Table 19 Whether banks should refund phishing losses

19) Do you take any precautions to protect yourself against phishing on your home computer? If you answer yes to this question, please outline the precautions below.				
			Response Percent	Response Total
1	yes		65.24%	229
2	no		34.76%	122
			answered	351
			skipped	3

Taking precautions	% of answers adjusted	Men	Women	% of answers unadjusted
yes	65.3%	65.69%	64.92%	65.24%
no	34.7%	34.31%	35.08%	34.76%

Table 20 Whether people take precautions against phishing

The following strategies were supplied. Charts show strategy, number of respondents using it and a typical comment about that strategy:

Use known websites

Only use trusted sites	19	I only make purchases thru websites I trust; my bank, amazon, clothing stores...essentially websites that start with https. – female, 26-35, medium high expertise
------------------------	----	---

Use security indicators

Look out for https indicator	18	Do not click on any suspicious links - make sure url has "https" – female, 26-35, medium low expertise
Check web addresses/URLs	14	If I receive an email from my bank or other website that has personal information, I never click on the links in the email. Instead, I go to their main page and navigate to the information from there. I double-check that I enter the right web address, and make sure that the https indicator is on websites that normally have it on. – female, 18-25, expert
Browser alerts	8	Anti-virus, uses chrome which alerts you when the website is fishy, pay attention to https website designation. – female, 26-35, medium high expertise
Check certificates	7	By generally being a suspicious b****rd. Keeping browser and operating system up to date, security-wise. Never entering any financial or sensitive information unless the page is https with a verified chain of trust for the security certificate. – male, 36-45, expert
Email software flags up/blocks phishing emails	5	Anti virus software flags potential fishing as does email software and browser. Also practice safe surfing – male, 56-65, medium high expertise

Caution with emails

Don't open or respond to / delete unsolicited mail	33	Don't open phishing emails, duh – female, 46-55, medium low expertise
Don't click on email or chat links	30	I never open email attachments from people I don't know or that look suspicious. I do not click links from friends in chat unless I know what they are. – female, 26-35, medium low expertise
Go direct/manually to bank/official sites	24	Anti-Phishing filter, vigilant that link goes where it says it is, typing bank urls directly, check site security certificates on first visit, fresh browser window. – male, 26-35, medium high expertise
Spam filters	18	I have a range of spam filters in place which catch a lot of phishing attempts; I never respond to emails that ask for personal or financial info; I never click links in emails or open attachments purporting to be from financial institutions; I always read the security info on the banking website; I never trust online communication purporting to come from a bank, Paypal or eBay without checking independently; I have keylogging protection when logging onto banking sites; I never do online banking on unsecured computers; I bank with a small outfit with a low profile and have never had an email purporting to be from them, whereas all the major banks get their share; (not sure if this one helps me, but I have a dedicated online credit card with a low limit that is not linked to my other accounts); and I exercise normal online precautions such as up to date AV, script blockers and malicious site checkers. – female, 46-55, medium high expertise
Contact company to check about suspicious emails	6	if something that I receive puts up a red flag, I will connect with the company directly to confirm legitimacy; this happened twice within the last 2wks from PayPal; when I connected directly with PayPal, they confirmed that it was a phishing attempt. – female, 26-35, expert
Don't trust email from bank	6	Spam filter etc - never open emails from banking organisations (my bank will never contact me by email) – female, 36-45, medium low expertise
Examine email headers/origin	5	Always check SSL certs, never click email links, check SMTP headers on emails and forward phishing to abuse addresses when appropriate. Run Linux, check firewalls, use OS integrity checker. – male, 18-25, medium high expertise
Hover over links	5	I check the header information of any suspicious emails (also, any "official" emails, i.e. from my bank, or from Facebook); if it's credit-card-related, I call the number on the back of my card or

		go directly to the bank/credit card website, rather than click on links in the email itself; I hover over any links in the email to see if they are redirecting me to suspicious websites – female, 26-35, medium low expertise
Don't open emails with spelling/grammar mistakes	3	Always check who the email is from, never respond to emails that contain odd language/grammar, never open attachments from unknown sources, never send personal details via email – female, 26-35, medium high expertise
Don't respond to requests for login details in email	3	Common sense! Always check the url, is correct and there a script at the end Dont open emails from unnown senders. Spelling and grammatical errors in official looking emails. Anything that asks me to verify my login details. – male, 35-45, medium high expertise
Use separate email address for banking	2	I use different email addresses for different activities, so if I get a phishing email at an address that I never use to contact that company, I know immediately that it's fake. If I'm asked to click on a link and enter my info, I instead directly type in the real site URL to make sure I don't get redirected. – female, 26-35, expert

The following strategies also got one mention each:

- Don't trust email from ebay/paypal;
- Only open email addressed to me by name;
- Read emails before clicking on links;
- Use a paid for email account.

Specialist anti-phishing software

Install bank provided software	10	use rapport (http://www.trusteer.com/product/trusteer-rapport) and hopefully up to date software (browser, AV etc) – male, 36-45, expert
Norton Phishing Protection	2	Use Norton protection systems which warn that sites aren't genuine/may be phishing. – female, 18-15, medium high expertise

Avoid infection

Anti-virus software	39	Never open e-mails from unknown or that look unusual Run virus software before and after any financial transactions online Have two different virus checking tools that are used – male, 46-55, medium low expertise
Security protection package	10	I dont know what phishing is, but I take precautions like safe Internet software. – female, 26-35, medium low expertise
Don't open attachments	9	I don't open suspicious emails/attachments/go to fake websites – female, 36-45, medium high expertise
Anti malware software	7	Have malware detection software installed. Never allowing the browser to save passwords. – female, 26-35, medium high expertise
Keep software updated	6	Don't open fishy emails, keep security software updated – female, 26-35, expert
No downloads	5	I don't download anything. I bank directly at the bank's website or in person. – female, 26-35, medium low expertise
Don't use Windows/do use Linux/Mac	5	Only using trusted sites Don't use Windows or Windows programmes – female, 36-45, medium high expertise
Anti spyware software	3	Make sure site is secure, anti-spyware installed on computer, not clicking on unfamiliar links, not using the same password for

		bank, paypal, facebook, etc – female, 18-25, medium high expertise
Software (unspecified)	3	Software – female, 46-55, medium high expertise

The following strategies also got one mention each:

- Don't allow other people's USB sticks on machine;
- Scan attachments.

Network security

Firewall	19	antivirus + firewall which asks me everytime a certain ip tries connecting in whatever way to my computer – male, 18-25, medium high expertise
----------	----	---

The following strategies also got one mention each:

- Password on router;
- Updated network security .

Password habits

Change passwords regularly	8	change passwords and have security software – female, 36-45, medium low expertise
Don't allow browser to save passwords	8	don't have passwords for banks saved, am generally careful about passwords – female, 18-25, medium high expertise
Strong passwords	3	Very strong password and make sure the URL is correct and secure during login. – female, 18-25, medium high expertise
Don't use same password for banking, ebay etc	3	1. Do not click links from spam emails 2. Do not give out sensitive information on unsecure websites 3. Different passwords for different sites 4. Log out of sites when finished – female, 26-35, medium high expertise

The following strategies also got one mention each:

- Use banking security questions

Control who gets their details

Don't or be very cautious give out email address/personal details	14	I don't share email on non trustworthy sites, and I delete things from people I don't know or from sites I didn't sign up for. – female, 18-25, medium low expertise
Never send personal details in email or over Internet	7	No sending of personal information on the Internet – female, 26-35, medium low expertise
Don't disclose personal details over phone	2	Check urls before clicking them. Also never respond to unsolicited e-mails or e-mails from unknown sources. Never give out security information or passwords either on the phone or by email – male, 46-55, medium high expertise

The following strategies also got one mention each:

- Hide personal information on Facebook etc
- Don't give out personal details unless site is 'virus safe'
- Don't allow retailer websites to store my details
- Only give personal details to Visa partners

General caution and judgment

Common sense	9	I use a very old Mac so have made the decision not to use antivirus. As for phishing, I don't think antivirus helps with that, you have to just not be fooled. – female, 46-55, medium high expertise
High security setting on browser	7	Don't save passwords, regularly clear histories, high levels security on browser, daily scans of computer, email filters, delete email if in doubt - female, 46-55, medium high expertise
Don't go to fake websites	6	dont bank on sites that are not legit – male, 18-25, medium high expertise
Stay informed	3	I have spyware, anti-virus, etc. I read cnet.com and follow advice b/c they have great advice and hundreds of reviews from users. I read e-mails from my bank and don't open suspicious e-mails. – female, 26-35, medium low expertise
Be careful	2	I'm not a twat – male, 36-45, expert

The following strategies also got one mention each:

- Don't answer scams
- Read security information on bank website
- General technical awareness
- Keep browser/operating system up to date
- Google for information
- Follow recommendations

Let someone else deal with it

Rely on bank guarantee/use credit card on web	3	The banks can policies that refund my money if I buy from a fraudulent company, isn't it essentially the same thing? – female, 26-35, medium high expertise
Delegate	2	don't know, i get someone to do it for me - female, 26-35, medium high expertise

Other/unclassifiable

Report phishing emails to bank	5	I report any junk mail I receive that appears to be a phishing scam. – female, 18-25, medium high expertise
Ad/popup blocker	4	By not clicking on links in emails and going directly to websites. Installing pop-up blockers, malware detectors and using security provided through browsers to check websites to see if they are genuine – male, 26-35, medium high expertise
Use different browsers	3	different passwords, using different web browsers, firewall and other security, not opening attachments/links from people I don't know/not expecting – female, 26-35, medium low expertise
Don't bank/shop online	3	Don't bank online The best protection package possible – female, 46-55, medium high expertise
Clear browser history	2	Don't save passwords, regularly clear histories, high levels security on browser, daily scans of computer, email filters,

		delete email if in doubt. – female, 46-55, medium high expertise
Log out of sites when finished	2	norton anti virus, logging off everything after use, only using credit card details online – female, 18-25, medium low expertise
Don't do online banking on unsecured computer	2	I have a range of spam filters in place which catch a lot of phishing attempts; I never respond to emails that ask for personal or financial info; I never click links in emails or open attachments purporting to be from financial institutions; I always read the security info on the banking website; I never trust online communication purporting to come from a bank, Paypal or eBay without checking independently; I have keylogging protection when logging onto banking sites; I never do online banking on unsecured computers; I bank with a small outfit with a low profile and have never had an email purporting to be from them, whereas all the major banks get their share; (not sure if this one helps me, but I have a dedicated online credit card with a low limit that is not linked to my other accounts); and I exercise normal online precautions such as up to date AV, script blockers and malicious site checkers. - female, 46-55, medium high expertise
Use prepaid card for online shopping	2	I always use a prepaid card to shop online – female, 18-25, medium high expertise

The following strategies also got one mention each:

- Don't use Adobe software
- Don't accept images in email
- Scan computer daily
- Only use Paypal online
- Don't allow silent redirect
- Use firefox
- Don't allow script plugins
- Use stealth mode
- Use keylogging protection for banking
- Bank with a small bank
- Dedicated online credit card
- Have several hard drives
- Check the sign-in page
- Practice safe surfing
- Use Linux live CD to log into bank sites
- Use operating system integrity checker
- Sandbox execution
- Don't do much online

20) Please describe what you consider when you decide whether to click on a link in an email.

The following strategies were supplied. Charts show strategy, number of respondents using it and a typical comment about that strategy:

Never click on links

I never click on links	9	I never do. Better safe than sorry. – male, 56-65, medium low expertise
Use bookmarked links only	2	I tend to only use the bookmarked links I have saved for my bank and credit cards. If i am suspicious, i look at the structure of the email (layout, graphics, wording, email account it was sent from) and compare it to previous emails I have received from the financial agency. – female, 26-35, expert
Copy and paste link	2	I do not click on links in emails. (If I really trust the source I may copy/paste the link - as you know the link URL and the link description do not necessarily correspond in a some spoof mails.) – male, 46-55, expert

The following strategy also received one mention:

- Check with the person sending before clicking

Email source

Known sender/source	119	If I know the sender, it doesn't cross my mind. I don't click the link if the sender is unknown. – female, under 18, medium low expertise
Who the sender is	64	I never click on an email link from any financial body. I only click if it's an online retailer I know, such as Amazon. If I were using a link to get to a web page and decided to buy something I would never continue from there, I would log in to the website directly. – female, 46-55, medium high expertise
Email expected/solicited (e.g. order acknowledgment)	47	I almost never click on a link in an email unless I am expecting links from someone. I also check to see if it's from somewhere that I recognize. I would be more apt to click on a link that comes from a website that I go on, than from one that I had never heard of before. – female, 18-25, expert
Trustworthiness of sender	36	Is this an expected email from a trusted source? Do I know where this is going to take me? Is it somewhere I want or expect to go. – male, over 65, expert
Email address of sender	23	Proper grammar: most phishing attempts I get are written in broken English. The sending email address is from the correct and matching site. The link goes where the text says it does, and it's the real site. The email format strongly resembles other official communication from that business. The email doesn't list hysterical reasons why my account is in question or about to be deleted (e.g. linked with funding terrorists). – female, 26-35, expert
Is it from a bank?	9	Who it's from. I never look at ones "from my bank". They have told me they will never email me asking for me to follow a link. – female, 26-35, medium high expertise
True email address of sender as shown in header	4	source server; content of mail; actual email header(something like source code); destination of link shown when mouse hover – male, 26-35, expert

The following strategies also received one mention each:

- If I have an account with sender, do not click
- Check source server
- Does this person email me a lot?
- Is it genuinely from the sender?
- Should the named company actually have my contact details?
- Am I a customer of theirs?

Email content

Nature/subject/intention of content	28	Whether I recognise the sender, whether the subject applies to me, what the intention is of the email - trying to sell me something, inform me of something, how well something is written, whether what I can see is accurate, what the email address looks like. – female, 18-25, medium low expertise
Grammar/spelling in email	24	is it from a trusted source or known person. How good is the English, ie are there spelling mistakes, bad grammar. Are they asking for very private information. Does the link in the email match the supposed sender website - a phishing bank email will not send you to the banks website. – female, 46-55, expert
Does it look/feel genuine/right?	23	Whether it looks legit. It's not difficult to tell if it's real or not. – female, 18-25, medium high expertise
Whether content has known sender's writing/content style	14	Known sender. Written in expected style of the sender. No wierd grammatical errors. Not from a bank. – male, 46-55, expert
Is it about something I'm interested in/relevant to me?	13	Whether my antivirus considers it is safe to do so, and whether I am interested in the link obviously – female, 18-25, medium high expertise
Nature of subject header	10	I'd submitted a contact form on the website of a company of scaffolders in order to complain about damage caused to a tree. When I received an email from a man whose name I didn't recognise, I assumed it must be a response to my complaint because the subject said "Damage to tree" so I assumed it would be safe. – female, 36-45, medium high expertise
Legitimacy of content	7	If it's from a trusted source If the email came to my inbox, rather than the 'junk' If the email content seems genuine – female, 18-25, medium high expertise
What information they are asking for about me?	6	As a rule if it is asking for me to confirm details i dont click – female, 18-25, medium high expertise
Are there other recipients?	5	Would this person send me something like this? How many other people are listed as recipients? Does it state contradictory information or instructions? Does the email say that I can only get to the linked page by clicking the link? – female, 18-25, medium low expertise
Does it contain a company logo/match format of company emails?	5	Who is it from, does it look legit (company logo etc) – female, 18-25, medium high expertise
Correctness of contact information/addressed by name	5	Entirely based on whether the email address is recognisable and is addressed to me in the normal way. For example, bank or PayPal ones always use your name in the email title, phishing ones are far more 'dear customer' generic. If in any doubt at all, I do not open the email – female, 26-35, medium low expertise
Does it look trustworthy?	4	Does the email look trustworthy? – female, 18-25, medium high expertise
Logic of content	4	I don't click a link unless the link makes sense to me within the context of the email. – female, 26-35, medium low expertise
Email format	3	The address of the e-mail The basic grammar of the text The format Whether it is a known/trusted company or not The nature of the e-mail - male, 18-25, medium high expertise
Is the content/subject general or specific?	3	I first check that I know the sender, then that I know why the person is sending the link. If the text is poorly written or lacks specificity, I ask before I click. For example, I do not click links that just say "check this out." – female, 26-35, medium low expertise
Is it safe?	3	Whether it is safe. – male, 36-45, medium high expertise

Is the content about financial information/account closure etc?	2	The sender, the URL I see when I hover over the link, whether it regards financial information. – female, 26-35, medium high expertise
Which of my email addresses was it sent to?	2	<ul style="list-style-type: none"> - Has the email arrived in my spam folder. - Which of my email addresses has been used. - What email address did it come from. - spelling errors - claims I can check before answering or clicking on any links (e.g. when emails claim that my account has been deactivated) - the general look of the email compared to other forms in which this organisation has contacted me before – female, 18-25, medium low expertise

The following strategies also received one mention each:

- Does it look professional?
- Does it contain foreign words?
- Can I double check the information in the email?
- Only open if there is a subject in header
- Only open if there is not a subject in header
- What is disclosed by looking at smtp header
- Does not look like spam
- Do I know what it is?
- How important is it?
- Is it worth the risk?
- Does it contain information only the sender could know?
- Is the link the only content?

Security filtering

Did it get through spam/phishing filter?	17	Whether I know who it's from or what it's regarding - I usually delete all emails that go in my spam or are from people I don't know. – female, 18-25, medium low expertise
If it has a virus/passes anti-virus	8	safety, viruses – female, 26-35, medium low expertise
Security (undefined)	3	security, is it trust worthy, why am i going there – female, 26-35, medium high expertise

Nature of link destination

Destination of the link	40	examine actual destination of link, if it looks suspicious, then I usually open it in a sandbox browser just to see what sort damage it would have caused – male, 26-35, expert
Hover over the link to see if address matches	15	If in any doubt I hover over it to see what the address really is. – female, 56-65, medium high expertise
Validity/legitimacy of link	11	who sent it, legitimate URL, https:// vs http://, tone, spelling, and grammar of email – female, 26-35, medium low expertise
Do I recognise the link address?	7	I usually won't, but if I do, I hover over the link (or right click) to look at its real address, and if it is an address I recognize, the chances are higher that I'll click on it. – female, 26-35, medium low expertise
Is link to https url/secure site?	5	who sent it, legitimate URL, https:// vs http://, tone, spelling, and grammar of email – female, 26-36, medium low expertise
Trustworthiness of link	4	If I feel I can trust the link. I only open emails that I think I can

		trust. – female, 36-45, medium low expertise
Can the linked site only be reached by clicking?	3	Would this person send me something like this? How many other people are listed as recipients? Does it state contradictory information or instructions? Does the email say that I can only get to the linked page by clicking the link? – female, 18-25, medium low expertise
Does the website at the end of the link look legitimate?	3	Language/typos etc Whether they are saying and asking for something that the institution is likely to ask for Is the website you're taken to legitimate If in doubt, I've called the company. – female, 46-55, medium high expertise
Weirdness of link	2	I have gmail so it's rearely an issue but weird links etc. – female, 26-35, expert
Safety of link	2	Check the hyperlink to see if it is safe. – female, 18-25, medium high expertise

The following strategies also received one mention each:

- Length of link
- Is the link masked or obfuscated?
- Only if it's a website I already use
- Format of the link address
- I only click if it's from a website where I don't need to log in

Other

Gut feeling	6	-Does it seem sketchy -Does it seem legit -Is my spider sense tingling – male, 26-35, medium low expertise
Check against list of known spammers/google message	5	Whether I have requested this information. Does it look right. google the company and address spaminform.com has lots of dodgy companies listed. – female, 46-55, medium high expertise
I don't bank online	2	I decide whether it is real or fake. I don't use online banking so if I get an email from a bank I know right way it is a fake, and I add it to my Block List. I never click an email if I don't know where it's came from, - female, 18-25, medium low expertise

The following strategies received one mention each:

- Where my details would go
- Will my details be used elsewhere?
- I click anyway and leave if it's weird
- Relevance to me
- I click in any case and then run malware scan
- Run a WHOIS check on the link destination
- Depends on mood

21) Please describe what you consider when you decide whether to enter your bank or payment card details into a website.

The following strategies were supplied. Charts show strategy, number of respondents using it and a typical comment about that strategy:

Reputation of the website

Only use good reputation/trustworthy/trusted site	149	is it a website i know and trust – female, 18-25, medium high expertise
Google for reviews of the website	17	How official it looks, I google suspicious companies to check out if they have any bad reviews before buying online – female, 18-25, medium high expertise
Check to see if the website has known security issues	11	Check to see if the website has known security issues. – female, 18-25, medium low expertise
Reputation of their payment processor	5	The payment broker they are using, and their reputation as a company. – female, 26-35, very low expertise
Site must belong to retailer with bricks and mortar presence	2	Company must have brand recognition outside of the Internet, and if I'm unfamiliar with the site I either ask a trustworthy person's opinion or check the guarantee/endorsements for safe shopping. – female, 18-25, medium low expertise
Run a WHOIS check on the site	2	I check the security certificates, Google for others' experience with the site, check for evidence of scams relating to the site, and run a WHOIS check in order to determine who is responsible for it, how long it's been registered for and how long the registration is set to run for, and so on. – female, 26-35, medium high expertise
Do I know the brand?	2	Recognised brand? – female, 26-35, medium low expertise

The following strategies also received one mention each:

- Is it approved by google?
- Has a reputation for being safe

Personal experience

Previous positive experience with the website – own/friends	37	Security is very important, would have to be a site that I have used before and trust. – female, 26-35, medium low expertise
---	----	---

Is website/connection secure?

Check if there is https	68	secure site (https) – female, 46-55, medium high expertise
If website is secure (but no explanation of what secure means)	42	If it states it is a secure website. – female, 36-45, medium high expertise
Look for security indicator logos	32	I check to see that there is the little closed padlock on the screen. Is it a site I trust? Is it a reputable company. – female, 46-55, medium high expertise
Does the site have a security certificate?	11	security certificate and reputation of the website – female, 18-25, medium low expertise
Is secure checkout available?	8	Use of a secure method of payment processing, will check if it's unfamiliar to me. Check if website has been flagged as a phishing website. – female, 36-45, medium high expertise
Is the security certificate up to date and valid?	5	HTTPS secure site, with valid Certificate. Know the company before hand, google site name if any doubts. Prefer to use paypal when option available. – male, 36-45, medium high expertise
Am I forwarded to a 3D Secure page?	5	Good question... Do I know the company - have I dealt with them before (especially face-to-face) - is the website "secure" (HTTPS) - sometimes I back out of a transaction if it doesn't "feel right" e.g. if they seem to ask for the bare minimum of card details, or

		don't forward me to the bank's verification site (e.g. Verified by Visa). – male, 46-55, medium high expertise
What sort of encryption it uses?	3	If it's "secure", what kind of encryption it uses, and if the info won't be stored on their servers – female, 36-45, medium high expertise
Is it externally verified?	3	Usually I only put my card details onto sites that i trust and that are verified by external sources. – male, 18-25, medium high expertise
Is it password protected?	2	I am always quite worried when I do that and I do it only when buying things online. I am happy when I see a message which states I need to give a security code to verify the transaction as it means to me it is a secure connection – female, 36-45, medium low expertise
Is the network secure?	2	is it a legitimate website how secure is their network – female, 18-25, very low expertise
Do I trust the connection?	2	is it really necessary, ie am i buying something? do i trust the website? and do i trust my Internet connection? – female, 26-35, medium low expertise

The following strategies also received one mention each:

- Is my security image showing?
- Does the site have a secure server?
- Is my security up to date?
- Who the certificate authority is
- The credentials on the website

Look and feel

Legitimate looking site	24	Who owns the website, how legit it looks, how I got there – female, 18-25, expert
Legitimate looking /correct url	15	If the website is an https site, if it is a known website, if the url looks normal/logical – female, 26-35, medium high expertise
Does it make sense/is it necessary that this information is requested?	6	Does this site look legitimate, does it have an address that begins with (https), does it make sense that they want my personal information? – other/prefer not to answer, 18-25, medium low expertise
Url resolves properly	4	HTTPS address, URL resolves properly and is recognisable as the one I'm expecting! – female, 36-35, medium high expertise
Does it look professional?	4	if the site is certified secure, if the sit generally looks professional and legitimate – female, 18-25, medium high expertise
Has the look of the site changed from previous visit?	3	Whether it looks different from previously and if the security image and keyword I choose appears there. – male, 46-55, expert
Is the website safe?	5	Is this a 'safe' website. Have I used this site before. – female, 18-25, very low expertise
Gut feel/trust	2	I pay with credit card only when necessary, does the website look trustworthy (I realize that's not the best indicator), do I know the website is generally trusted, do they have the security certificate logos (also not the best indicator) – female, 18-25, medium high expertise
Page layout	2	url of the website, layout, where do the links lead to (exact url)? – didn't disclose, 18-25, expert

The following strategies also received one mention each:

- Size of the webpages

- Only use websites that don't use Java, Flash or plugins
- Does it look like the site I meant to visit?
- Are all the page elements suitable?
- How serious is the website?
- Compare site with site found by googling
- Does the site state that it is secure?

Rely on browser or anti virus warnings

What does browser say?	4	Whether my browser says site is secure, whether it is a site I trust, whether I chose to go the site or I got there via a non-straightforward means. – female, 36-45, medium low expertise
Look at anti-virus software toolbar	3	I will only enter any bank details into shopping sites which the anti virus believes is safe and has secure banking. The only other time i enter details is on the bank providers website – female, 18-25, medium high expertise

Control risk

Use Paypal or Google checkout	33	how professional a website looks and where there is a paypal symbol or some other kind of validate security symbol. – female, 18-25, medium low expertise
Don't enter bank detail into any site	6	Does the website belong to a know reputable company Did I go directly to the site or get transferred there from a link If I am not fully confident I use PayPal I never enter by bank data in ANY site – male, 56-65, medium high expertise
Only use credit card	6	I ensure that the site is using SSL. If possible I am looking for the green extended validation indication. I do not enter bank account details on line in preference using a credit card. I also try and check the site out a bit. Is this a brand I know and does the web site I am on match up with the site that I get to by searching for the company etc. – male, 36-45, expert
Don't or rarely shop online	6	I dont enter details – female, 18-25, medium low expertise
Only use prepaid cards	3	I don't. I use either PayPal or prepaid cards. – male, 26-35, expert
Don't use debit cards	2	Is the webpage secure (https)? Use browser "private browsing" mode. Reluctant to use debit cards online (only for national lottery website). Use paypal where possible to avoid giving credit card details for one-off purchases (or for some regular ones). – male, 46-55, medium high expertise
Use credit card temporary number function	2	I look for https in the URL and also make sure the domain of the url is what I expect. I frequently take advantage of my credit card's temporary number feature, where I can create a new, temporary credit card number with a low maximum to protect myself against online fraud. – female, 26-35, medium low expertise
Use special online only credit card	2	Have special credit card for online. Only used for that. Check seller carefully – male, 46-55, medium high expertise

The following strategies received one mention each:

- Only give out information when setting up account
- Only give out information on transactions I initiated
- Don't give out information in return for free gifts/trials
- Doublecheck that links to Paypal etc are genuine

- Only use bank's secure bill pay service
- I only ever use an account with a low balance

Other/ambiguous

How did I get to the site? Where link originated?	19	Who owns the website, how legit it looks, how I got there – female, 18-25, expert
Look for customer service helpline number/contact details on site	7	Is the connection secured? Does the site publish phone and address detail for the site owner? – male, 46-55, expert
Only when I'm buying something	4	How did I get here? (Directly entered URL, saved bookmark or link from a respectable web store are Ok, nothing else is.) Is this information logically required? (I.e. am I buying something from them, or doing some other financial transaction). Is this a https page with a trusted security certificate? Does the URL match the company I think I'm doing business with? – male, 36-45, expert
Look for guarantee information/security policies, terms and conditions on website	4	I do not use online banking. However, if I am buying something online I only use websites I trust, or that have been recommended to me by others. I always check that there is a guarantee and a good returns/ cancellation policy etc. – female, 18-25, medium low expertise
Reliability of site	4	lock desing on the browser and reliability of the website – female, 26-35, medium low expertise
Make sure the site is genuine	4	make sure it is genuine, don't buy from unsolicited email links. Use a top-up credit card with small credit limit just for online purchases. – male, 46-55, medium high expertise
How much do I want to buy the item?	3	Do I really want to buy what they're selling? – male, 56-65, medium high expertise
Only if they don't store my details?	3	If it's "secure", what kind of encryption it uses, and if the info won't be stored on their servers. – female, 36-45, medium high expertise
I only enter details on the bank website	3	Only enter info into known vendors/bank websites – female, 26-35, medium low expertise
Did I initiate the transaction?	2	did i initiate transaction? is website secure? use only credit card # not banking info no personal info given unless i am setting up bank or credit card acct – female, 46-55, medium low expertise
Whose computer am I using?	2	I only do this on well known, well established sites - and on my own computer (not a public one) – female, 18-25, medium low expertise
Type of site	2	type of web – female, 18-25, medium low expertise
Goes ahead and make purchases anyhow/don't think about it	2	If I get to that point, I've already decided that I wish to go ahead with the transaction. If it's fraudulent, then it's my own fault. – male, 46-55, expert

The following strategies also got one mention each:

- Rely on bank flagging up fraud
- Site must have address and phone number in my country
- Address must be verifiable
- Will my details be stored securely?
- I only use secure routers
- Security messages
- Site location
- Security of the brand
- Am I making a payment?

- Personal convenience
- Site information
- Amount of time website has existed
- Am I willing to take the risk?
- Is it the right site?
- Does not trust Paypal
- Am I using private browsing mode?
- Who owns the website
- Website name
- Is the site protected?
- Why am I purchasing from the site?
- Will I be defrauded?
- Is it valid?
- Do I know how much I am being charged?
- How often do I use it?

Question 22 was an open question asking for comments on previous questions on the page. Selected comments are reproduced below:

- sketchy sites: avoid them.
- i never click on an unsolicited email asking for personal info
- Never received a phishing email, as far as I know.
- If I come across a link or an email that is in any way suspicious, but I'm still interested, I open up a new browser tab and type in the URL manually to see if I can still access the same information
- In regards to question 20 even if an email seems to be from a trusted brand if they have no reason to know of my email address I would just delete it.
- Most phishing attempts are very transparent if you know what to look for. I've only received ~3 ever that I thought might fool an experienced user.
- On 18, I do think the bank should return the money in some cases if they were at fault, e.g., they had poor security practices that led to the breach.
- You haven't asked questions about where people are accessing the Internet from. For example, I feel safer entering my bank details in a website when I'm using my laptop at home, but I think twice about using WiFi in public places, or using Internet cafes. Sometimes I haven't really had a choice and have needed to book flights or trains using Internet cafe computers and the idea of key logging or phishing software being installed on third party computers concerns me.
If I had unavoidably used an insecure computer or connection to make such a transaction, I'd monitor my bank balance and frequently check bank statements online from secure computers for a while afterwards, so that I'd hopefully spot anything untoward quite quickly.
I haven't yet carried out any financial transactions over the Internet with my mobile, but I'm concerned about security should the need arise for me to do so. I would only do so if it were unavoidable.
- Clearmymail.com has a good website on how to spot fake emails and websites
- If the phishers ever learn to use proper English, I'd feel in a lot more danger.
- Rider on question 18 - I wouldn't expect the bank to refund if I've blatantly broken all the rules of avoiding being phished; it's a different matter, though, if their system has been hacked to email customers and therefore looking legitimate.
- about question 18, I answered yes, but that would apply in case the bank had not informed me about phishing or if the site had security breaks.
- I do think, unlike other cyber crime, that victims of phishing specifically could have been more careful.

- i'm very worried about my parents (who are in their 80's) falling prey to phishing scheme, but in all the years i've been online, i've only received 1 email i think was a phishing attempt.
- I've been buying 'stuff' online for nearly 20 years. In the early days, card details were sent in email (clear text). Generally, protection has improved, but I think that users have become paranoid about online crime.
- (18) yes for me because I make the effort to thwart phishing attacks.
(18) yes otherwise the banks would be even less secure than they are now.
(18) no for people how have not made an effort to understand phishing attacks.
The banks need to make basic security measures effective eg:
Check the link target in the status bar. If javascript is enabled this is pointless.
- Do not use Microsoft Windows.
If online then never with root access.
Software installation only from secure sources.
- The only ever phishing attempts I have seen have been miserably bad.
- Become second nature to not throw away all fishy stuff
- To Q.18 - I don't think they should necessarily refund you if the phishing incident was a fairly obvious one, whatever obvious is as I'm quite suspicious - Nigerian money transfer emails, that sort of thing. I would want my money back if it was something that the bank had allowed/facilitated through their own practices or systems.
- Unless you are about to enter them in the next few pages then my behavior is different when I am using a fully fledged PC and a smartphone or tablet. On a PC it is often easier to do more background research and you do not typically have the pressures of being on the go that you have with a smartphone. I know from recent personal experience that I was much more likely to be duped by a phishing attack on my smartphone than on my PC, to the point I nearly fell for one.
- Banks should offer a free second credit/debit card on accounts that can only be used to pay a preset amount, like a prepaid debit card but tied to your normal chequing/current account and Billing Address for easy admin and NO FEES. This would cut down on their losses from fraud and give customers peace of mind when shopping that the potential loss is limited to what they preloaded onto the second card
- Phishing relies on people being incautious or even just plain stupid. Just in the same way you wouldn't leave your door unlocked when you go away on holiday, you don't give thieves the opportunity to rob you online. You should always be vigilant.
- My credit card accounts are protected from fraudulent use as long as I have acted in good faith.
- I pay for protection on all of my cards for fraud.
- Usually you can tell if it is a phishing scan due to the poor english or the formatting - usually from a bank that you dont use telling you that your access has been suspended. I think that should the bank/building society/hmrc want to get in contact they would phone/contact ou in writing rather than an informal email... Maybe i'm just old fashioned though?
- Not sure about banks paying out - I suppose they could be liable in some cases, if their security was lax - letting someone get details from them
- I received a full refund from my then credit card company. They noticed the strange transactions before me!
- SOMETIMES I HAVE ENTERED CARD DETAILS TO PAY WHEN THE PADLOCK SIGN HAS NOT BEEN THERE, BUT IT HAS BEEN IF A COMPANY I KNOW SUCH AS ASDA. I STILL DON'T FEEL 100% SAFE DOING IT THOUGH. AND I AM A LITTLE DUBIOUS WHEN THE VERIFIED BY VISA BOX DOES NOT COME UP YET THE PAYMENT GOES THROUGH.
- for question 18 I think it depends on the situation but generally if the banks security settings have not helped in preventing fraud then they should be required to refund the money since we are trusting them to hold it for us and in a lot of cases pay monthly for them to do so.
- Phishing is not the fault of the bank so they should not be responsible for compensation.

- Regarding question 18: The bank should only refund, if it's out of my control and it wasn't my fault. If I entered my data on a phishing site then it's my own fault and I should not get a refund.
- I don't generally shop from websites that aren't well known i.e. I shop from amazon.co.uk because it's well known and I trust it
- Sent several phishing emails onwards to the supposed originator, the banks didn't reply, paypal thanked me every time.

14 A6 - Evaluation framework

Research question	Selected references	Expected findings based on literature	Actual findings – expert interviews	Actual findings - survey
Why do users fall for phishing?	Sun, Wen, and Liang, 2010 Anandpara, Dingman, Jakobsson, Liu, and Roinestad, 2007 Kumaraguru, Sheng, Acquisti, Cranor, and Hong, 2007 Furnell, 2007 ed: Roessler and Saldhana, 2010 Egelman, Cranor, and Hong, 2008 Downs, Holbrook, and Crainor, 2006 Downs, Holbrook, and Crainor, 2007 Dhamija, Tygar, and Hearst, 2006 Schechter, Rachna, Ozment, and Fischer, 2007 Egelman, Cranor, and Hong, 2008 Wu, Miller, and Garfinkel, 2006 Jagatic, Johnson, Jakobsson and	Lack of awareness and understanding of phishing	Suggestion that there is ignorance but reluctance to be too damning.	General confusion about how phishing differs from other security threats.
		Complacency about existing knowledge and protection	Suggestion that users may feel more protected than they are, due to lack of understanding.	Users feel protected but use poor strategies.
		Carelessness and lack of interest in security and risk	Expert interviewees tended to back up this view.	Users mainly appear interested and responsible but lack the knowledge to protect themselves.
		Ignorance of security procedures	Some users are ignorant but many are misled by inadequate advice or security measures.	Many users are confused as to what specifically to do to counter phishing and use inappropriate measures.
		Focus on primary task rather than security	Experts agree with this assessment.	Users think about security but also allow tools to take decisions for them so it can become secondary.
		Ritual nature of task activity	Not explicitly discussed by	Not borne out by answers.

	Menczer, 2007		follows from above.	
		Social context matters	Users tend to believe what they are told but at the same time the Internet makes questions of trust difficult.	Users strongly bore out the findings of the research, depending heavily on who sent emails as to whether they trusted them.
Do personality factors have any effect on how people deal with phishing?	Pattinson, Jerram, Parsons, McCormac and Butavicius 2012 Kumaraguru, Rhee, Sheng, Hasan, Acquisti, Cranor and Hong, 2007 Downs, Holbrook, and Crainor, 2006	Personality traits make a difference (extraversion)	Not addressed	Not addressed
		Degree of impulsiveness – no consensus on significance	Seen as potentially interesting area for investigation.	Some differences with general population registered especially regarding reading of bank messages.
		Concern about what sender of email thinks of recipient	More deferential personalities might fall victim more easily.	Not borne out by survey.
Relationship between online behaviour and offline behaviour	Baym, 1998 Zhao, 2006	Online identity behaviour reflects and is anchored in offline behaviour	Interviews reflected opposing view that there are differences between online and offline behaviour.	Survey showed that people do take online responsibilities fairly seriously and are more concerned about online than offline crime.
User reaction to anti-phishing methods	Sample, 2012 Downs, Holbrook, and Crainor, 2006 Downs, Holbrook, and Crainor, 2007 Pattinson, Jerram, Parsons, McCormac and	Confused by warnings, indicators and education	Confirmed. See comments about ignorance and lack of understanding.	Confirmed. See comments about ignorance and lack of understanding.
		Focus on site content, graphics rather than security indicators	Strong agreement from the interviews, as well as gut feeling.	Mixed picture – general agreement but many people also look out for https.

	Butavicius 2012 Kumaraguru, et al., 2009 Kumaraguru, et al., 2007 Wu, Miller, and Garfinkel, 2006 ed: Roessler and Saldhana, 2010	Education too complex	Either it is too complex or users are unaware of it.	Users are aware and say it is not too complex but they do not appear to learn from it.
		Security indicators are not effective/are ignored	Interviewees preferred to focus on non-user controlled technology	Some users are dependent on these but it is difficult to tell how effective they are.
		Banks/website owners cause confusion by not following own guidelines or by having poor security practices	Confirmed by interviewees.	Too complex a point for most survey participants but one did raise it.
Means of improving anti-phishing methods	Wu, Miller, and Garfinkel, 2006 Egelman, Cranor, and Hong, 2008 ed: Roessler and Saldhana, 2010 Dhamija and Dusseault, 2008 Schechter, Rachna, Ozment, and Fischer, 2007 Mannan and van Oorschot, 2010 Kumaraguru, et al., 2009 Kumaraguru, et al., 2007 Parsons, McCormac, Butavicius, and Ferguson, 2010	Embedded education	One bank links customers through to APWG material.	Not mentioned.
		Making education relevant to the real world/more personalised	Relevance considered important, personalisation may be more difficult.	Official information is preferred, information from friends and family is more likely to be acted on.
		Use of positive reinforcement Use of negative reinforcement	Negative reinforcement the only way	People with previous bad experience are more worried.
		Use of active warnings that cannot be ignored	Not really discussed and people may just click through them even if a reaction is required.	Not really discussed.
		Consistent interfaces	Not really discussed.	Not really discussed.
		Important role of mobile authentication	Agreement that there is a role for this but caution about additional risks.	Very little user input.
		Helpfulness or	Not discussed.	One user

		otherwise of site authentication images		mentioned these as a security indicator.
Responsibility for protecting user against phishing	Downs, Holbrook, and Crainor, 2007	Users don't believe they have responsibility for protecting themselves and do not care about risk	Sharing is ideal but taking responsibility at least in part is business decision for bank.	Shared responsibility, in that users protect themselves but expect bank refunds.