Personality Caught in the Social Net:
Facebook Phishing

Kelly L. Price

N00104556

Institute of Art, Design and Technology, Dún Laoghaire

Dissertation submitted as a requirement for the degree of MSc in Cyberpsychology, Institute of Art, Design and Technology, Dún Laoghaire 2012.

Declaration

This dissertation is entirely of my own work, and has not been previously submitted to this or any other third level institution.

_____ _____

Kelly L. Price Date

Acknowledgements

This dissertation is dedicated to Tadhg, Conor, Shane and Felim, the four wonderful men in my life who not only gave me the time and space to complete this work, but also encouraged me to do my best. Thank you for believing in me.

This research would not have been possible without the guidance and sagacious advice from my dearest sister, Kimber. I am indebted to her for her patience, kindheartedness and scholastic wisdom. She is a true inspiration to all who have laboured in the fields of learning.

I wish to thank my mother, Linda, who paved the way for me to believe that everything is accomplishable. Thank you for showing me that learning never stops.

I would like to show gratitude to my teachers and supervisors at IADT, in particular Dr. Grainne Kirwan, Hannah Barton and Dr. Marion Palmer. I am also grateful to my supportive colleagues who helped make the last two years *fun*.

Agus ar deireadh thiar, a Mhná na hÉireann, ba mhaith liom mo bhuíochas ó chroí a ghabháil libhse as an spéis, an spreagadh, an cairdeas agus as an gcion a thug sibh dom. A dheirfiúracha Éireannacha, chuir sibh fáilte romham isteach in bhur mbaile féin; i ngeall air sin ní scarfar ó chéile sinn go deo.

(Lastly, to the women of Ireland, I owe my deepest appreciation for the interest, encouragement, friendship and love you give to me. My Irish sisters, you have accepted me into your home; for that, we are forever tied.)

Table of Contents

Abstract 1

Introduction 2

Terms and Definitions 5

Facebook Phishing 6

Trust Indicators 6

Social Engineering Practices and Persuasion 9

Post-Phishing Analysis 10

Understanding the Psychology of Phishing Success 11

Victimisation: Financial and Psychological Effects 12

Personality Factors 14

Impulsivity 16

Trust 18

Demographic Factors 19

Research Aim 19

Method 21

Participants 21

Materials 21

Procedure 26

Ethics 26

Results 28

Personality 29

Impulsivity 32

Trust in Facebook 34

Trust Factors 35

Authenticity Ranking 36

Other Findings 37
Discussion 38
Personality 38
Impulsivity 39
Trust in Facebook 40
Trust Factors 41
Authenticity Ranking 42
Other Findings 42
Limitations 43
Implications 44
Future Research 45
Conclusion 46
References 47

List of Appendices

Appendix A Descriptives 54

Appendix B Big Five Inventory Scale 44 56

Appendix C Barratt Impulsiveness Scale (BIS-11) 58

Appendix D Individual Trust in Online Firms Scale 59

Appendix E Stimuli Authenticity 60

Appendix F Rating and Stimuli Identification Sheet 65

Appendix G Consent Form 69

Appendix H Screenshot Section Oral Instructions 70

Appendix I Debrief 71

Appendix J Nonparametric Correlations Personality and Ratings 72

Appendix K Nonparametric Correlations Personality and Stimuli Count 73

Appendix L Nonparametric Correlations Impulsivity and Ratings 74

Appendix M Nonparametric Correlations Impulsivity and Stimuli Count 75

Appendix N Nonparametric Correlations Trust in Facebook, Ratings and Stimuli Count 76

List of Tables

Table 1 Personality Domains, Facets and Scoring Adjectives 14
Table 2 Barratt Impulsiveness Scale - Factor Structure and Description 17
Table 3 Descriptive Statistics..... 28
Table 4 Nonparametric Correlations Personality and Ratings..... 72
Table 5 Nonparametric Correlations Personality and Stimuli Count 73
Table 6 Nonparametric Correlations Impulsivity and Ratings 74
Table 7 Nonparametric Correlations Impulsivity and Stimuli Count..... 75
Table 8 Nonparametric Correlations Trust in Facebook, Ratings and Stimuli Count 76

List of Figures

Figure 1. Facebook phishing email 7
Figure 2. Facebook phishing login page 9
Figure 3. Missing elements from phishing example 9
Figure 4. Genuine Facebook email 23
Figure 5. Phishing Facebook email with phish elements 24
Figure 6. Genuine Facebook web login page 24
Figure 7. Phishing Facebook login page with phish elements 25
Figure 8. Gender and age distribution 29
Figure 9. Total count rating for email (phish) screenshot 29
Figure 10. Total count rating for website (phish) screenshot 30
Figure 11. Conscientiousness and correctly rated phish count 31
Figure 12. Conscientiousness and incorrectly rated phish count 31
Figure 13. Conscientiousness identified stimuli count 32
Figure 14. Impulsivity and correctly rated phish count 32
Figure 15. Impulsivity and incorrectly rated phish count 33
Figure 16. Cognitive instability correlations 33
Figure 17. Trust in Facebook and correctly rated phish count 34
Figure 18. Trust in Facebook and incorrectly rated phish count 34
Figure 19. Trust in Facebook stimuli and age groups 35
Figure 20. Phishing trust factor identification rate 36
Figure 21. Screenshot ratings 37

Abstract

Phishing is a well-documented social phenomenon whereby an individual poses as a trustworthy source to lure an unsuspecting user to give up sensitive, personal details willingly; this data is deceitfully utilised in identity theft, cash transfer and fraudulent credit card transactions. This study focuses on the correlation of phishing and Facebook users' personality traits. Participants were asked to complete questionnaires measuring conscientiousness, impulsivity and trust in online firms; additionally they were asked to rate the legitimacy of Facebook email and web login page stimuli where some samples were genuine and others were phish. The findings indicate individuals who score highly in cognitive instability, a subscale of impulsivity, log in more frequently and identify fewer phishing stimuli than those who score lowly in cognitive instability; not all users identify all trust factors (present or missing) in Facebook emails and web sites; and individuals mistake authentic Facebook emails and web pages as phish.

Keywords: phishing, fraud, identity theft, social engineering, personality, conscientiousness, impulsivity, trust in online firms, victimistion, trust indicators, Facebook

Introduction

Phishing is a well–documented social phenomenon (Anandpara, Dingman, Jakobsson, Liu, & Roinestad, 2007) whereby an individual poses as a trustworthy source to lure an unsuspecting user to willingly give up sensitive, personal details (Soghoian & Jakobsson, 2009). This research focuses on Facebook phishing, personality, impulsivity and trust in Facebook as an online firm. Background information provides a foundation to phishing, phishers and associated damages; descriptions, terms and definitions establish an understanding of phishing and its implications; and research review reveals trust indicator studies, social engineering practices and post-phishing analysis data. Additionally, personality factors, impulsivity, trust in online firms and demographic findings provide psychological links with technological elements. Based on these findings and corresponding rationale, five hypotheses provide a basis for an experimental study.

Data harvested from phishing is deceitfully utilised to achieve identity theft, cash transfer and fraudulent credit card transactions (Feigelson & Calman, 2010; Jakobsson, Tsow, Shah, Blevis, & Lim, 2007; Jewkes & Yar, 2010). Phishing is a sophisticated social engineering technique that reaches global audiences, from postal letters, faxes and telephone soliciting (Holt & Graves, 2007; US Federal Trade Commission, 2011) to emails, Instant Messaging (Amin, Okhiria, Lu, & An, 2010; Nykodym, Kahle-Piasecki, Ariss, & Toussaint, 2010) links and compromised, or illegitimate, webpages (Anti-Phishing Work Group, 2011; Symantec, 2012a). Social engineering exploits human, rather than technological, weaknesses (Parrish, Bailey, & Courtney, 2009). The key to social engineering is to use deceitful techniques to convince a target to supply the required information in order to obtain access to a security system (Simon & Mitnick, 2002).

Phishers utilise these social engineering techniques and technical strategies to persuade potential victims to provide the details required to carry out these fraudulent actions (Nykodym et al., 2010). For example, an email may account a fabricated story of misfortune, requiring immediate help; entering dialog with the phisher establishes the potential to ‘hook’ the individual to engage in financial transactions. This is also known as a Nigerian 4-1-9 Letter Scam or Advance Fee Fraud. A phisher may also provide an email link which, when clicked, leads to a decoy webpage

designed to entice a user to bequeath account and password information (Jewkes & Yar, 2010).

Additionally a phisher may conceal hateful software in an email, email attachment, web link or web page intended to cause computer damage or, more sinisterly, record key combinations (known as keylogging) input onto particular websites, such as online banking pages, and return the codes covertly back to the phisher (Kirwan & Power, 2011).

Phishing poses a grave threat to international security and economy (Bergholz et al., 2010); estimates indicate $50 billion was lost to phishing in the USA in 2008 (Wright & Marett, 2010). It is also acknowledged that the figure is probably much higher but much of it goes unreported due to individuals being too embarrassed to admit they were victims of the scams (Bergholz et al., 2010; Holt & Graves, 2007; Purvis, 2011). Phishing is a lucrative business, where, on average, a phisher receives $4,500 for each attack (EMC Corporation, 2012). In the USA, over 750,000 fraud related complaints were filed and over 250,000 cases of identity fraud were reported in 2010; statistics indicate that nearly 200,000 fraud related reports were instigated by email, compared to nearly 54,000 by ordinary post (US Federal Trade Commission, 2011). Reports of financial loss to fraud victims amounts to over $1.7 billion annually (US Federal Trade Commission, 2011).

Phishing scams in the first half of 2011 were dominated by the financial sector at 47% (for example, banking, e-commerce and retailers) and the payment services (such as Paypal) sector at 26% (Anti-Phishing Work Group, 2011). Although social networking phishing represents only 4.2% of the overall phishing sectors (Anti-Phishing Work Group, 2011), it is significant in its relation to automated toolkits. Automated toolkits enable fraudsters to create websites and hosting for phishing attacks (EMC Corporation, 2012); attacks used with these toolkits increased by 316% in the month of November, 2011(Symantec, 2012b). In particular, an attack during this month on a popular social networking site was toolkit-based and represented a majority of all toolkit-based attacks globally (Symantec, 2012b). In addition to phishing tool-kits, another opportunity phishers have for gaining access to social networking sites is to exploit the openness of Application Programming Interfaces (APIs). Felt and Evans (2008) iterate the gravity of API openness and the lack of

privacy preserving that leaves individuals open to data harvesting. The API gateway can provide a direct path to a user's personal profile, and typically to the friends (and friends of friends) of the user as well. Without adequate privacy controls, misuse of this data may provide an avenue for malware distribution via posts, comments, links and tags (Geier, 2011; Symantec, 2012b); additionally, clicking on a malicious link may show that the user 'likes' it, thus sending it further into the network for additional data mining (Symantec, 2012). Lastly, fraudulent data mining often results in data being sold on the black market to other phishers or for targeting specific individuals or groups in order to penetrate and access as much detail from that group as possible (Anti-Phishing Work Group, 2011; Bergholz et al., 2010; Downs, Holbrook, & Cranor, 2006). This type of individual or group targeting is known as spear phishing (Kirwan & Power, 2011).

Phishing scams are short lived, usually doing the most damage in twenty four hours and vanishing after a few days (Jagatic, Johnson, Jakobsson, & Menczer, 2007). Risk and effort are low for phishers and, due to the anonymity of the web and global geographical distribution, capturing and prosecuting criminals is rare (Wright & Marett, 2010).

Phishing has similarities with its homophonic partner, fishing, in that a "bait" is cast into a wide arena (mass emails), and a "hook" (leading the user to an illegitimate website, for example) takes place for a "catch" where possible data submission may take place (Wright & Marett, 2010). Internet phishing became evident in circa 1996 when phishers gained access to AOL accounts by tricking users for their passwords (Anti-Phishing Work Group, 2012). Other successful phishing attempts have also involved the US Internal Revenue Service (IRS, 2012), Citigroup (Reuters, 2011), and more recently, social networking sites such as Twitter and Facebook (Feigelson & Calman, 2010; Nykodym et al., 2010).

Reports indicate that social media phishing is on the rise, up 80% from October to November 2010 (Symantec, 2010). Although there is much discussion of social media phishing in internet magazines, forums and intelligence reports (Krebs, 2009; Symantec, 2012a) most is about the scams themselves or the technicalities of *how* the scams are executed (Bergholz et al., 2010; Petre, 2010). Some literature has been completed about *why* some people fall prey to online attacks, such as inherent

phishing properties unawareness (language, layout and structure) (Chandrasekaran, Narayanan, & Upadhyaya, 2006; Vishwanath, Herath, Chen, Wang, & Rao, 2011; Workman, 2008) however, even less exists to date about *who* is the most susceptible to internet phishing (Purvis, 2011). There may be aspects of personality that may lead an individual to be more susceptible to phishing, as identified in a framework by Parrish et al. (2009). Parrish et al. provided an investigative model for future research that recommended four phishing and personality relationship considerations: personal, experiential, personality profile and phishing susceptibility. This study focuses on identifying *who* are most vulnerable to Facebook phishing by examining personal (age and gender), personality, experiential (Facebook login frequency and duration) with email notifications and web login pages attack factors. Relationship consideration is also given to dimensions of impulsivity and trust in Facebook as an online firm.

Terms and Definitions

To understand the terminology related to internet fraud, it must be clarified that *spam* is an unsolicited email which is a nuisance to users and can create network stability problems for Internet Service Providers (ISPs) and *phishing* is a subset of spam that is intended to extract personal information with intent to deceive (Bergholz et al., 2010). When a sender uses a false name or identifier, the user is a *spoofer*; an impersonated spam or phishing email, or even an illegitimate website, is known as a *spoof* (Wright & Marett, 2010). An example of the simplest form of phishing is an email requesting a user to reply with details such as name address, bank account number, credit card number and so on (Bergholz et al., 2010). If a phishing email includes a link for a user to click to obtain more information (which leads to a spoofed website and possible identity disclosure), this is *pharming*. Links clicked by a user may reveal *malware*, a term derived from malicious software, which robotically downloads software intended to corrupt files, applications and computing systems (Nykodym et al., 2010). Types of malware include trojans, viruses, worms and rogueware (Anti-Phishing Work Group, 2011). Any type of encounter where deceitful or malicious phishing is constructed is known as a *scam*.

There are two different types of phishing categories: *deceptive phishing*, the act of trying to deceive the user into submitting personal details (Bergholz et al., 2010) and *malicious phishing*, where malware (of any type) is installed onto an individual PC or

computer system to cause harm (Feigelson & Calman, 2010; Nykodym et al., 2010). These attacks are becoming more sophisticated as users try to avoid them with stringent anti-virus software and education techniques. Although this focus is important, the effort to prevent phishing is somewhat misdirected; phishing attacks the most vulnerable link in the security chain which the user (Amin et al., 2010; Feigelson & Calman, 2010).

Facebook Phishing

Information contained in social networking accounts can provide a phisher with copious amounts of personal user data (Kirwan & Power, 2011). Facebook regularly receives phishing and massive malware attacks (Amin et al., 2010; Bonneau, Anderson, & Danezis, 2009) which manifest in auto-generated emails and website pages.

In Facebook, a personal account can be configured to routinely update a subscriber via email of any changes to the account (such as a *Like, Comment, Friend Request* or *Photo Tag*) (Facebook, 2012). The user knows which friend triggers the notification by examining the *subject* and *content*, with the option to click on a link to go to Facebook to learn more. However, genuine Facebook auto-email and link syntaxes are complex and are difficult for ordinary users to distinguish as phish (Bonneau et al., 2009). For example, because the following genuine link belonging to the researcher contains unfamiliar syntax, it could easily be mistaken as pharming:

http://www.facebook.com/n/?permalink.phpandstory_fbid=10150128030712949andid=577887948andmid=3f82bdbG2271deccG671057bG36andbcode=LcJLjvD7andn_m=klp%40eircom.net

Trust Indicators

Research has identified various elements, or cues, within emails and web pages that underpin a user's trust level in establishing phishing security (Bergholz et al., 2010; Dhamija, Tygar, & Hearst, 2006; Jakobsson et al., 2007). Jakobsson et al (2007) completed an experiment with seventeen participants by showing them a mixture of authentic and fake website and email stimuli. The research revealed there are factors that make a difference to believing email or website authenticity, and people *do* notice them. For example, spelling, design, logos, relevance and personalisation make a

difference when evaluating legitimacy; people look at web addresses (uniform resource locators, or URLs); and too much security can look phishy. In a separate study, Jakobsson et al. (2007) observe that users who notice elements missing on a screen sometimes rate the example as phish, even if it is genuine.

Examples of email security trust factor types include the subject line, “From” email address (Facebook.com must be part of the address) and “Reply-to” email address (email address is normally related to the email, and is never duplicated with “from” email address). Other trust factors include the greeting (the Facebook username is always used), login (login text is not used by Facebook, however login links are provided), content (matches the subject line) and links (hovering over links must point to Facebook.com) (Bergholz et al., 2010). Figure 1 represents an example of a Facebook phishing email.

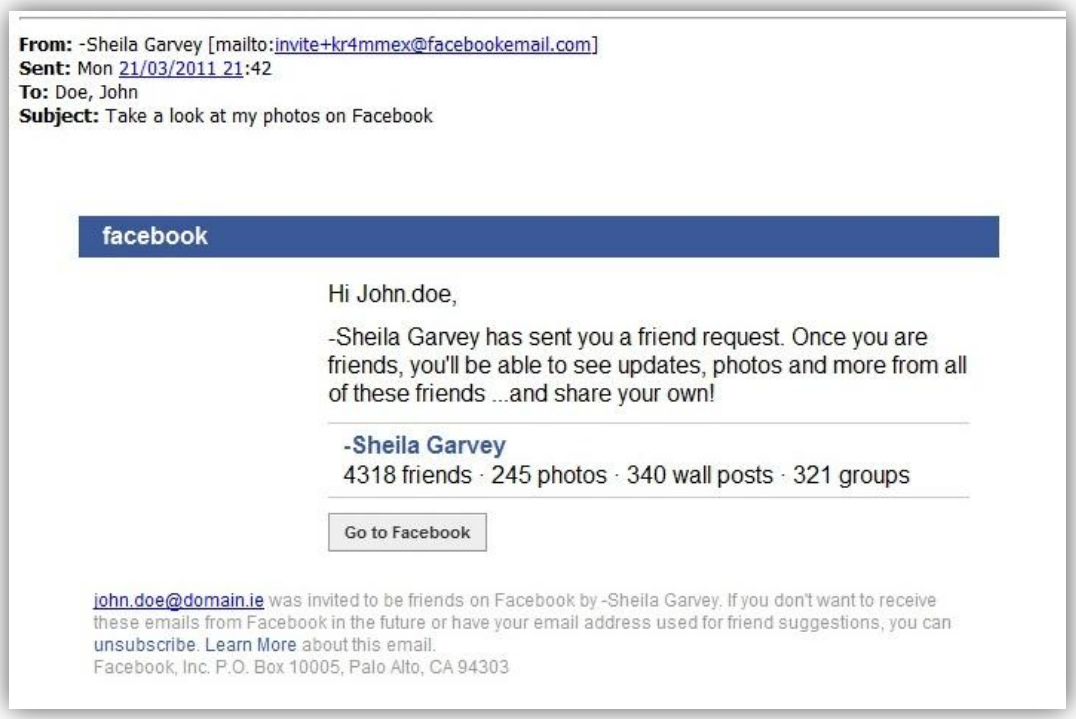


Figure 1. Facebook phishing email

In the example above, there are several trust factor violations to indicate this is not a genuine Facebook email. The “From” field has an obscure dash and the domain is facebookemail.com instead of facebookmail.com; the “Return-to” line is missing and the “From” content (invite), subject line (photos) and content (friend request) do not

match. Less noticeable, the Facebook logo is not the correct font and the greeting (Hi John.Doe) does not follow the standard format (Hi John). The case of 4318 friends is an obvious alarm, and all links point to facebookemail.com.

If the user did not notice the email was not genuine and clicked *Go to Facebook*, the user would possibly be pharmed to another website for more phishing or possible malware. This is a particular example of a mass phishing attack, where a generic email is sent to thousands of people. This type of phishing is simple; the design of the email (visual graphics, layout, colour palates) and the writing techniques (language and style) are easily replicated from any genuine Facebook email.

It has been found that spoofed emails and websites which look *too good* are noticed by users as possible fakes; errors are made in thinking websites which are actually phishy are legitimate (Jakobsson, 2007), or trust is assumed because the apparent source is from a connected friend (Petre, 2010). Amin et al (2010) constructed a mock phishing experiment where, using a fake Facebook account sent spoofed Facebook email messages to two hundred strangers asking to “Check out my latest pictures”. Surprisingly 35% of the recipients clicked on the link inside the email, which could have opened a site containing malware.

While logos and page elements are important to check, they are extremely easily to replicate using the brand’s open source code. Figure 2 is an example of a Facebook phishing login page.

Figure 2. Facebook phishing login page

Figure 2 looks genuine, but there are several factors to indicate it is not authentic. The URL is loginfacebook.com and not the standard facebook.com. There are two areas missing which would normally indicate a genuine sample: *Why do I need to provide my birthday*, *Terms and Data Use Policy* and *Create a Page* (see Figure 3).

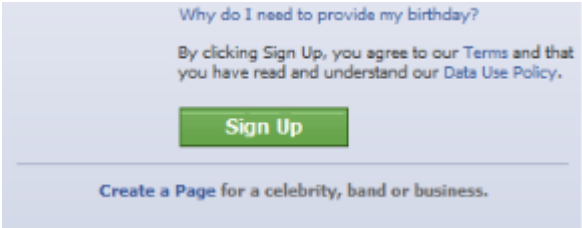


Figure 3. Missing elements from phishing example

Additionally, the links point to loginfacebook.com, which becomes apparent in the taskbar when a user hovers over the link.

Social Engineering Practices and Persuasion

Social engineering is the psychological manipulation of an individual to perform a certain behaviour that they would not normally do (Parrish et al., 2009; Soghoian & Jakobsson, 2009; Wright, Chakraborty, Basoglu, & Marett, 2010). In a phishing context, the exploiter does not focus on technological weaknesses, but on an

individual's vulnerabilities. In psychology, social engineering may have a foundation in persuasion (Workman, 2008).

Persuasive techniques relating to reciprocation, consistency, social proof, likeability, authority and scarcity (Cialdini, 1993) were reviewed with an industrial-focused sample with findings relating to phishing susceptibility and commitment (Workman, 2008). Those who rated high in normative commitment were more likely to reciprocate with sensitive corporate details when offered free items such as software and vouchers; those who rated highly in continuance commitment provided confidential information when repeatedly asked to do so; and individuals rating highly in affective commitment provided information in order to be included or accepted (Workman, 2008). The use of self-reports in this study may not completely represent the true behaviour of the sampler; further research in this area would be useful.

Post-Phishing Analysis

It is noted in experimental phishing studies that results may not fairly represent the true level of participant phishing knowledge due to a heightened level of awareness (Dhamija et al., 2006; Vishwanath et al., 2011; Wright et al., 2010). The Hawthorne effect, identified by Roethlisberger and Dickson (1934) and later coined by Landsberger (1958), identifies the change of an individual's behaviour when the individual is being observed. For example, participants asked to rate phishing trust factors may take more time and consideration in an experimental setting with a researcher than what would be normal. Researchers also encounter ethical and technical concerns while studying behaviour responses in deceptive phishing experiments (Vishwanath et al., 2011). Some participants have become angered about being misled and have demanded researchers to be dismissed or reprimanded (Jagatic et al., 2007).

A recent group of researchers were provided with the opportunity to examine responses to two genuine phishing attacks without the added complexities of the Hawthorne effect or technical/ethical impediments of a deceptive experiment (Vishwanath et al., 2011). The phishing attacks occurred over the space of a week and targeted a general university population for university login and password information using urgent language, "UPGRADE YOUR EMAIL ACCOUNT NOW" (email 1 subject line) and "VERIFY YOUR UNIVERSITY EMAIL ACCOUNT

NOW" (email 2 body text) (Vishwanath et al., 2011). The authors conducted post-phishing analysis by asking intended university victims to participate in a survey about student email use; students were shown, in random order, the two phishing emails and were asked if they remembered the mail, how they likely they were to respond to it and if they actually did respond. Of 325 responses, four participants responded to the first email, four to the second email and one participant responded to both. The authors found that overall participants focused mainly on urgency cues and less on other trust factors such as email source, grammar and spelling. High habitual media use (such as logging into email the same time every day while eating breakfast) indicated there was less cognitive involvement and was identified as a factor in phishing susceptibility. Email load was also significant; those who received more emails were more likely to be phished.

Understanding the Psychology of Phishing Success

As discussed, convincing trust indicators are one method in which users fall for phish. The more professional it looks in terms of, for example, logos, spelling and relevance, the more susceptible someone is to fall for a scam (Bergholz et al., 2010; Dhamija et al., 2006; Jakobsson et al., 2007). Kirwan and Power (2011) recognise cues as aspects of human decision-making; recognisable elements help users to determine if what they see is within the right context and therefore trustworthy. The way humans interpret cues in order to make a decision is multifaceted from a psychological perspective; factors which may influence the decision making process in phishing legitimacy include cognitive biases and personal emotions.

Prejudices such as the optimism bias, where an individual underestimates a negative risk involved, may leave an individual with unrealistic views vulnerable to phishing (for example, "I have a new computer with good software, it will not happen to me"). Representativeness heuristic, where a judgment is made based on information represented in memory (Tversky & Kahneman, 1974), could lead to an erroneous decision (such as, "the logo and layout look good to me so they must be right"). Cognitive dissonance, the feeling of conflict in a situation with personal ideals (Festinger, 1957) provides a chance for a user to justify previous behaviour (for example, responding to a spiritually slanted email in order to help missionaries spread the word of God). Confirmation bias, where an individual looks for validating cues to

support a belief (Plous, 1993), may enable a user to overlook dubious stimuli (for example, a user who trusts an email to be from Facebook looks for other cues such as personalisation and language use to confirm the belief; meanwhile, links within the text may point to bogus destinations). Salience, the prominence level at which an item stands out amongst other similar elements (R. Miller & Grace, 2002) may sway individuals into thinking an email is satisfactory (for example, a national bank logo regularly received by its personal customers). Lastly, cognitive load, or the capacity at which an individual uses working memory (G. Miller, 1956), may impede an individual's ability to make a level decision when there are too many thoughts being processed . For example, a busy manager who has many phone calls emails and meetings may not have the time or ability to check emails and webpages for trust factors.

Personal emotions such as greed, fear, anxiety and guilt also play an important role in making decisions that may affect a user's susceptibility to phish (Parrish et al., 2009). A user who is tempted by greed may easily fall for a lottery phishing email. Fear of having a savings account closed may motivate a customer to click on an illegitimate bank email. A user with trait anxiety may respond anxiously to a time pressured email such as, "reply immediately to claim a prize"; and an individual sensitive to guilt may respond to an email, "please help us, we do not have enough to eat".

Each of these psychological biases and emotions act as influencers in human decision-making. By acknowledging the qualities that exist in society, it is easier to understand the psychology of phishing success and the ease in which psychological elements may provide a gateway to phishing vulnerability.

Victimisation: Financial and Psychological Effects

As previously indicated, the financial implications of phishing are immense. In the case of identity theft, not only is there usually monetary loss for both the individual and financial institution, but there are time losses in releasing credit card and bank accounts restrictions, and for restoring a bad credit rating (Feigelson & Calman, 2010; Kirwan & Power, 2011).

The psychological effects on victims manifest in physical, emotional and compounded victimisation conditions. A group of researchers completed an impact and coping

study on individuals who had been victims of identity theft and found the individuals displayed both emotional and physical symptoms at two weeks and twenty six weeks intervals after learning about the theft (Sharp, Shreve-Neiger, Fremouw, Kane, & Hutton, 2004). Emotional symptoms reported included anxiety/fear, frustration, disbelief/shock, distress/desperation, mistrust/paranoia and depression. Somatic symptoms included anxiety, nervousness, appetite problems, weight loss, headaches, gastrointestinal problems, muscle tension, skin reactions, fatigue/lethargy and depression. Not surprisingly, those who had not had a resolution to their situation twenty-six later reported much higher rates of somatisation, depression and anxiety than those who had resolution (Sharp et al., 2004)

Other aspects of victimisation include victim facilitation, where the victim may (unintentionally) provide easy access for a phisher; victim precipitation, where there is shared responsibility; and secondary victimisation, where family, friends or authorities may place blame on the victim (Mendelsohn, as cited in Kirwan & Power, 2011, p. 105). For example, Steve enjoys playing Facebook games and apps online with his friends, and receives regular posts about his game playing on his wall. Steve has used his credit card on several occasions to buy credit to purchase virtual goods to use in the games and permanently stores his credit card details within his Facebook account for easy access. One day Steve receives an email notification relating to his game and clicks on a link to log him in to Facebook directly. When he enters his username and password, he receives a message that Facebook is undergoing temporary maintenance. It is several days later when he receives a call from the bank that he realises his login credentials were stolen and he has become a victim of credit card fraud, incurring substantial personal damages. Steve feels very upset and thinks Facebook should pay for the reimbursements for not keeping his details secure; however, Facebook maintain it is the responsibility of the user to keep login credentials safe. Meanwhile, Steve's friends and family think Steve could have been more careful about that dubious link and not have stored his credit card information online. This is a typical example of Steve facilitating the phisher (victim facilitation) and being a subject of secondary victimisation (blame by the friends and family).

Identifying the financial and psychological effects of phishing victims helps to link the fraudulent cybernetic arena with the actual world and physical human beings.

This consideration to victimisation enables a holistic approach for understanding phishing and its successes.

Personality Factors

Personality is commonly categorised into five domains, each containing six facets or subsets relating to that domain. Domains include extraversion, openness to experiences, conscientiousness and agreeableness. The Neuroticism, Extraversion, Openness to experiences Personality Inventory Revised (NEO PI-R) (Costa & McCrae, 1992) is a globally recognised personality measure (commonly known as the Five Factor Model), which identifies these elements. Table 1 details facets and adjectives for each domain (McCrae & John, 1992). The NEO PI-R is a self-reporting scale consisting of 240 questions, which takes approximately 30-40 minutes to complete. Another reliable scale to measure personality domains is the Big Five Inventory 44 (John & Srivastava, 1999), or BFI 44. This measure consists of 44 questions and takes approximately five to ten minutes to complete.

Table 1

Personality Domains, Facets and Scoring Adjectives

Domain	Facet	High Scoring	Low Scoring
Neuroticism	Anxiety	Worried	Calm
	Angry-Hostility	Temperamental	Even-tempered
	Depression	Self-conscious	Comfortable
	Self-Consciousness	Emotional	Unemotional
	Impulsiveness		
	Vulnerability		
Extraversion	Warmth	Joiner	Loner
	Gregariousness	Talkative	Quiet
	Assertiveness	Active	Passive
	Activity	Affectionate	Reserved
	Excitement seeking		
	Positive Emotion		
Openness to Experience	Fantasy	Imaginative	Down-to-earth
	Aesthetics	Creative	Uncreative
	Feelings	Original	Conventional
	Actions	Curious	Uncurious
	Ideas		
	Values		
Agreeableness	Trust	Trusting	Suspicious
	Straightforwardness	Lenient	Critical
	Altruism	Soft-hearted	Ruthless
	Compliance	Good-natured	Irritable
	Modesty		
	Tender mindedness		
Conscientiousness	Competence	Conscientious	Negligent

Domain	Facet	High Scoring	Low Scoring
	Order	Hard-working	Lazy
	Dutifulness	Well-organised	Disorganised
	Achievement striving	Punctual	Late
	Self-Discipline		
	Deliberation		

When looking at the area of personality and social networking, research in each domain is emerging.

Neuroticism, associated with apprehension, nervousness and sensitivity to stress, is linked with extraversion in expressing their "true selves" online (Amichai-Hamburger, Wainapel, & Fox, 2002; Tosun & Lajunen, 2010). Together with openness, those who score highly in neuroticism are more likely to blog (Guadagno, Okdie, & Eno, 2008), and individuals scoring high on neuroticism spend more time on Facebook (Ross et al., 2009). These users are also more likely to post photographs of themselves (Amichai-Hamburger & Vinitzky, 2010).

Extraversion is linked to sociability and positive emotion. Facebook users, when compared to non-Facebook users, are more extraverted and narcissistic (Ryan & Xenos, 2011) and extroversion and neuroticism are significantly related to online activities (Correa, Hinsley, & de Zúñiga, 2010). Extraversion is also significantly correlated with Facebook's communication features chat, messages, comments and wall interaction (Ryan & Xenos, 2011) as well as belonging to Facebook groups (Ross et al., 2009). Demographically, extraversion (for men) and extraversion and openness (for women) were positively related to the amount of time spent on instant messaging and social networking sites; additionally, extraversion is linked to this type of social media and young adults (Correa et al., 2010).

Openness is the willingness to undergo new experiences and to explore creative and cognitive interests. One research study found that individuals who scored highly in openness were more willing to use Facebook, and used the personal information features within Facebook more than those individuals who had a low score of openness (Amichai-Hamburger & Vinitzky, 2010; Ross et al., 2009). Additionally, those scoring high in openness also added and replaced photographs more than those who did not rate as highly on openness (Gosling, Augustine, Vazire, Holtzman, & Gaddis, 2011).

Agreeableness reflects individuals who are cooperative, trustful and unselfish. One study found that females who rate highly in agreeableness have more photographs in their Facebook accounts than their less-agreeable counterparts (Amichai-Hamburger & Vinitzky, 2010). It was also found that these individuals viewed more pages, including their own and pages belonging to others (Gosling et al., 2011).

Conscientiousness echoes a level of meticulousness, organisation and precision of an individual. Research results support that Facebook users do not rate as highly on conscientiousness as non-Facebook users (Ryan & Xenos, 2011) and those who score lowly on conscientiousness spend more time on Facebook (Gosling et al., 2011; Ryan & Xenos, 2011). However, it is purported that individuals who scored high on conscientiousness had a higher number of Facebook friends and uploaded fewer pictures (Amichai-Hamburger & Vinitzky, 2010).

While research exists regarding relationships between personality, internet use and social networking sites, gaps in literature exist between these elements and phishing susceptibility.

In terms of conscientiousness, which is the focal personality trait in this study, and victimisation, research suggests there is a positive correlation between high levels of conscientiousness and less victimisation in adolescents (Jensen-Campbell & Malcolm, 2007). A further study linked poor self-control in adolescents with those who exhibited external problem responses, such as aggression and poor impulse control, with conscientiousness; these children were more likely to become physically victimised than those adolescents who rated positively with self-control (Harris, 2009). Although study participants are limited to adolescents, there is literature opportunity to examine the correlation between conscientiousness and victimisation in adults.

Impulsivity

According to Evenden (1999), impulsivity is a subset of all personality traits, regardless of any theoretical approach and McCrae and John (1992) categorised impulsivity as one of the six facets of neuroticism. Although there is discrepancy in what defines impulsivity, most researchers find that impulsivity relates to an individual’s ability to behave without the complete forethought or realisation of what

is usually a negative consequence. There are also assessment disagreements (Evenden, 1999), however the Barratt Impulsiveness Scale (BIS-11) (Patton, Stanford, & Barratt, 1995) is the most widely used self-reporting mechanism to ascertain impulsivity; this scale consists of several second and first order factors, as illustrated in Table 2 below.

Table 2

Barratt Impulsiveness Scale - Factor Structure and Description

2nd Order Factors	1st Order Factors	Descriptions
Attentional	Attention	I do not "pay attention." I "squirm" at plays or lectures.
	Cognitive Instability	I have "racing" thoughts. I change hobbies.
Motor	Motor	I do things without thinking. I make-up my mind quickly. I act on the spur of the moment.
	Perseverance	I change jobs. I change residences. I can only think about one thing at a time.
Nonplanning	Self-Control	I say things without thinking.
	Cognitive Complexity	I get easily bored when solving thought problems. I am more interested in the present than the future.

In the area of impulsivity and victimisation, Purvis (2011) highlights that risk perception, trust and impulse influence individual vulnerability to online attack. Purvis's method, however, was literature review based (peer reviewed journals, conference papers and internet search engines) and little detail is presented to describe how the results were analysed. Separately, another study examined the participants in fraudulent Ponzi schemes and found that most victims who invested in these schemes were men rated highly in risk and impulsivity, and were susceptible to gambling (Barnard, 2009). Lastly, a study examining self-control and online victimisation conducted an online experiment involving 295 university students (mean age=40) purported that self-control was positively related with online harassment from strangers and non-strangers and negatively related with person-based cybercrime

victimisation (the user was a specific target) (Ngo & Paternoster, 2011). Additionally, the researchers noted they did not find any significance to phishing, but stated that anyone, regardless of self-control, is a potential phishing victim.

Trust

McCrae and John (1992) categorised trust as one of the six facets of agreeableness. Trust represents a level of security felt towards another individual (McKnight, Choudhury, & Kacmar, 2002). Phishers have learned quickly they are more successful at retrieving personal data when they impersonate a trusted entity such as a bank, ISP or government agency (Feigelson & Calman, 2010). Due to routine interactions between people who share common interests, Facebook provides the environment for a level of trust to develop; people trust others who are perceived to be real (Amin et al., 2010). Additionally, it is found that trusting behaviour is determined by former trusting experiences, as well as by the level of social relationships (Glaeser, Laibson, Scheinkman, & Soutter, 2000). Workman (2008) found those who were more trusting were more susceptible to social engineering that those who were not as trusting.

Petre (2010) demonstrated the ease in which a phisher could enter a circle of friends by setting up a Facebook account, joining groups to acquire friends, and sending the new Facebook friends an illegitimate link. Twenty four per cent of the new Facebook friends followed this link even though they did not know *really* whom it was from or where the link was going. Petre and the new Facebook friends had never met in real life, which demonstrates the power of online trust purely from social connections.

Trust research has been completed in online firms (Bhattacherjee, 2002; McKnight et al., 2002) and it has been found that trust and familiarity is directly related to whether a user interacts with the company (Bhattacherjee, 2002). Trust online is the security that neither the e-commerce company nor the customer will take advantage of the other's vulnerabilities (Bhattacherjee, 2002). It is noted by Bhattacherjee (2002) and McKnight et al. (2002) that consumers base trust in online merchants according to the merchant's ability (competence), benevolence and integrity. Bhattacherjee defines ability as the proficiency and knowledge of the vendor to perform an expected transaction; benevolence as a company's expression of good faith and certainty; and

integrity as the credibility in which a seller conducts transactions, defines (and upholds) policies and handles consumer data.

Demographic Factors

According to Sheng, Holbrook, Kumaraguru, Cranor and Downs (2010), women are more susceptible to phishing than men, and participants aged 18-25 are more susceptible than any other age group. The study by Sheng et al. looked at age, gender and technical knowledge of participants by presenting real and fake emails and websites. After the initial experiment, each participant received training before being retested. Although there was an improvement of 40%, there were users who avoided legitimate links all together, thus creating false positives in the results. Sheng et al (2010) suggest women do not perform as well as men because women are not as technical (in training and knowledge); additionally, it is believed the reason younger individuals fall for phish more than any other age group is attributed to lower education level, internet inexperience, absence of training opportunities and fewer aversions to risks.

Research Aim

When considering data relating to personality, impulsivity and trust with online fraud and Facebook, the following research question emerges:

Research Question 1: Is there a correlation between personality and a susceptibility to Facebook phishing?

As discussed, conscientiousness is associated with meticulousness and self-discipline. According to Ryan and Xenos (2011) and Gosling et al. (2011), those who score highly on conscientiousness spend less time on Facebook, which arguably is less of an opportunity for phishing to occur. Research in adolescents also suggests a lower rate of victimisation in those who score highly in conscientiousness (Jensen-Campbell & Malcolm, 2007). Based on this rationale, and the absence of research in the area of Facebook phishing and personality, the following hypothesis is purported:

Hypothesis 1: Participants who score highly in conscientiousness are less susceptible to Facebook phishing than participants who score lowly in conscientiousness.

Regarding impulsivity, Purvis (2011) suggested individual impulsivity was an influencer in online attack while Barnard (2009) found that men who fell for Ponzi schemes had impulsive characteristics. Ngo and Paternoster (2011) reported that low self-control was a target indicator to cybercrime and that there was no significance between self-control and phishing. On this basis, and the absence of research in the area of Facebook phishing and impulsivity, the following hypothesis is alleged:

Hypothesis 2: Participants who score highly in impulsivity are more susceptible to Facebook phishing than participants who score lowly in impulsivity.

Considering Facebook regularly receives phishing and massive malware attacks (Amin et al., 2010; Bonneau et al., 2009), contains obscure auto-email and link syntaxes (Bonneau et al., 2009) and provides the environment for a level of trust to develop (Petre, 2010), the following hypothesis is presented:

Hypothesis 3: Participants who score highly in trust in Facebook as an online company are more susceptible to Facebook phishing than participants who score lowly in trust in Facebook as an online company.

When considering data relating to email and webpage trust factors and authenticity, a second research question arises:

Research Question 2: How observant are users to phish stimuli?

Jakobsson et al. (2007) observed that users who notice missing components in a genuine screenshot rate the example as not genuine; additionally, the researchers observed errors are made in thinking legitimate websites are actually phish. Hence, the following hypotheses are considered:

Hypothesis 4: Users will not identify all trust factors (present or missing) in Facebook emails and websites.

Hypothesis 5: Users will mistake authentic Facebook emails and web pages as phish.

Method

This phishing study was experimental in design and consisted of two parts. A questionnaire measured demographic, Facebook behaviour, Facebook trust, personality and impulsivity data (independent variables); and Facebook email and login web page screenshots measured phishing stimuli and rating figures (dependent variables). All data was quantitatively analysed.

Participants

This study was open to participants 18 years and older. Participant prerequisites included Facebook account holders with no prior computer security training or computer science degree within the last 15 years. This exclusion was due to their potential understanding of phishing, an insight advantageous over other groups and not a true reflection of the majority of Facebook users. Participants were recruited by convenience sampling among college students and professionals.

Materials

Each participant completed a four-section questionnaire before the phishing screenshots section took place. The questionnaire consisted of brief participant demographics and Facebook behaviour queries (see Appendix A) and three extensively used scales: the Big Five Inventory 44 (John & Srivastava, 1999) (see Appendix B), the Barratt Impulsiveness Scale (BIS-11) (Patton et al., 1995) (see Appendix C), and the Individual Trust in Online Firms Scale (Bhattacherjee, 2002) (see Appendix D).

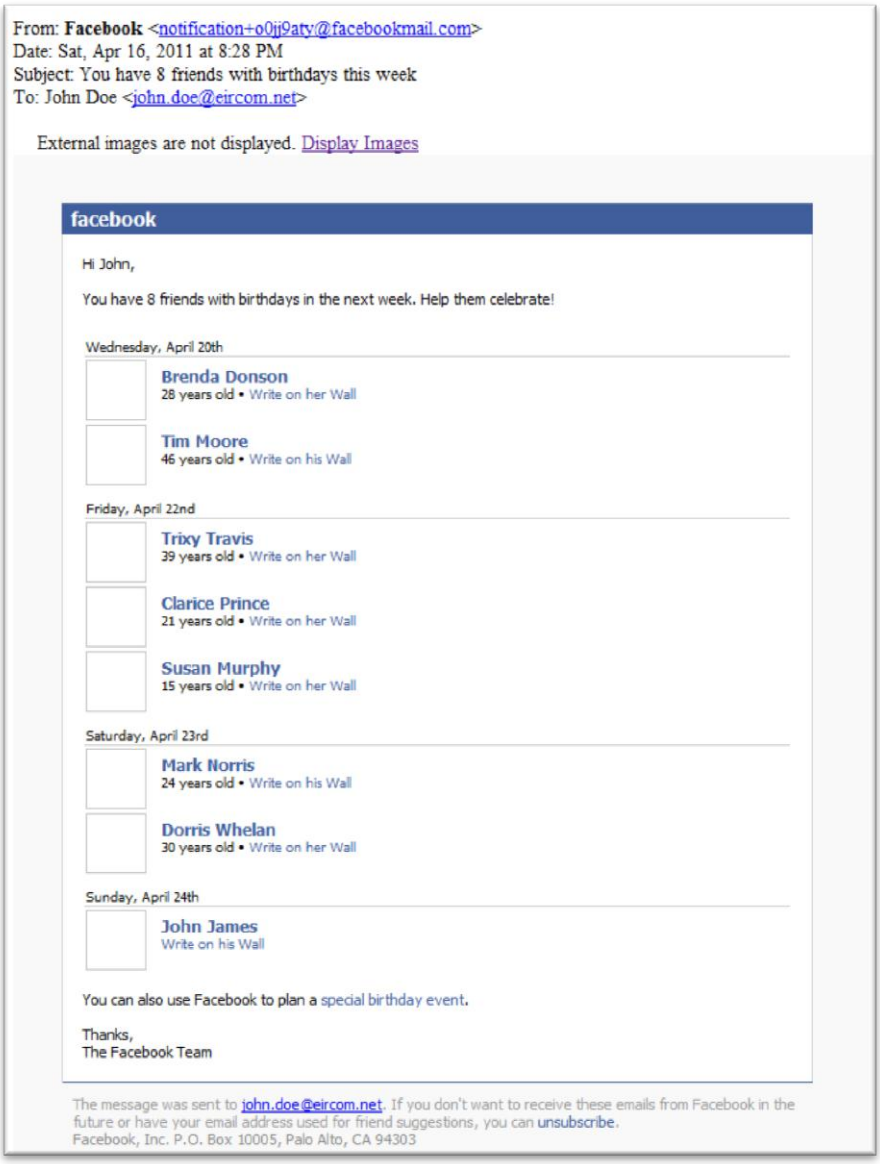
The Big Five Inventory 44 (John & Srivastava, 1999) measured neuroticism, extraversion, openness to experiences, conscientiousness and agreeableness personality factors amongst participants. This test is known to be reliable scale; John and Srivastava provide alpha reliability ranges on this scale that range from .75 to .90 in the US and Canada; three-month test-retest reliabilities range from .80 to .90, with a mean of .85. This test was chosen over other personality scales, such as the NEO-PI developed (Costa & McCrae, 1992), for time convenience.

The Barratt Impulsiveness Scale (BIS-11) (Patton et al., 1995) is a widely used self-reporting mechanism to ascertain impulsivity; this scale consists of several second order and first order factors, as illustrated in Table 2. Patton et al. demonstrate this

test to be a valid, reliable scale and report alpha coefficient ranges from 0.79 to 0.83. This scale contains 30 questions, which was considered a good fit for the experimental time allocation.

The Individual Trust in Online Firms Scale (Bhattacherjee, 2002) was selected to establish participants' trust in Facebook as an online company. This scale investigates the trustee's ability, benevolence and integrity. Reliability and validity (convergent, discriminant and nomological) for this scale were tested and accepted; Cronbach alphas ranged between 0.83 and 0.89. This scale contains ten items and was chosen for its ease of use and time for administration.

The second stage incorporated visual stimuli presented within four screenshots: one each to represent an authentic email, phish email, authentic web login and phish web login, as illustrated in the figures below.



From: **Facebook** <notification+o0jj9aty@facebookmail.com>
Date: Sat, Apr 16, 2011 at 8:28 PM
Subject: You have 8 friends with birthdays this week
To: John Doe <john.doe@eircom.net>

External images are not displayed. Display Images

facebook

Hi John,

You have 8 friends with birthdays in the next week. Help them celebrate!

Wednesday, April 20th

Brenda Donson
28 years old • Write on her Wall

Tim Moore
46 years old • Write on his Wall

Friday, April 22nd

Trixy Travis
39 years old • Write on her Wall

Clarice Prince
21 years old • Write on her Wall

Susan Murphy
15 years old • Write on her Wall

Saturday, April 23rd

Mark Norris
24 years old • Write on his Wall

Dorris Whelan
30 years old • Write on her Wall

Sunday, April 24th

John James
Write on his Wall

You can also use Facebook to plan a special birthday event.

Thanks,
The Facebook Team

The message was sent to john.doe@eircom.net. If you don't want to receive these emails from Facebook in the future or have your email address used for friend suggestions, you can unsubscribe.
Facebook, Inc. P.O. Box 10005, Palo Alto, CA 94303

Figure 4. Genuine Facebook email

Figure 5. Phishing Facebook email with phish elements

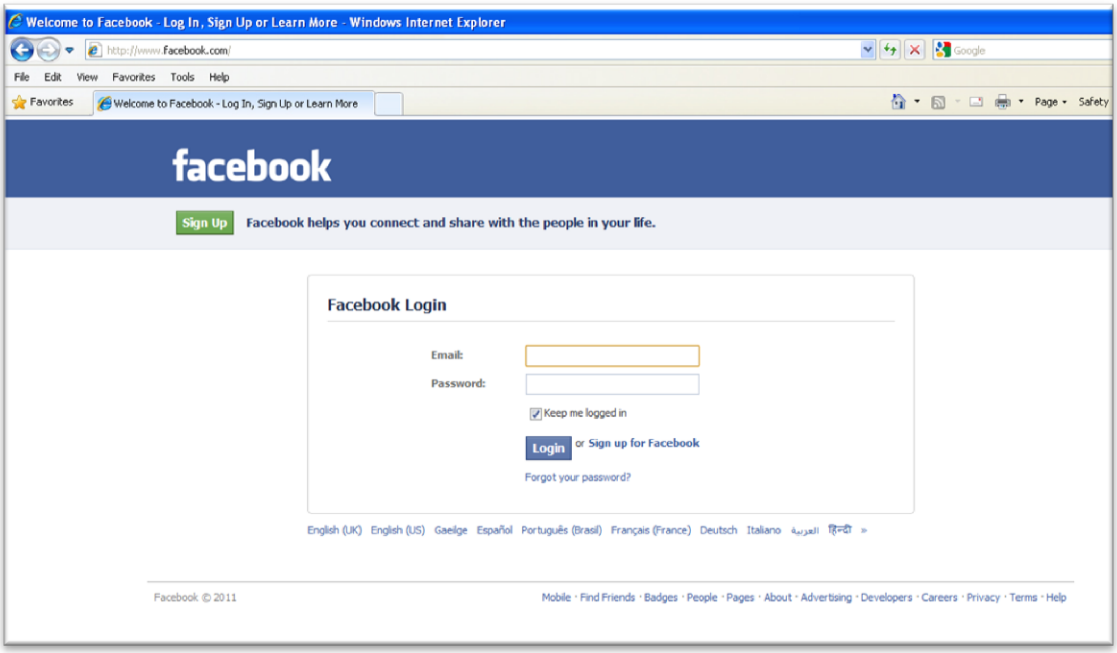


Figure 6. Genuine Facebook web login page

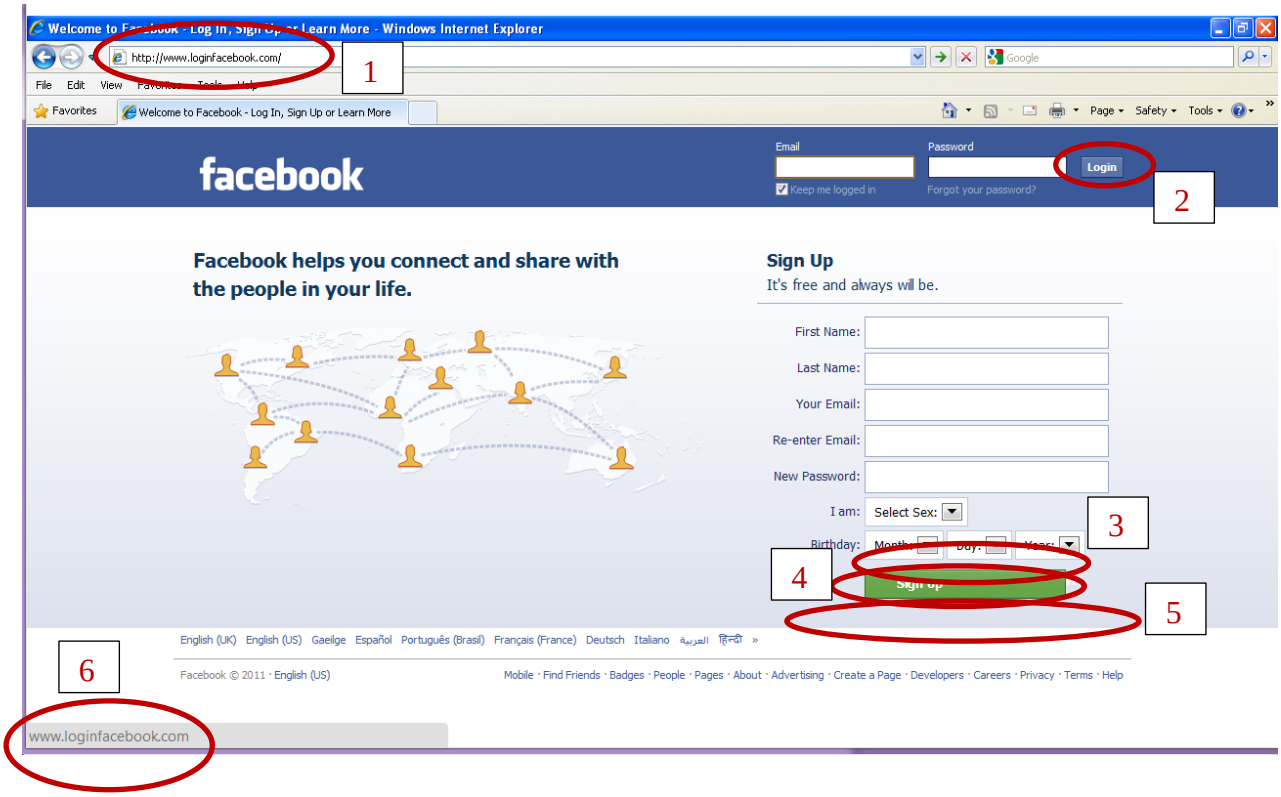


Figure 7. Phishing Facebook login page with phish elements

The HTML screenshots contained between six and twelve stimuli (see Appendix E for all stimuli and authentication); each screen included live links to facilitate hovering, and link destination views. All examples were modeled on legitimate email and login pages; however, the researcher manipulated genuine data to create bogus examples. Screenshot cues (both authentic and spurious) include email sender name, email address, subject line text, body content, logo, url, greeting, language selection, footer, copyright and links with active destinations. All screen sizes were 1071 x 605 pixels and 72 dots per inch (dpi).

Screenshot ratings and stimuli identification were recorded on a mirrored screenshot datasheet. Each stimulus (for bogus and genuine examples) was numbered with a rating checkbox (see Appendix F).

The screenshot section was audio recorded for verification purposes, which were utilised in the data analysis stage. The experiment was conducted on a laptop computer; the same computer and stimuli were used for all participants. A mouse was provided for participants unfamiliar with a touchpad. Prior to the main research, two participants completed pilot studies. This resulted in some questionnaire terminology changes and minor enhancements to screenshot stimuli.

Procedure

Research was conducted on a one to one basis to encourage participants to 'think out loud'. Verbal precondition assessments of computer security training, computer science degree and Facebook account status took place for each participant before performing the experiment. Each experiment took approximately twenty minutes to complete and consent was given before initiating the testing (see Appendix G).

Screenshots were preloaded in four separate tabs within a popular web browser. Once the questionnaire was completed, the participant was asked if he/she were familiar with the mouse and touchpad; it was important not to lead the participant to use the mouse or touchpad, but to let them know it was available. The audio recording was switched on and the participants were told they would be shown four Facebook email and login page examples (see Appendix H). They were asked to examine the pages to determine if the examples genuinely belonged to Facebook or were phish. Participants were asked to verbalise their observations.

As participants spoke about their observations, each identified cue was check-marked on a hard copy by the researcher (see Appendix F). The researcher also documented other observations, such as scrolling, hovering and clicking in field notes. Internet connection was not necessary for this study; clicking on links (genuine and illegitimate) lead the participant to a generic landing page, where they were asked to click the 'back page' arrow icon.

After reviewing each example, participants were asked to rate the examples as certainly phishing, probably phishing, unsure, probably not phishing or certainly not phishing. If not already disclosed, the participant was asked which features inspired confidence or generated suspicion in authenticity. A debrief page was provided at the completion of the experiment (see Appendix I).

Ethics

All participants were required to be over the age of 18 and sign a consent form prior to experiment commencement (see Appendix G). The consent form described the study purpose, provided a phishing definition and clarified the experiment was to be recorded. The consent form also explained that all data was completely confidential, participant anonymity was maintained and data would not be identified as theirs.

Participants had the right to refuse to take part and not answer questions. A debriefing form (see Appendix I) was provided with links to relevant websites should the participant have felt affected by the study or wished to learn more about internet safety and phishing.

Results

Descriptive statistics indicated the dependent variable stimuli count (genuine login webpage) was not normally distributed (skewness=3.339, kurtosis=11.190); thus, all data was analysed with non-parametric Spearman's rank-order correlations (two-tailed; α=0.05). Table 3 presents the means and standard deviations of measures. Note that screenshot rating values (for example, Rating Phish Email), range from 1 = certainly phish to 5 = certainly not phish.

Table 3

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Openness	17	28.00	45.00	37.1176	4.80732
Conscientiousness	17	26.00	41.00	31.1765	4.31908
Extraversion	16	14.00	40.00	27.2500	6.31928
Agreeableness	17	25.00	41.00	32.0588	4.27888
Neuroticism	17	10.00	31.00	22.7059	5.34748
Impulsivity	16	52.00	75.00	64.5000	7.04273
Attention	16	8.00	14.00	9.7500	1.94936
Cognitive Instability	16	4.00	10.00	6.3125	1.49304
Trust in Facebook	18	19.00	30.00	23.5556	3.16641
Rating Phish Email	19	1.00	4.00	2.0526	.97032
Rating Genuine Login	19	2.00	5.00	4.4737	.84119
Rating Genuine Email	19	1.00	5.00	2.6842	1.45498
Rating Phish Login	19	1.00	5.00	3.1053	1.79179
Stimuli Count Phish Email	19	.00	4.00	2.1053	1.24252
Stimuli Count Genuine Login	19	.00	3.00	.3158	.82007
Stimuli Count Genuine Email	19	.00	4.00	.9474	1.12909
Stimuli Count Phish Login	19	.00	2.00	.5789	.69248

Participant ages ranged between 18-60 years; however, there were no participants in the 36-42 year age group. In total, there were 12 females (63%) and 7 (37%) males. Both the mean and median groups were the 27-35 year range. Figure 8 illustrates the gender and age distribution.

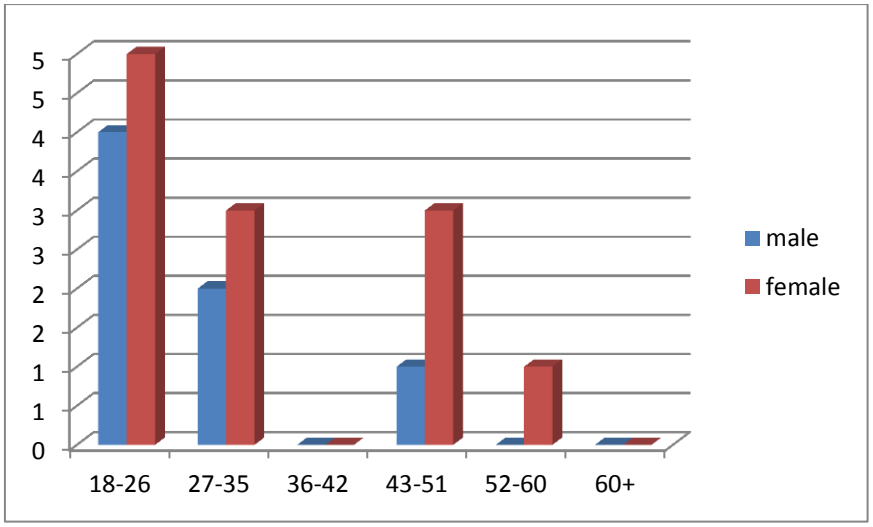


Figure 8. Gender and age distribution

Personality

Correlations of personality traits with screenshot ratings and stimuli count are listed in Table 4 and Table 5 located in Appendix J and Appendix K, respectively.

When comparing the relationships between screenshot ranking and personality traits, the following results for email (Figure 9) and website (Figure 10) phish screenshots were found:

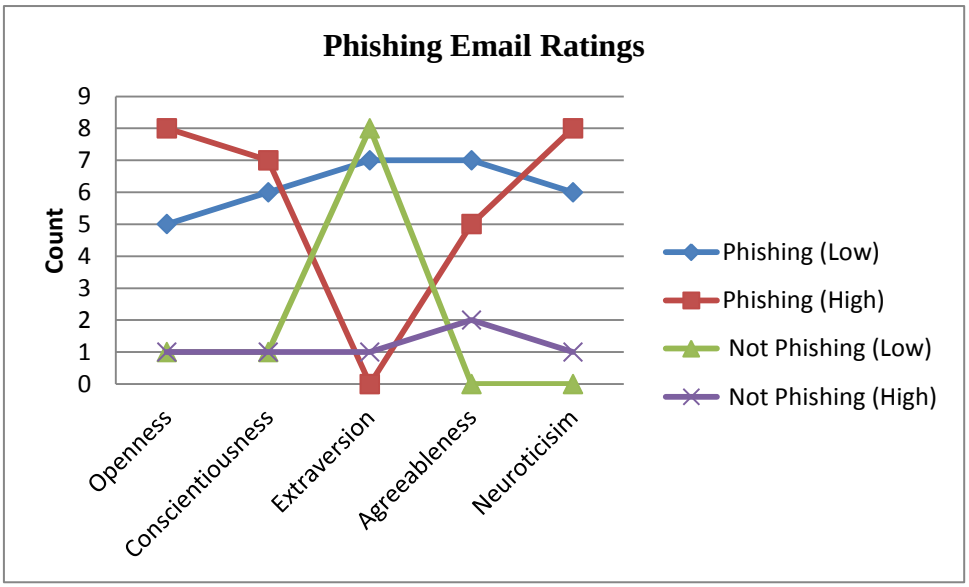


Figure 9. Total count rating for email (phish) screenshot

In the phishing email screenshot, 89% of participants correctly identified the example as phish; there were more individuals who rated the phishing email correctly that were

rated highly in openness and neuroticism. Following this group, those who scored highly in conscientiousness and lowly in agreeableness also answered correctly. Participants with introversion (low extraversion) were more likely to rate the email erroneously. Conversely, there were slightly different results in the phish website login rating, as seen in the figure below.

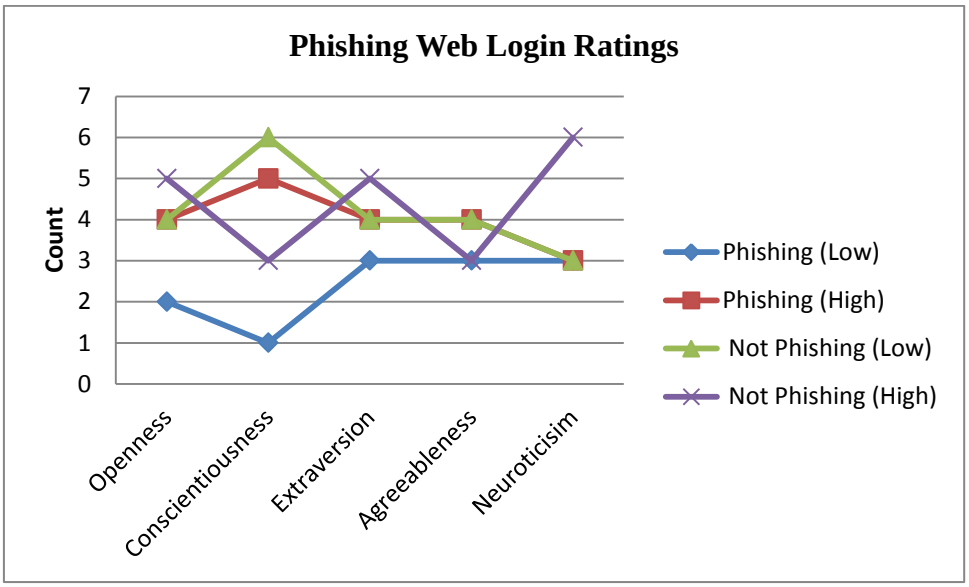


Figure 10. Total count rating for website (phish) screenshot

In the above phishing website screen rating, 58% of participants answered incorrectly; individuals who rated this screen incorrectly scored lowly on conscientiousness and highly on neuroticism. Most of those who rated the screen correctly scored highly on conscientiousness.

In terms of agreeableness, there was a positive correlation with cognitive instability (a subscale of impulsivity) (r_s = .536, p<.05). Additionally, there was a negative correlation with the genuine web login screenshot rating (r_s = -.486, p<.05), which indicates that participants who score highly in agreeableness erroneously mistake the genuine sample as phish. Lastly, agreeableness is positively related with Facebook login frequency (r_s = -.549, p<.05), which indicates more login instances (frequent login was reversed scored).

Hypothesis 1 posited that participants who score highly in conscientiousness are less susceptible to Facebook phishing than participants who score lowly in conscientiousness. While conscientiousness was not correlated with the rating number results for the phishing email (r_s = -.131, p=.617), and rating of the phishing web

login page was marginally correlated (r_s = -.461, p=.063). This indicates that participants with lower levels of conscientiousness may fail to identify the phishing web login correctly (see Figure 11 below).

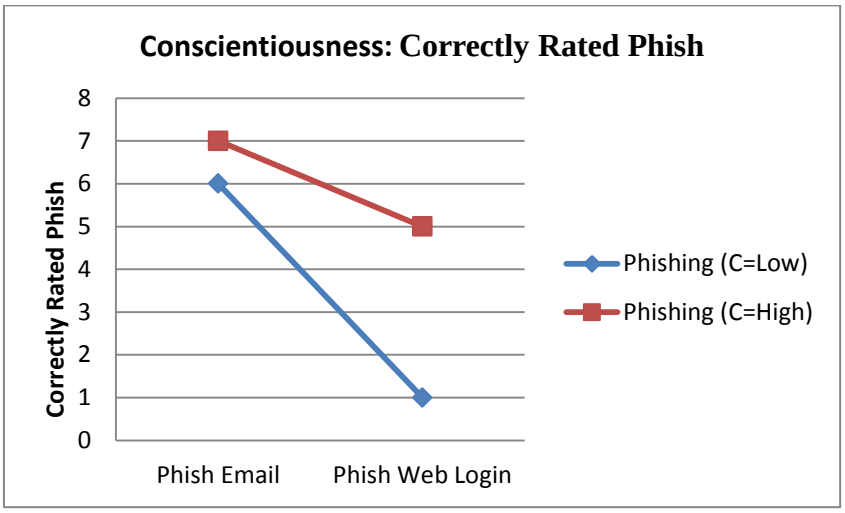


Figure 11. Conscientiousness and correctly rated phish count

Conversely, when looking at conscientiousness and incorrectly rated phish, those who rated lowly in conscientiousness made more rating errors than participants who rated highly in conscientiousness (see Figure 12).

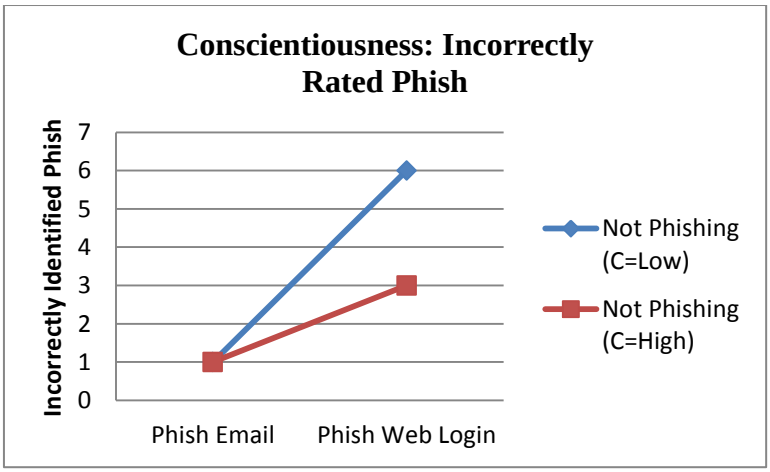


Figure 12. Conscientiousness and incorrectly rated phish count

When considering conscientiousness and the number of stimuli identified on the phishing email (r_s = -.078, p=.766) and web login page (r_s = .176, p=.499), there are no significant correlation findings (see Figure 13).

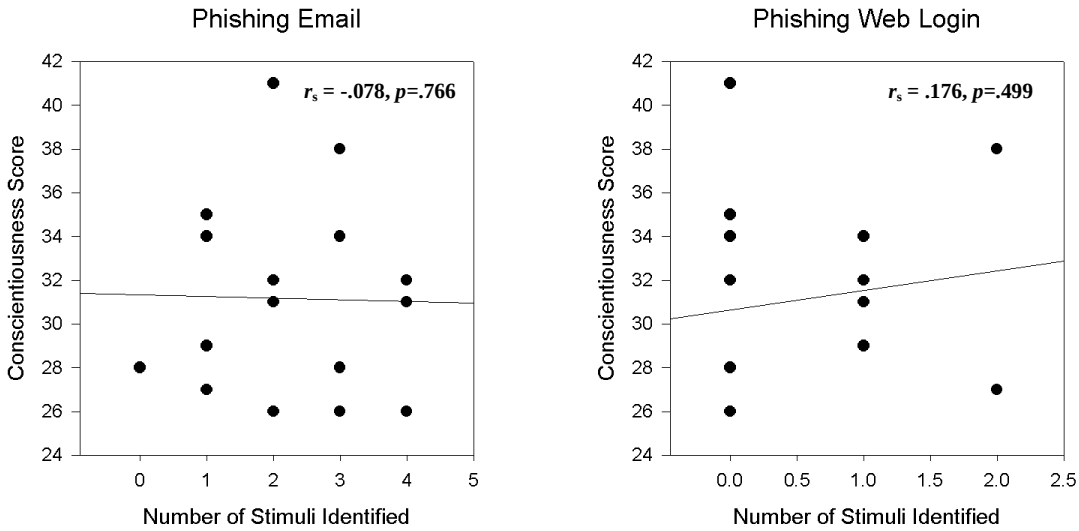


Figure 13. Conscientiousness identified stimuli count

Impulsivity

Correlations of measures of impulsivity and screenshot ratings and stimuli count are located in Table 6 and Table 7 in Appendix L and Appendix M, respectively. When focusing on participant impulsivity levels and correctly identifying both phishing screenshots as phish, 35% of the users who have a high level of impulsivity answered correctly and 65% of users who have a low level of impulsivity answered correctly (see Figure 14). Additionally, 70% of the users who incorrectly rated phishing as genuine scored highly in impulsivity (see Figure 15). In other words, those users who score lowly in impulsivity are better at correctly rating phish and make fewer mistakes in rating a genuine example as phish.

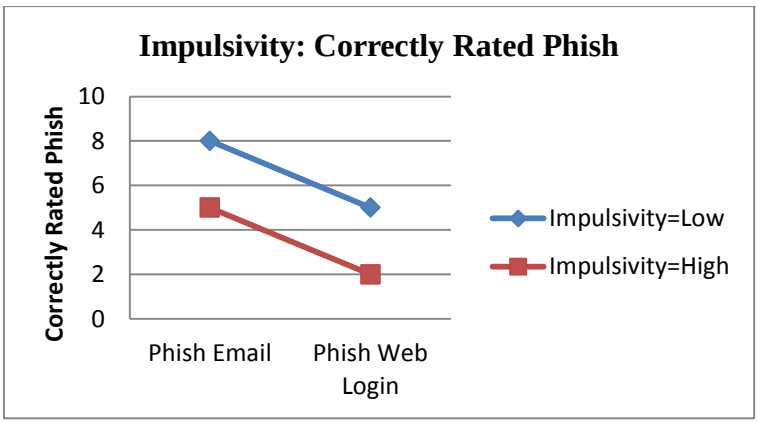


Figure 14. Impulsivity and correctly rated phish count

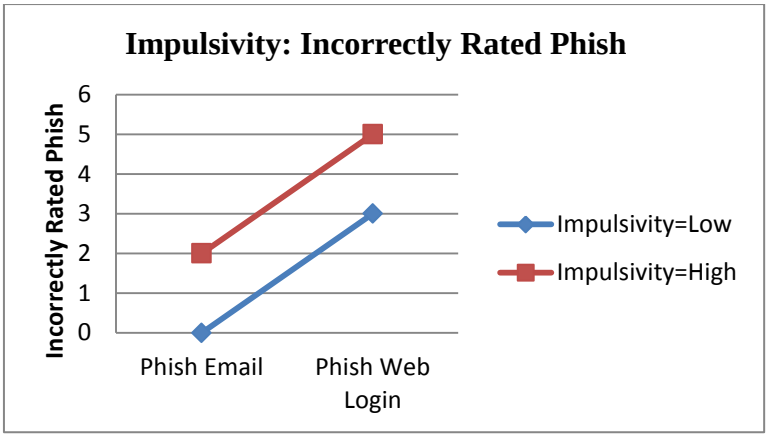


Figure 15. Impulsivity and incorrectly rated phish count

Cognitive instability, a subscale of impulsivity, was negatively correlated (r_s = -.591, p<0.05) with identifying phishing stimuli in a Facebook phishing email; this indicates that participants who scored highly on this measure were less likely to identify phishing components on a bogus email. Participants with high ratings of cognitive instability also logged in more frequently on Facebook (r_s = .594, p<0.05) (see Figure 16). Additionally, cognitive instability was positively correlated with agreeableness (r_s = .536, p<0.05).

Another finding worth mentioning is a positive correlation between the impulsivity subscale of attention with neuroticism (r_s = .620, p<0.05).

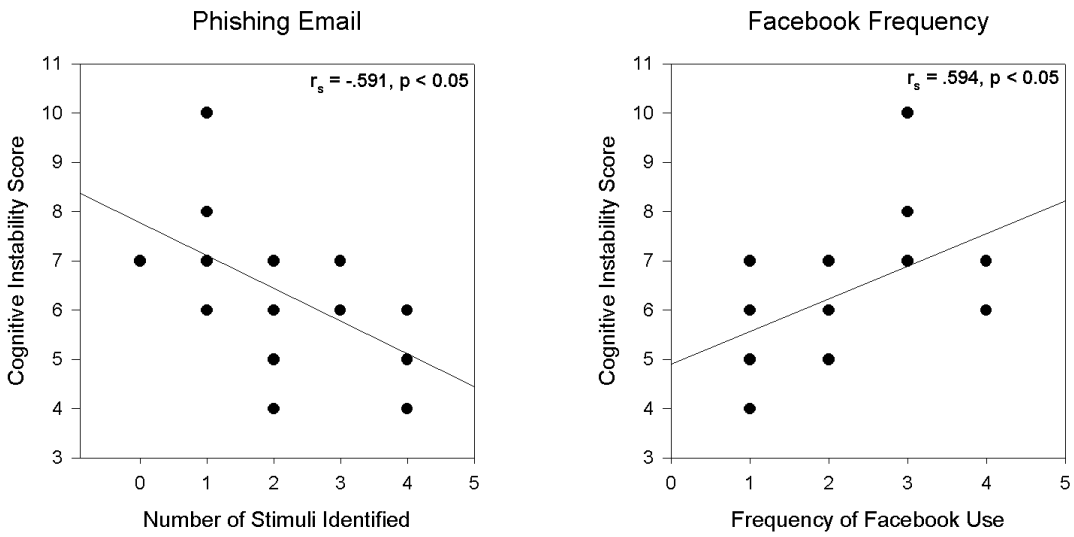


Figure 16. Cognitive instability correlations

Trust in Facebook

Correlations of trust in Facebook and screenshot ratings and stimuli count are listed in Table 8 in Appendix N. As can be seen in Figure 17, individuals who have higher trust in Facebook correctly identify phish more often than users who have lower trust in Facebook, although there were no significant correlation results. Conversely, there were no differences in low versus high trust ratings when incorrectly rating phish (see Figure 18).

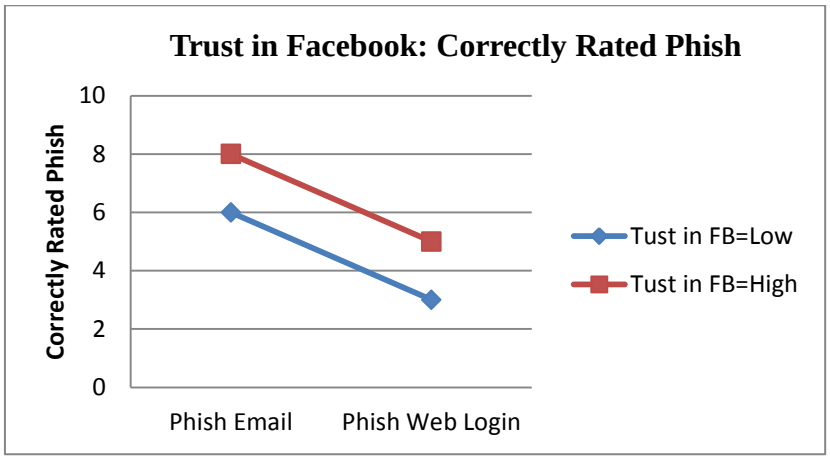


Figure 17. Trust in Facebook and correctly rated phish count

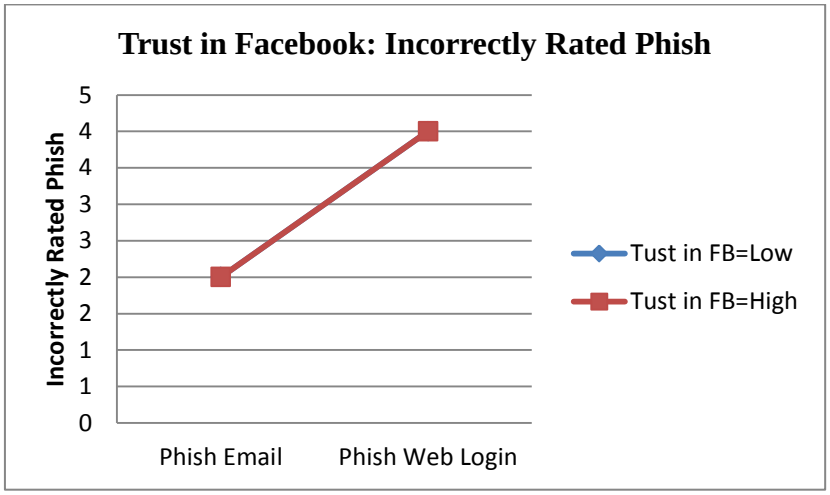


Figure 18. Trust in Facebook and incorrectly rated phish count

Those who had low trust in Facebook erroneously identified components on a real Facebook email page as phish; likewise, as trust in Facebook became stronger, the number of stimuli identified in the genuine email as phishing elements decreased (r_s =

-.640, p<0.01). Additionally, age was negatively correlated with trust in Facebook; younger participants were more likely to trust Facebook as an online company than older participants (r_s = -.546, p<0.05) (see Figure 19). Age had a mean value of 2.1053 and a standard deviation of 1.37011.

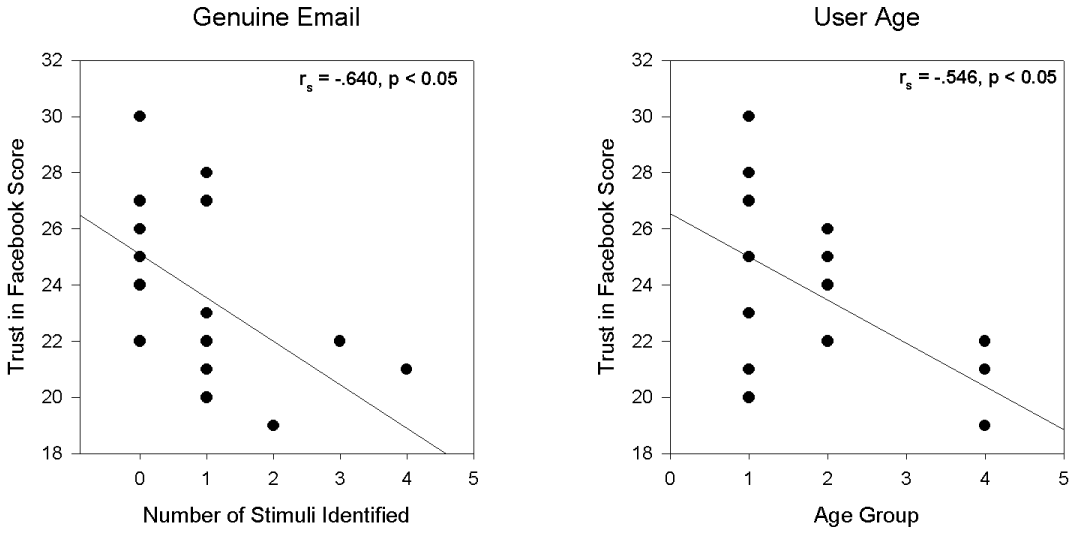


Figure 19. Trust in Facebook stimuli and age groups

Trust Factors

Ranking the genuine email as legitimate had a negative relationship with the number of components identified as phish on the same screenshot (r_s = -.583, p<0.01); this indicates that as the example was identified correctly as real, the participants actually indicated fewer elements that looked like phish.

There were eleven trust factors (present and missing) in the phishing email example and six in the web login screenshot. On average, users identified two stimuli for the phishing email and .58 for the phishing web login, which is represents an 18% and 10% successful stimuli identification rate respectively. Overall, for both phishing examples, 18% of stimuli were identified and 82% were unidentified (see Figure 20).

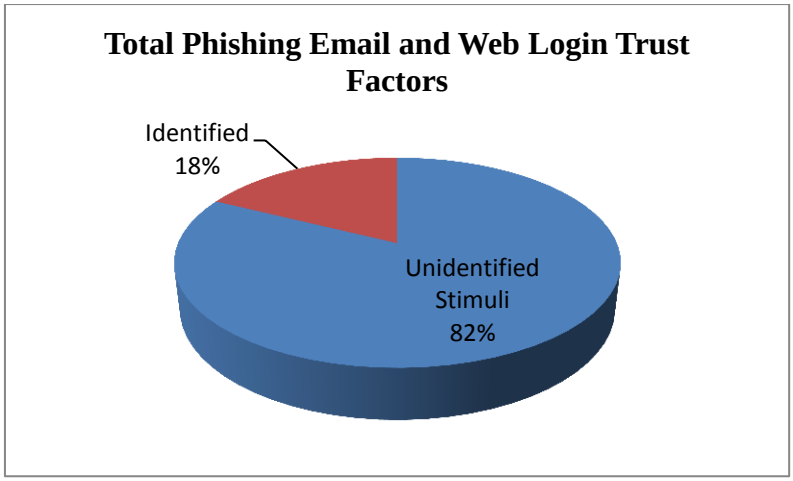


Figure 20. Phishing trust factor identification rate

Authenticity Ranking

There was a positive rank-order correlation coefficient between individuals who ranked the phish email as phish, and individuals who ranked the genuine email also as phish (r_s = .620, p<0.01). If participants thought the genuine screenshot was phish, they (incorrectly) identified more items that were convincing as phishing components (r_s = -.583, p<0.01). Individuals who ranked the genuine email as genuine received email notifications from Facebook (r_s = -.485, p<0.05). Email notifications from Facebook had a mean of 1.3889 and a standard deviation of .60768.

Participants' ability to correctly identify screenshots was similar under both conditions of phishing screenshots (49%) and genuine screenshots (51%). Incorrectly rated phishing screenshot rates represent 56% while authentic examples signify 44%. When combining the correct and incorrect ratings for phishing and genuine screenshot examples, there is a higher account of correct ratings, as illustrated in Figure 21.

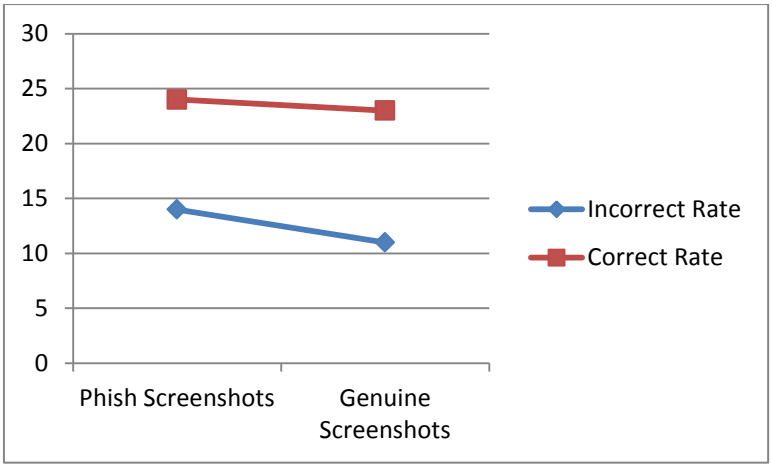


Figure 21. Screenshot ratings

Other Findings

Attention, a subscale of impulsivity, was positively correlated with neuroticism (r_s = -.497, p<0.05) and was negatively correlated with link and drop-down menu clicking during the experiment (r_s = -.497, p<0.05). The higher a participant scored in attention, the more the user tended to click the mouse. Clicking had a mean value of 1.8421, a standard deviation of .37463 and was scored reversely. Clicking rates represented 16% of the sample during the experiment, whereas 84% did not click at all.

Users who rated highly in openness visited Facebook most frequently (r_s = -.593, p<0.05). Facebook frequency had a mean value of 2.2105, a standard deviation of 1.13426 and was scored reversely. Users who rated highly in openness also used the mouse (however, not clicking) most often (r_s = -.492, p<0.05). Mouse usage had a mean value of 1.2105 and a standard deviation of .41885. Most participants moused at some stage in the experiment (79%), whereas 21% did not mouse at all.

Discussion

Results indicate there were some correlations between personality and a susceptibility to Facebook phishing. There were no significant results reported for conscientiousness and Facebook phishing vulnerabilities, although outcomes for cognitive instability and agreeableness contain insights into possible Facebook phishing susceptibility high-risk groups.

Analysis also indicates that users with high trust in Facebook correctly rate phish more often than users with low trust in Facebook; as trust in Facebook became stronger, the number of stimuli identified in the genuine email as phishing elements decreased; and younger participants trust Facebook as an online firm more than older participants do.

Research also found that users identified only 18% of all stimuli on combined phishing examples. Although there is a higher percentage of users who rate genuine examples correctly, 44% of participants rated the genuine email and web login falsely. Users who ranked the genuine email as genuine received email notifications from Facebook; this suggests that familiarity is a possible contributor for correctly identifying real Facebook emails.

Personality

Hypothesis 1 posited that participants who score highly in conscientiousness are less susceptible to Facebook phishing than participants who score lowly in conscientiousness. These results indicate that, in this sample and under these test conditions, this hypothesis was not fully supported.

Most of those who rated the website correctly scored highly on conscientiousness, which was marginally correlated. This indicates that participants with lower levels of conscientiousness may fail to identify the phishing web login correctly. When considering both elements of phishing examples, those who did not rate as highly in conscientiousness made more rating errors than participants who rated highly in conscientiousness.

Eighty-nine per cent of the participants correctly identified the email example as phish. When looking at personality trait correlations in this group, these individuals rated highly in openness and neuroticism. The participants who scored highly in

conscientiousness and lowly in agreeableness, also answered correctly. Participants with introversion (low extraversion) were more likely to rate the email inaccurately.

In the phishing website rating, 58% of participants answered incorrectly. In this group, individuals scored lowly on conscientiousness and highly on neuroticism. There were no significant correlations for conscientiousness and the phishing email or web login in terms of the number of stimuli identified.

There was a positive relationship with cognitive instability and agreeableness. The more agreeable a participant, the more likely the user would have a high level of cognitive instability. Those who rated highly in agreeableness were also most likely to inaccurately rate the genuine web login sample as phish. Additionally, high levels of agreeableness were positively related to Facebook login frequency; the more often a user logs in to Facebook, the more agreeable the user tends to be. This group may potentially be a high-risk group due to the inability to recognise a genuine website and a high log in rate.

There were no findings to support Ryan and Xenos (2011) and Gosling et al. (2011), who found that those who score highly on conscientiousness spend less time on Facebook. This difference in results possibly relates to sample; the study conducted by Ryan and Xenos had 1324 participants aging from 18-44 years, and the experiment performed by Gosling et al. had 159 participants studying psychology at university. The results of this research also did not support a previous observation of a lower rate of victimisation in those who score highly in conscientiousness (Jensen-Campbell & Malcolm, 2007). The non-correlated result in this case may possibly relate to the fact that the research performed by Jensen-Campbell and Malcolm was with adolescents and not adults.

Impulsivity

Hypothesis 2 purported participants who score highly in impulsivity are more susceptible to Facebook phishing than participants who score lowly in impulsivity. Based on the results presented in both ratings and the number of stimuli presented, this hypothesis is supported.

Participant impulsivity levels indicate that 35% of the users who have a high level of impulsivity correctly identified both examples of phish and 65% of users who have a

low level of impulsivity also answered correctly. Therefore, users who rate lowly in impulsivity correctly rate phish more that those who rate highly in impulsivity. Related with this finding, those who incorrectly rated phishing as genuine scored highly in impulsivity. To summarise, those users who score lowly in impulsivity are better at correctly rating phish and make fewer mistakes in rating a genuine example as phish.

Cognitive instability was negatively related with identifying phishing stimuli in a Facebook phishing email. This suggests that participants who scored highly in cognitive instability were less likely to identify phishing components on a fake email. Individuals in this group logged in more frequently on Facebook and were also positively correlated with agreeableness. This finding may indicate a high-risk group for Facebook phishing susceptibility.

Although Purvis (2011) indicated that impulsivity was an influencer in online attack, this study did not find that impulsivity generally supported this statement, but the impulsivity sub-scale cognitive instability did. While Barnard (2009) found that men who fell for Ponzi schemes had impulsive characteristics, there was no support in this research to indicate males fell for phish more than women did.

Trust in Facebook

Hypothesis 3 proposed that participants who score highly in trust in Facebook as an online company are more susceptible to Facebook phishing than participants who score lowly in trust in Facebook as an online company. Analysis indicates that users with high trust in Facebook correctly rate phish more often than users with low trust in Facebook and thus the hypothesis is not supported.

Based on count rate, individuals who have higher trust in Facebook correctly identify phish more often than users who have lower trust in Facebook, although there were no significant correlations to support this. Those who had low trust in Facebook erroneously identified components on a real Facebook email page as phish; likewise, as trust in Facebook became stronger, the number of stimuli identified in the genuine email as phishing elements decreased. Additionally, younger participants were more likely to trust Facebook as an online company than older participants were. Users who

had low trust in Facebook were most likely sceptical, thus incorrectly identifying phishing elements on the genuine email.

Existing literature suggests that Facebook is vulnerable to phishing attacks (Amin et al., 2010; Bonneau et al., 2009), uses complicates syntaxes (Bonneau et al., 2009) and facilitates an environment for trust to develop (Petre, 2010). It would appear these factors would aid phishing, however it is possible that users who trust Facebook are familiar with Facebook and recognize its genuine trust elements.

Trust Factors

Jakobsson et al. (2007) observed that users noticed missing components in a genuine screenshot and rated the example as not genuine; this observation was a basis for hypothesis 4, which maintained that users would not identify all trust factors (present or missing) in Facebook emails and websites. Based on result findings that users identified only 18% of all stimuli on combined phishing examples, hypothesis 4 is supported.

This study found that users identified 18% of all stimuli on combined phishing examples. On the web login screenshot (phish) where elements were missing, no user noticed their absence.

This study found that individuals who ranked the genuine email as legitimate noticed fewer phishing stimuli on same screenshot. This possibly indicates that a user who already thinks an example is real may spend less time looking for other elements which may be otherwise convincing; this is a confirmation bias, as identified by Plous (1993).

Some phish examples had genuine elements (such as footers and the ‘keep me logged in’ box which was ticked). However, participants recognised trust factors but none validated the cues by verifying links.

Some users identified phishing stimuli, but because the stimuli looked good, the users felt the stimuli were real; the good-looking phish stimuli reinforced their decision that it was indeed genuine (for example, the Facebook logo, which normally has a its own unique font, was replaced with Arial in the phishing email example). This is an example of salience, as explained by R. Miller and Grace (2002).

One user noticed the lack of the security lock in the address bar, probably because that participant has Secure Socket Layer (SSL), an encryption protocol setting offered to all Facebook users, enabled for his own Facebook account.

Participants had different analyses of trust factors. For example, if there were no spelling errors, users thought the example was authentic. In the (genuine) Facebook birthday email, there were no images displayed in the example, which is a common setting in email clients to block possible offensive images that may accompany spam. Although there was an "External Images are not displayed. Display Images" link at the top of the email body content to turn the images on, one user felt that because the images were not visible, the example must be phish.

Authenticity Ranking

Research from this study found that individuals ranked the genuine email as phish. Additionally, this study found that those who incorrectly ranked the genuine email as phish also correctly ranked the phish email as phish. When users rated the genuine email as phish, they (incorrectly) identified more items that were convincing as phishing components. Users who ranked the genuine email as genuine received email notifications from Facebook; this suggests that familiarity is a possible contributor for correctly identifying real Facebook emails.

Based on the findings of Jakobsson et al. (2007), who found that some users rank legitimate websites as phish, hypothesis 5 suggested that users would mistake authentic Facebook emails and web pages as phish. Although there is a higher percentage of users who rate genuine examples correctly, 44% of participants rated the genuine email and web login falsely; hence, the hypothesis is supported.

Other Findings

The most frequent users to visit Facebook were those users who rated highly in openness. These users also used the mouse the most often during the experiment (but not for clicking).

In the experiment, links were live and drop-down boxes were operable. It was found that the higher a participant scored in attention (impulsivity subscale), the more the user tended to click the links and boxes. Although 79% of the participants moused

and 16% clicked, no one actually hovered over a link to verify the link destination. Attention was also positively correlated with neuroticism.

Because the experiment was conducted on a laptop, two screens (genuine email and phishing web login) needed scrolling in order to see all elements properly. Participants who did not scroll (21%), made their authenticity decisions on those screenshots without checking what was at the bottom of the example.

There were two minor technical issues involving the two phishing examples. In the phishing email example there was a link that was not visually, or technically, complete and was overlooked during the pilot experiments. Normally, text that is hyperlinked to a destination is underlined; in this case, the email timestamp, 21:43, was partially underlined. Two participants noticed this during the experiment; one individual rated the phishing as phish and the other rated it as probably not phish. The second technical issue involved an image on the web login example (phish). If the laptop browser had not cached facebook.com, the Facebook map image located on this screen was not present for the experiment. This affected four participants before the problem was rectified. Each user verbalised that something was missing, but three users still rated the example incorrectly as a genuine login page.

Limitations

The most obvious limitation of this study is the sample size. Although there was a wide age range (18-60), there were only 19 participants, and none representing the 36-42 year age group. Additionally, 63% were females and 37% were males, which does not represent balanced gender results. Participants were recruited by convenience sampling, which has biases for truly representing a cross section of societal groups.

Because the experiment was conducted on a one to one basis and the researcher was present, there was the probably influence of the Hawthorne effect (Landsberger, 1958). Users were asked to make any comments in relation to the study and several stated that they would not normally take such care in their observations and decisions relating to Facebook emails and web login pages. Another area, which may have had some influence from the researcher, concerned the mouse; some users may have hesitated in using the mouse even though they were told they could do so from the

start. Most participants who did mouse did not start using the mouse until half way through the screenshots.

The questionnaires were provided in paper form and the layout design was not optimal; three users mistakenly provided two answers on one line and none on another. The results for those scales were considered invalid and could not be included in the results.

The appearance of email examples may have affected user rating and stimuli responses due to formatting differences between email clients. In other words, a user who is used to seeing his Facebook emails using a particular email client (such as MS Office, Thunderbird or Gmail), way may be fooled into thinking the Facebook email examples were phish just because they looked different to what is normally seen.

Lastly, some participants use Facebook on their mobile handsets as the only method for accessing Facebook and are not familiar with the email and web login layouts on a laptop. The participants' answers may have been based on a cognitive bias, representativeness heuristic, where a decision is made based on information in memory (Tversky & Kahneman, 1974)

Implications

Outcomes for cognitive instability and agreeableness draw attention to possible Facebook phishing susceptibility high-risk groups. The biggest downfall for user susceptibility to phish may be users' inability to authenticate relevant information; most participants in this study never checked the URL on the web login pages and none checked link destinations by hovering.

Users who received email notifications from Facebook were the most likely to correctly identify Facebook emails. Perhaps familiarity by repeatedly seeing genuine correspondence is the key to developing awareness for Facebook emails.

In the researcher's field notes, participant comments for phish examples included, "looks authentic, looks real, everything looks right", which supports the theory of salience (R. Miller & Grace, 2002).

Future Research

It may be beneficial for future research to examine the way in which mobile users may be vulnerable to Facebook phish, especially since there are not as many verification methods (such as link hovering) to determine an email or web login authenticity. There is a need for research to examine who is susceptible to phishing *within* Facebook. Some phishing occurs via third party applications (such as games) and often spread to other account users. It is also possible that Facebook ads may be phishing lures, and studies into who clicks on Facebook ads would be advantageous to discovering possible individual vulnerabilities. Research would also be beneficial in the area of Facebook phishing victimisation, to supplement the studies conducted by Sharp et al. (2004). Lastly, research around Facebook phishing and cognitive load (G. Miller, 1956) may provide interesting results.

Conclusion

This study concentrated on the correlation between phishing and Facebook users' personality traits. Firstly, participants completed questionnaires measuring conscientiousness, impulsivity and trust in online firms; secondly, users were asked to rate the legitimacy of Facebook email and web login page stimuli where some samples were genuine and others were phish. The findings indicate individuals who scored highly in cognitive instability, a subscale of impulsivity, login more frequently and identified fewer phishing stimuli than those who score lowly in cognitive instability. Additionally, those who rated highly in agreeableness were also most likely to inaccurately rate the genuine web login sample as phish and login to Facebook frequently. These results suggest that individuals who score highly in cognitive instability and agreeableness may potentially be within a high-risk group of Facebook Phishing susceptibility. Additional findings indicate that not all users identify all trust factors (present or missing) in Facebook emails and web sites; and individuals may mistake authentic Facebook emails and web pages as phish.

References

Amichai-Hamburger, Y., & Vinitzky, G. (2010). Social Network Use and Personality. *Computers in Human Behavior*, *26*(6), 1289-1295.

Amichai-Hamburger, Y., Wainapel, G., & Fox, S. (2002). "On the Internet No One Knows I'm an Introvert": Extroversion, Neuroticism, and Internet Interaction. *CyberPsychology & Behavior*, *5*(2), 125-128. doi:10.1089/109493102753770507

Amin, T., Okhiria, O., Lu, L., & An, J. (2010). Facebook: A Comprehensive Analysis of Phishing on a Social System. *Retrieved March*, *10*.

Anandpara, V., Dingman, A., Jakobsson, M., Liu, D., & Roinestad, H. (2007). Phishing IQ Tests Measure Fear, Not Ability. *Proceedings from FC'07/USEC'07: 11th International Conference on Financial Cryptography and 1st International Conference on Usable Security* (pp. 362-366). Berlin, Heidelberg.

Anti-Phishing Work Group. (2011). *Phishing Activity Trends Report, First Half 2011* (p. 11). Retrieved from http://www.antiphishing.org/reports/apwg_trends_report_h1_2011.pdf

Anti-Phishing Work Group. (2012). APWG: Origins of the Word "Phishing." Retrieved January 19, 2012, from http://www.antiphishing.org/word_phish.html

Barnard, J. (2009). Why Men Fall Prey to Ponzi Schemes. *Conference Papers - Law & Society*, 1.

Bergholz, A., De_Beer, J., Glahn, S., Moens, M., Paaß, G., & Strobel, S. (2010). New Filtering Approaches for Phishing Email. *Journal of Computer Security*, *18*, 7-35.

Bhattacherjee, A. (2002). Individual Trust in Online Firms: Scale Development and Initial Test. *Journal of Management Information Systems*, *19*(1), 211-241. doi:Article

Bonneau, J., Anderson, J., & Danezis, G. (2009). xProceedings from: 2009 International Conference on Advances in Social Network Analysis and Mining (pp. 249-254).

Chandrasekaran, M., Narayanan, K., & Upadhyaya, S. (2006). Phishing Email Detection Based on Structural Properties. *Proceedings of the NYS Cyber Security Conference,*. New York.

Cialdini, R. (1993). *Influence : The Psychology of Persuasion* (Rev. ed.). New York: Morrow.

Correa, T., Hinsley, A. W., & de Zúñiga, H. G. (2010). Who Interacts on the Web?: The Intersection of Users' Personality and Social Media Use. *Computers in Human Behavior*, *26*(2), 247-253.

Costa, P., & McCrae, R. R. (1992). *Revised Neo PI-R: Professional Manual*. Odessa, FL: Psychological Assessment Resources.

Dhamija, R., Tygar, J., & Hearst, M. (2006). Why Phishing Works. *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*. Montreal, Canada: ACM Press. doi:10.1145/1124772.1124861

Downs, J., Holbrook, M., & Cranor, L. (2006). Decision Strategies and Susceptibility to Phishing. *Proceedings of the Second Symposium on Usable Privacy and Security* (Vol. 149, pp. 79-90). Presented at the SOUPS '06, Pennsylvania: ACM Press.

EMC Corporation. (2012). *The Year in Phishing*. Retrieved from http://www.rsa.com/solutions/consumer_authentication/intelreport/11635_Online_Fraud_report_0112.pdf

Evenden, J. L. (1999). Varieties of Impulsivity. *Psychopharmacology*, *146*(4), 348.

Facebook. (2012). Notifications - Facebook Help Centre. Retrieved February 5, 2012, from http://www.facebook.com/help/?faq=154884887910599&ref_query=ema

Feigelson, J., & Calman, C. (2010). Liability for the Costs of Phishing and Information Theft. *Journal of Internet Law*, *13*, 1-26.

Festinger, L. (1957). *A Theory of Cognitive Dissonance*. Stanford University Press.

Geier, E. (2011). 2012 in Security: Rising Danger. *PC World*, *29*(12), 35-36.

Glaeser, E. L., Laibson, D. I., Scheinkman, J. A., & Soutter, C. L. (2000). Measuring Trust. *Quarterly Journal of Economics*, *115*(3), 811-846. doi:10.1162/003355300554926

Gosling, S. D., Augustine, A. A., Vazire, S., Holtzman, N., & Gaddis, S. (2011). Manifestations of Personality in Online Social Networks: Self-Reported Facebook-Related Behaviors and Observable Profile Information. *CyberPsychology, Behavior & Social Networking*, *14*(9), 483-488.

Guadagno, R. E., Okdie, B. M., & Eno, C. A. (2008). Who Blogs? Personality Predictors of Blogging. *Computers in Human Behavior*, *24*(5), 1993-2004. doi:10.1016/j.chb.2007.09.001

Harris, M. J. (2009). *Bullying, Rejection, and Ppeer Victimization a Social Cognitive Neuroscience Perspective*. New York: Springer.

Holt, T., & Graves, D. (2007). A Qualitative Analysis of Advance Fee Fraud E-Mail Schemes. *International Journal of Cyber Criminology*, *1*, 137-154.

IRS. (2012). Phishing and Other Schemes Using the IRS Name. Retrieved February 3, 2012, from http://www.irs.gov/newsroom/article/0,,id=214917,00.html

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social Phishing. *Communications of the ACM*, *50*(10), 94-100.

Jakobsson, M., Tsow, A., Shah, A., Blevis, E., & Lim, Y. (2007). What Instills Trust? A Qualitative Study of Phishing. *Proceedings from FC'07/USEC'07: 11th International Conference on Financial Cryptography and 1st International Conference on Usable Security* (pp. 356-361). Berlin, Heidelberg.

Jensen-Campbell, L. A., & Malcolm, K. T. (2007). The Importance of Conscientiousness in Adolescent Interpersonal Relationships. *Personality and Social Psychology Bulletin*, *33*(3), 368-383. doi:10.1177/0146167206296104

Jewkes, Y., & Yar, M. (2010). *Handbook of Internet Crime*. Cullompton: Willan.

John, O. P., & Srivastava, S. (1999). The Big Five Trait Taxonomy: History, Measurement, and Theoretical Perspectives. In L. A. Pervin & O. P. John (Eds.),

Handbook of personality: Theory and research (2nd ed.). (pp. 102-138). New York, NY US: Guilford Press.

Kirwan, G., & Power, A. (2011). *The Psychology of Cyber Crime : Concepts and Principles*. Hershey PA: Information Science Reference.

Krebs, B. (2009). Spike in Social Media Malware, Phishing Attacks. *Retrieved March*. Retrieved from http://voices.washingtonpost.com/securityfix/2009/11/spike_in_social_media_malware.html

Landsberger, H. (1958). *Hawthorne Revisited: Management and the Worker, its Critics, and Developments in Human Relations in Industry*. Ithaca, New York: Cornell University.

McCrae, R. R., & John, O. P. (1992). An Introduction to the Five-Factor Model and its Applications. *Journal of Personality*, *60*(2), 175-215.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and Validating Trust Measures for e-Commerce: An Integrative Typology. *Information Systems Research*, *13*(3), 334-359.

Miller, G. (1956). The Magical Number Seven Plus or Minus Two: Some Llimits on our Capacity for Processing Iinformation. *Psychological Review*, *63*(2), 81-97.

Miller, R., & Grace, R. (2002). Conditioning and Learning. In A. F. Healy (Ed.), *Handbook of Psychology, Volume 4, Experimental Psychology* (Vol. 4, pp. 357-398). Hoboken, NJ: John Wiley & Sons. Retrieved from http://public.eblib.com/EBLPublic/PublicView.do?ptiID=151323userid=^u

Ngo, F., & Paternoster, R. (2011). Cybercrime Victimization: An Examination of Individual and Situational Level Factors. *International Journal of Cyber Criminology*, *5*(1), 773-793.

Nykodym, N., Kahle-Piasecki, L., Ariss, S., & Toussaint, T. (2010). Cybercrime and Business: How to not Get Caught by the Online Phisherman. *Journal of International Commercial Law and Technology*, *5*, 252-259.

Parrish, J., Bailey, J., & Courtney, J. (2009). A Personality Based Model for Determining Susceptibility to Phishing Attacks. *2009 Southwest Decision Sciences Institute Proceedings*. Oklahoma.

Patton, J. H., Stanford, M. S., & Barratt, E. S. (1995). Factor structure of the Barratt Impulsiveness Scale. *Journal of Clinical Psychology*, *51*(6), 768-774. doi:10.1002/1097-4679(199511)51:6<768::AID-JCLP2270510607>3.0.CO;2-1

Petre, G. (2010). Facebook: Another Breach in the Wall. Presented at the MIT Spam Conference of 2010, Cambridge, MA. Retrieved from http://labs.bitdefender.com/wp-content/uploads/2011/03/FB-Another-breach-in-the-wall.pdf

Plous, S. (1993). *The Psychology of Judgment and Decision Making*. New York: McGraw-Hill.

Purvis, L. (2011). Online Vulnerability: Identifying Characteristics for Victim Profiling. Presented at the Teesside Digital Forensics Conference 2011, Middlesbrough, UK. Retrieved from http://tdfcon.org.uk/conference_papers.php

Reuters. (2011). Regulators Pressure Banks After Citi Data breach. Retrieved February 3, 2012, from http://www.reuters.com/article/2011/06/09/us-citi-idUSTRE7580TM20110609

Roethlisberger, F. J., & Dickson, W. J. (1934). *Studies in Industrial Research: Technical vs. Social Organization in an Industrial Plant*. Oxford England: Harvard Univ., Graduate School of B.

Ross, C., Orr, E. S., Sisic, M., Arseneault, J. M., Simmering, M. G., & Orr, R. R. (2009). Personality and Motivations Associated with Facebook Use. *Computers in Human Behavior*, *25*(2), 578-586.

Ryan, T., & Xenos, S. (2011). Who Uses Facebook? An Investigation into the Relationship Between the Big Five, Shyness, Narcissism, Loneliness, and Facebook Usage. *Computers in Human Behavior*, *27*(5), 1658-1664.

Sharp, T., Shreve-Neiger, A., Fremouw, W., Kane, J., & Hutton, S. (2004). Exploring the Psychological and Somatic Impact of Identity Theft. *Journal of Forensic Sciences*, *49*(1), 131-136.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., & Downs, J. (2010). Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. *Proceedings of the 28th International Conference on Human Factors in Computing Systems*. Georgia: ACM Press.

Simon, W. L., & Mitnick, K. D. (2002). *The Art of Deception : Controlling the Human Element of Security*. Indianapolis, Ind.: Wiley.

Soghoian, C., & Jakobsson, M. (2009). Social Engineering in Phishing. *Information Assurance, Security and Privacy Services*. Bingley, UK: Emerald.

Symantec. (2012a). *Symantec Intelligence Report: February 2012*. Retrieved from http://www.symantec.com/content/en/us/enterprise/other_resources/b-intelligence_report_02_2012.en-us.pdf

Symantec. (2012b). *Symantec Intelligence Report: November 2011*. Retrieved from http://www.symantec.com/content/en/us/enterprise/other_resources/b-intelligence_report_11-2011.en-us.pdf

Tosun, L. P., & Lajunen, T. (2010). Does Internet use reflect your personality? Relationship between Eysenck's personality dimensions and Internet use. *Computers in Human Behavior*, *26*(2), 162-167.

Tversky, A., & Kahneman, D. (1974). Judgment Under Uncertainty: Heuristics and Biases. *Science*, *185*(4157), 1124-1131. doi:10.1126/science.185.4157.1124

US Federal Trade Commission. (2011). Consumer Sentinel Network Data Book for January - December 2010. Retrieved from http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2010.pdf

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why Do People get Phished? Testing Individual Differences in Phishing Vulnerability within an Integrated, Information Processing Model. *Decision Support Systems*, *51*(3), 576-586. doi:10.1016/j.dss.2011.03.002

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 & Technology*, *59*(4), 662-674.

Wright, R., Chakraborty, S., Basoglu, A., & Marett, K. (2010). Where Did They Go Right? Understanding the Deception in Phishing Communications. *Group Decision & Negotiation*, *19*(4), 391-416. doi:10.1007/s10726-009-9167-9

Wright, R., & Marett, K. (2010). The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived. *Journal of Information Management Systems*, *27*, 273-303.

Appendix A Descriptives

Facebook Phishing Participant #____

Please answer the following questions about yourself.

1. In which age group do you belong?

- ○ 18-26
- ○ 27-35
- ○ 36-42
- ○ 43-51
- ○ 52-60
- ○ 60+

2. Are you male or female?

- ○ Male
- ○ Female

3. How often do you visit Facebook?

- ○ Several times a day
- ○ Twice a day
- ○ Daily
- ○ Weekly
- ○ Bi-weekly
- ○ Hardly ever

Facebook Phishing Participant #____

4. Approximately how long do you spend on Facebook each time you visit the site?

- ○ Up to 15 minutes
- ○ Between 15 minutes and half an hour
- ○ Between 30 minutes and one hour
- ○ Between 1 and 2 hours
- ○ Between 2 and 5 hours
- ○ More than 5 hours

5. Do you receive email notifications from Facebook?

- ○ Yes
- ○ No
- ○ Not sure

6. In your opinion, are emails more trusting when they appear to come from a known person?

- ○ Yes
- ○ No
- ○ Not sure

Appendix B Big Five Inventory Scale 44

(John & Srivastava, 1999)

Facebook Phishing Participant #____

Here are a number of characteristics that may or may not apply to you. For example, do you agree that you are someone who likes to spend time with others? Please tick a box next to each statement to indicate the extent to which you agree or disagree with that statement.

I see myself as someone who...

		Disagree strongly	Disagree	Neither agree nor disagree	Agree	Agree strongly
1	Is talkative					
2	Tends to find fault with others					
3	Does a thorough job					
4	Is depressed, blue					
5	Is original, comes up with new ideas					
6	Is reserved					
7	Is helpful and unselfish with others					
8	Can be somewhat careless					
9	Is relaxed, handles stress well					
10	Is curious about many different things					
11	Is full of energy					
12	Starts quarrels with others					
13	Is a reliable worker					
14	Can be tense					
15	Is ingenious, a deep thinker					
16	Generates a lot of enthusiasm					
17	Has a forgiving nature					
18	Tends to be disorganized					
19	Worries a lot					
20	Has an active imagination					
21	Tends to be quiet					
22	Is generally trusting					
23	Tends to be lazy					
24	Is emotionally stable, not easily upset					
25	Is inventive					
26	Has an assertive personality					
27	Can be cold and aloof					
28	Perseveres until the task is finished					
29	Can be moody					

Facebook Phishing Participant #____

		Disagree strongly	Disagree	Neither agree nor disagree	Agree	Agree strongly
30	Values artistic, aesthetic experiences					
31	Is sometimes shy, inhibited					
32	Is considerate and kind to almost everyone					
33	Does things efficiently					
34	Remains calm in tense situations					
35	Prefers work that is routine					
36	Is outgoing, sociable					
37	Is sometimes rude to others					
38	Makes plans and follows through with them					
39	Gets nervous easily					
40	Likes to reflect, play with ideas					
41	Has few artistic interests					
42	Likes to cooperate with others					
43	Is easily distracted					
44	Is sophisticated in art, music, or literature					

Appendix C Barratt Impulsiveness Scale (BIS-11)

(Patton et al., 1995)

Facebook Phishing Participant #____

People differ in the ways they act and think in different situations. This is a test to measure some of the ways in which you act and think. Please tick a box next to each statement to indicate the extent to which you agree or disagree with that statement. Do not spend too much time on any statement. Answer quickly and honestly.

		Rarely/Never	Occasionally	Often	Almost always /Always
1	I plan tasks carefully.				
2	I do things without thinking.				
3	I make-up my mind quickly.				
4	I am happy-go-lucky.				
5	I don't "pay attention."				
6	I have "racing" thoughts.				
7	I plan trips well ahead of time.				
8	I am self-controlled.				
9	I concentrate easily.				
10	I save regularly.				
11	I "squirm" at plays or lectures.				
12	I am a careful thinker.				
13	I plan for job security.				
14	I say things without thinking.				
15	I like to think about complex problems.				
16	I change jobs.				
17	I act "on impulse."				
18	I get easily bored when solving thought problems.				
19	I act on the spur of the moment.				
20	I am a steady thinker.				
21	I change residences.				
22	I buy things on impulse.				
23	I can only think about one thing at a time.				
24	I change hobbies.				
25	I spend or charge more than I earn.				
26	I often have extraneous thoughts when thinking.				
27	I am more interested in the present than the future.				
28	I am restless at the theatre or lectures.				
29	I like puzzles.				
30	I am future oriented.				

Appendix D Individual Trust in Online Firms Scale

(Bhattacherjee, 2002)

Facebook Phishing Participant #____

The following questions relate to your views on Facebook as an online company. Please tick a box next to each statement to indicate the extent to which you agree or disagree with that statement.

		Disagree strongly	Disagree	Neither agree nor disagree	Agree	Agree strongly
1	Facebook has the skills and expertise to perform interactions in an expected manner.					
2	Facebook has access to the information needed to handle interactions appropriately.					
3	Facebook has the ability to meet most customer needs.					
4	Facebook is fair in its conduct with customer interactions.					
5	Facebook is fair in its use of private user data collected during an interaction.					
6	Facebook is fair in its customer service policies following an interaction.					
7	Facebook is open and receptive to customer needs.					
8	Facebook keeps its customers' best interest in mind during most interactions.					
9	Facebook makes good-faith efforts to address most customer concerns.					
10	Overall, Facebook is trustworthy.					

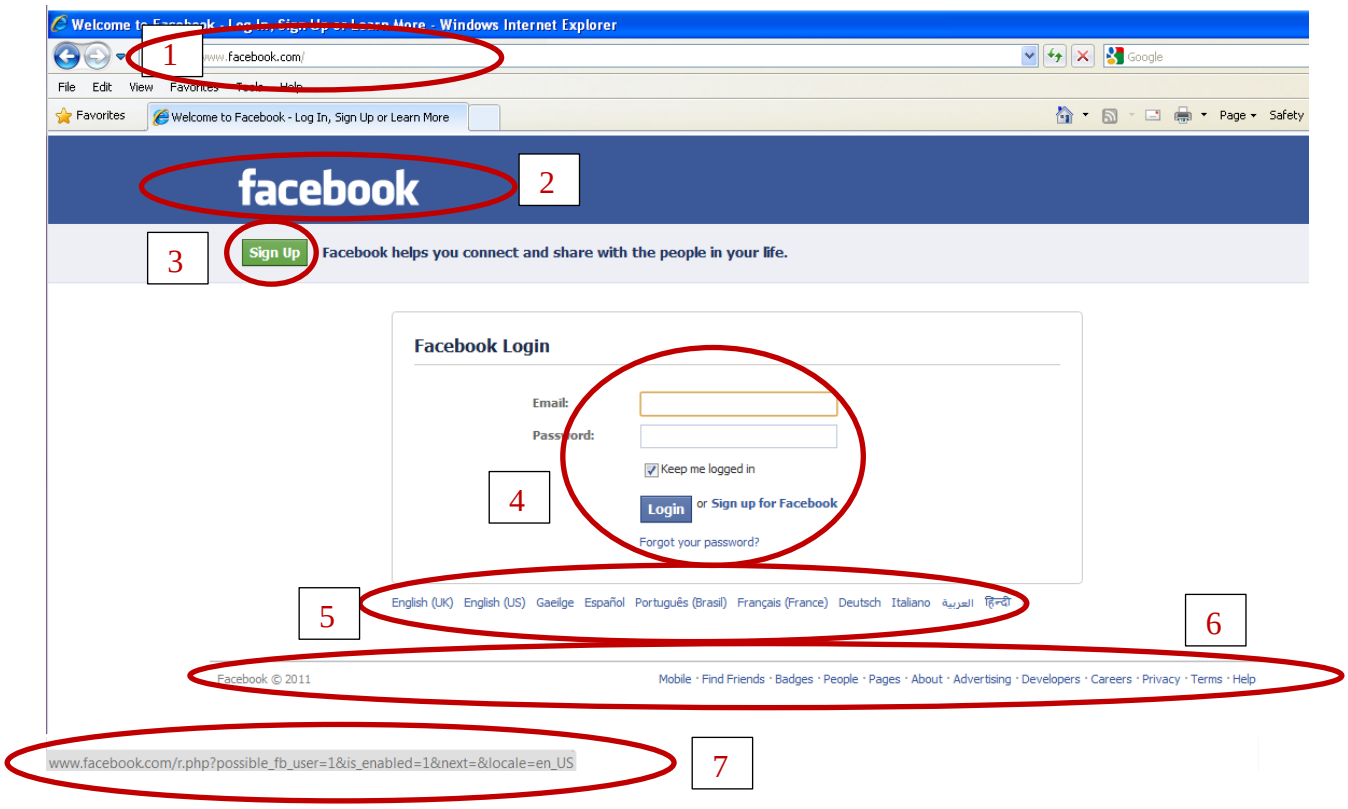
Appendix E Stimuli Authenticity

Screenshot 1: Phishing Email Stimuli Authenticity

This Facebook email example is phish for the following reasons:

- The email sender name has a curious ‘dash’ added, which is not standard in Facebook (1 and 7).
- Email address does not contain facebook.com or facebookmail.com as part of the email address (2).
- The subject line text (3) does not match the body content (6).
- Logo is not correct font (4) or link (11).
- Greeting – the Facebook username is always used, not the email prefix (5).
- It is rare for someone to have 4318 friends (8).
- The Facebook account holder (Sheila Garvey) does not have a picture (10).
- “Join Facebook” link (9) leads to bogus site (11).

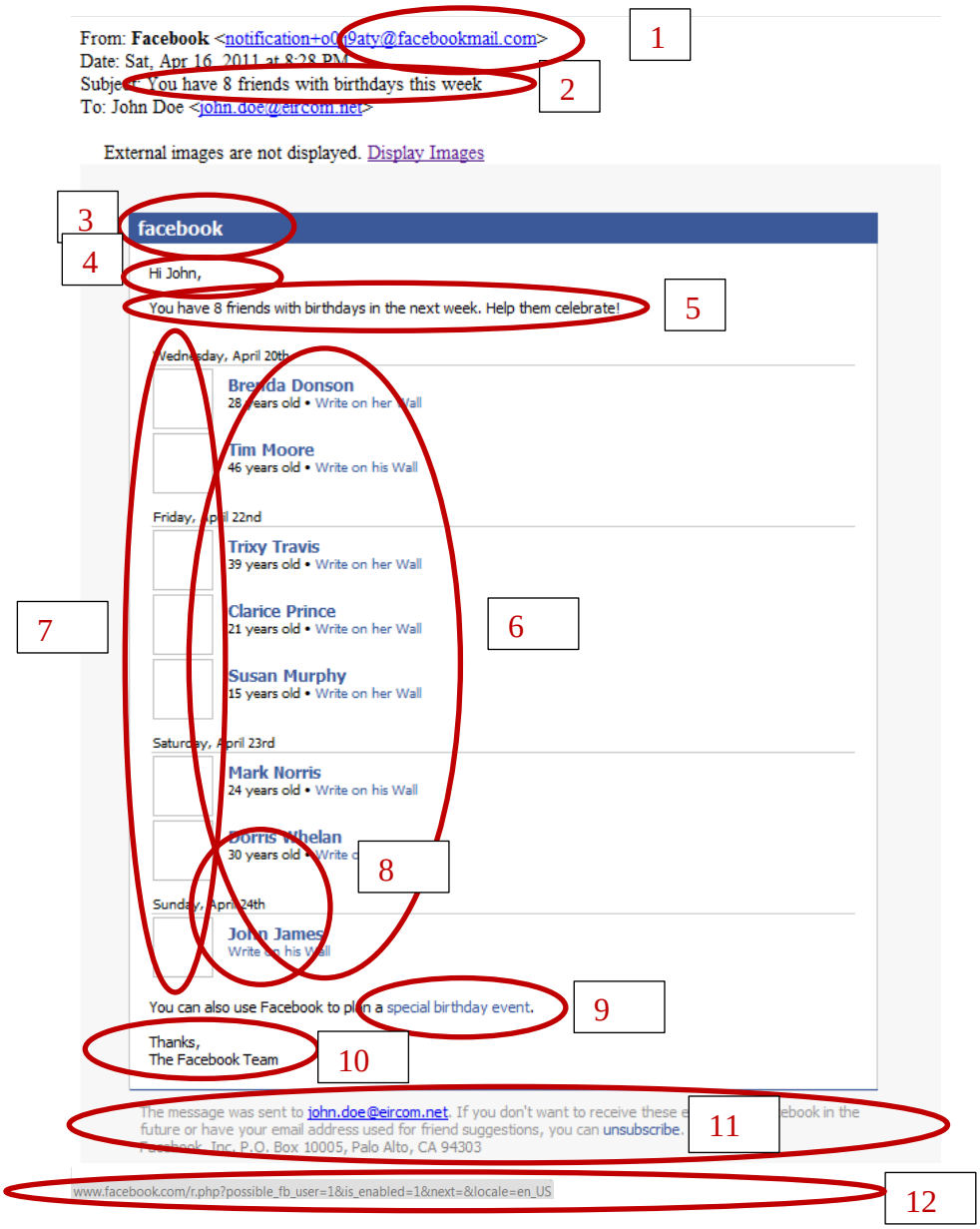
Screenshot 2: Genuine Web Login Stimuli Authenticity



This web login site is legitimate for the following reasons:

- URL is valid (1).
- The Facebook logo (2) is genuine with the unique font and link (7).
- All links (3 and 4) point to Facebook.com (7).
- Language selection (5) is present with valid links (7).
- Footer (6) is present with copyright and authentic links (7).

Screenshot 3 Genuine Email Stimuli Authenticity

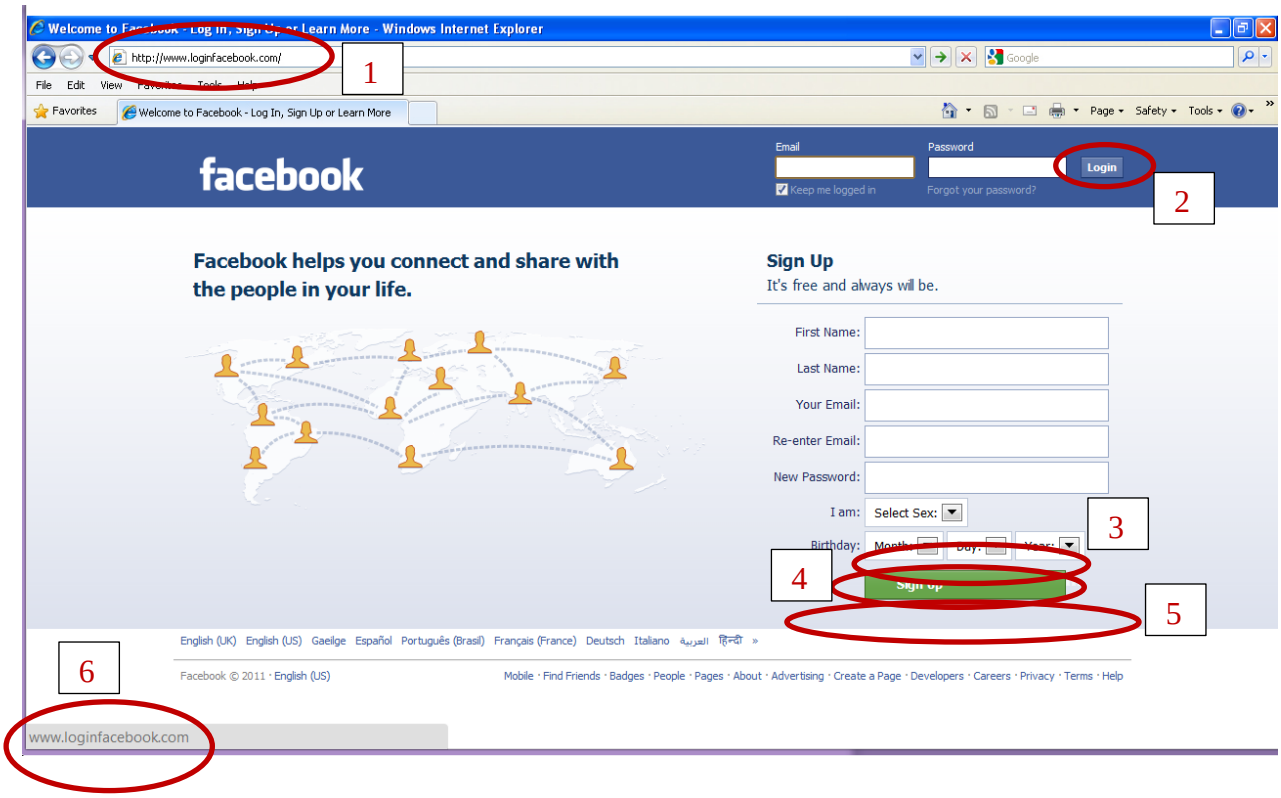


This web login site is legitimate for the following reasons:

- Email origin (1) and link (12) point to either facebookmail.com or facebook.com – both standard and authentic links.
- The subject line (2) and body content (5) match.
- The Facebook logo (3) is genuine with the unique font.
- The greeting (4) uses the user's name and not an email address.
- All birthday links (6) point to facebook.com in url bar (12).
- Although images are not displayed (7), links point to facebook.com (12).

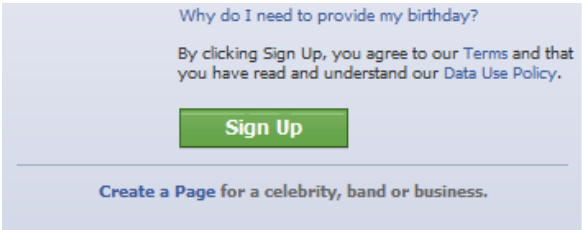
- The discrepancy between age display (8) is acceptable (based on privacy settings).
- A special birthday event (9) is always present and points to facebook.com (12).
- Birthday emails are always signed by the Facebook Team (10).
- The footer is present (11) with customary email unsubscribe detail.

Screenshot 3 Phish Web Login Stimuli Authenticity



This stimulus is phish for the following reasons:

- Wrong URL format (1).
- Login link (2) leads to bogus site (6)
- Why do I need my birthday (3) and Create a Page (5) are not present

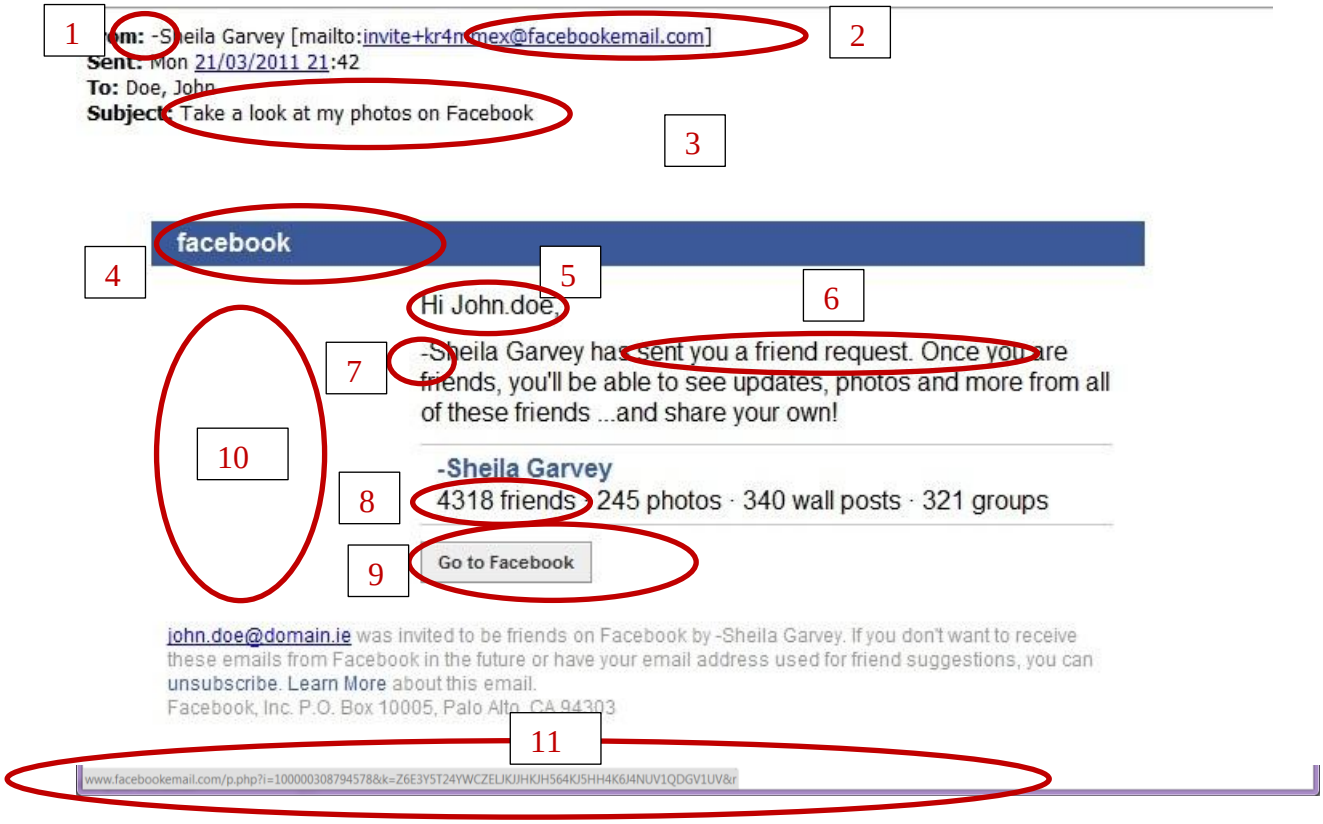


- Sign Up link (4) leads to bogus site (6)

Appendix F Rating and Stimuli Identification Sheet

Screenshot 1: Phishing email

Tick beside each stimuli as each is noticed verbally or by mouse movement.



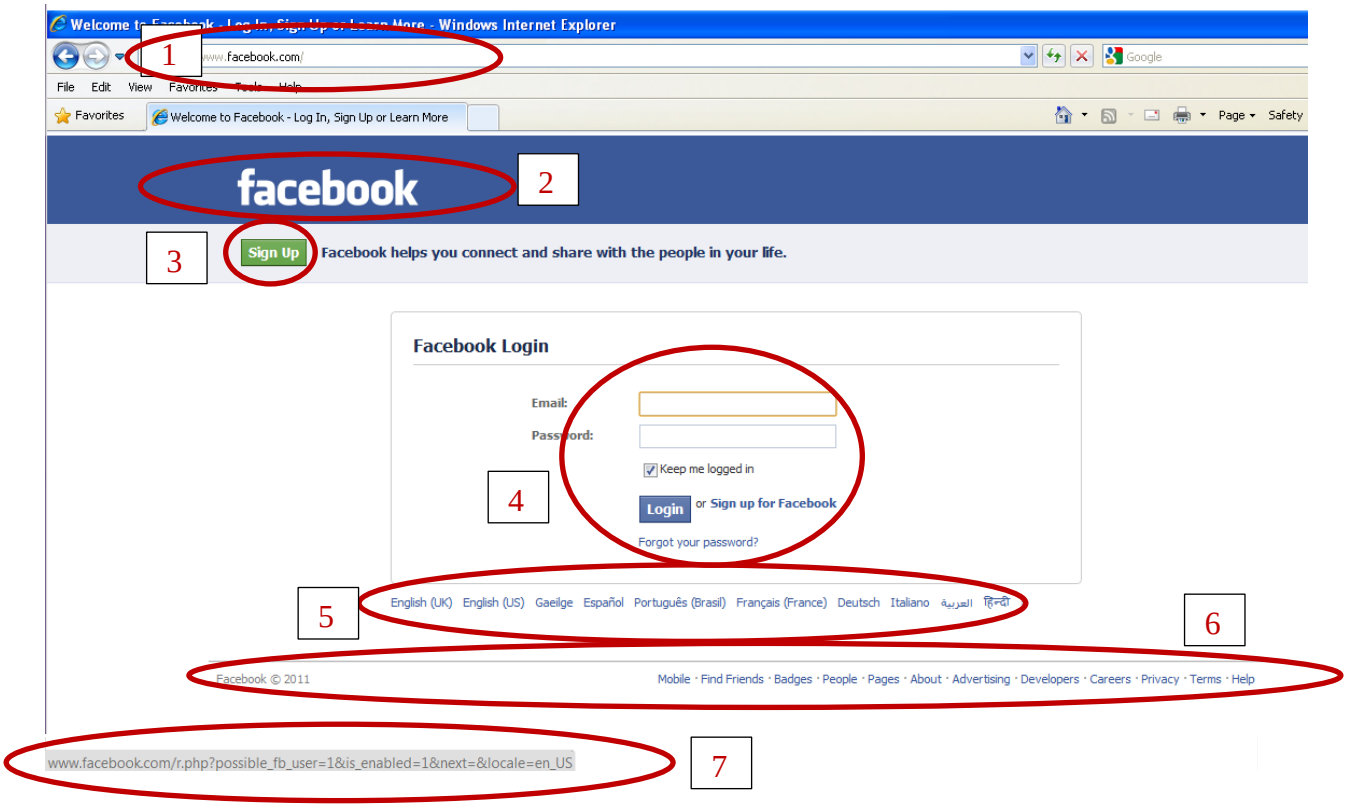
1. How do you rate this sample as a phishing email?

- ○ Certainly phishing
- ○ Probably phishing
- ○ Don't know
- ○ Probably not phishing
- ○ Certainly not phishing

2. What features inspired confidence or generated suspicion in authenticity?

Screenshot 2: Genuine login

Tick beside each stimuli as each is noticed verbally or by mouse movement.



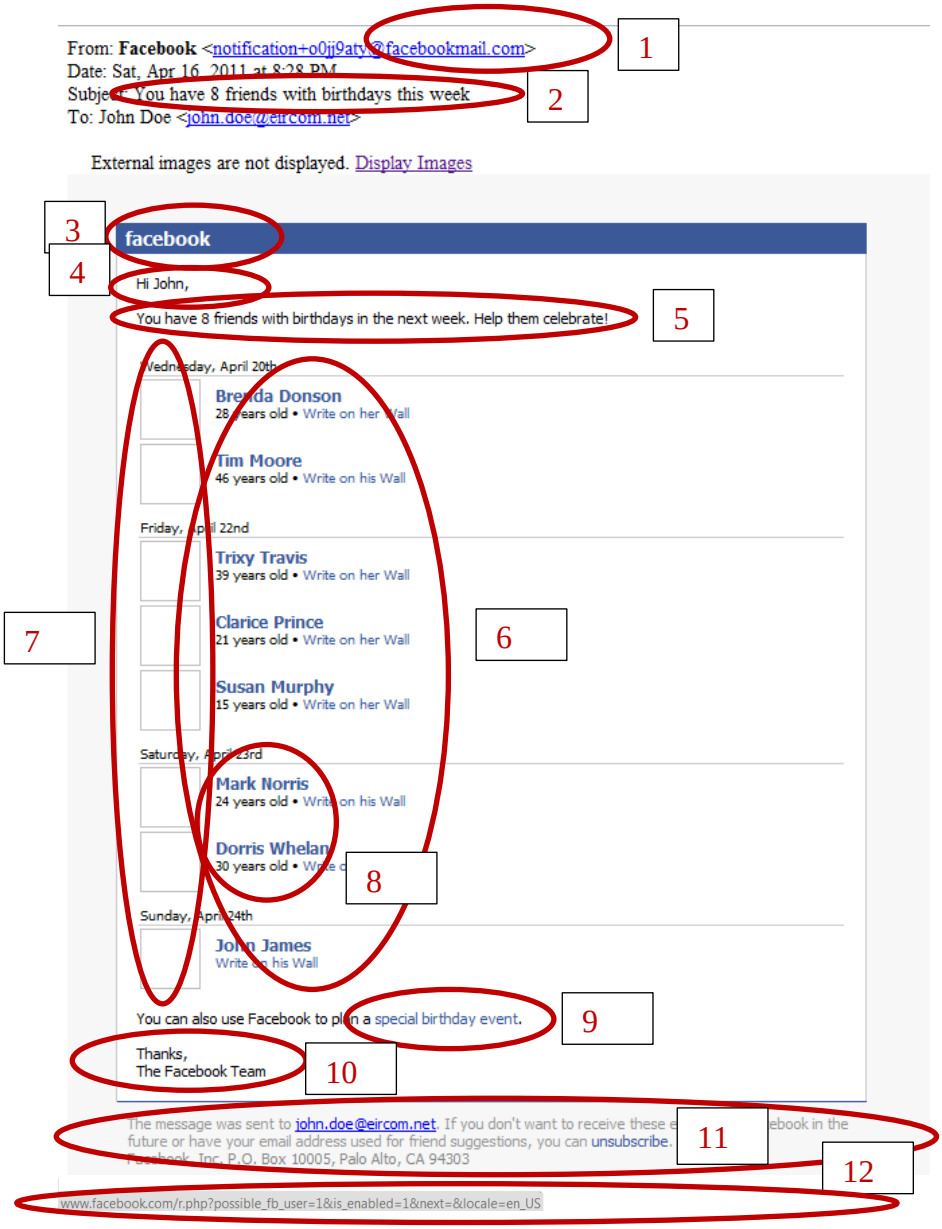
3. How do you rate this sample as a phishing webpage?

- ○ Certainly phishing
- ○ Probably phishing
- ○ No opinion
- ○ Probably not phishing
- ○ Certainly not phishing

4. What features inspired confidence or generated suspicion in authenticity?

Screenshot 3 Genuine email

Tick beside each stimuli as each is noticed verbally or by mouse movement.



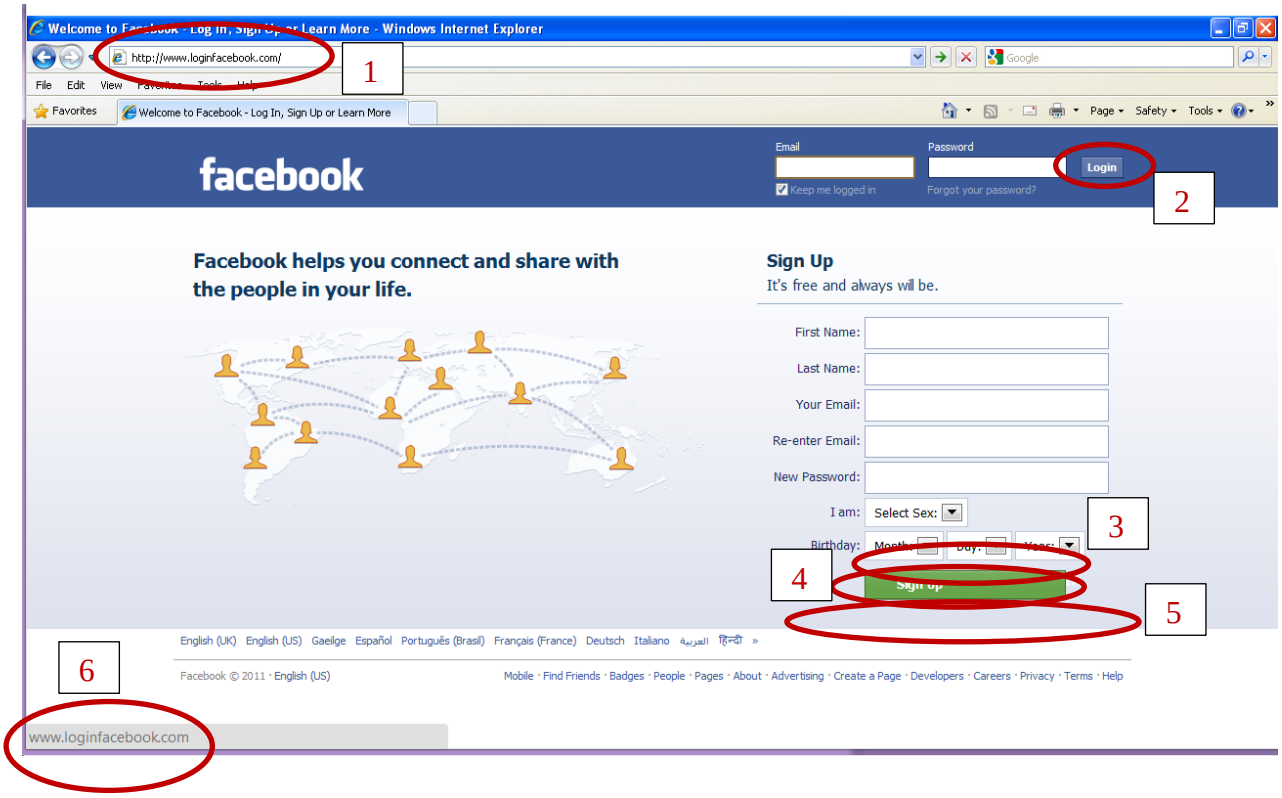
5. How do you rate this sample as a phishing email?

- ○ Certainly phishing
- ○ Probably phishing
- ○ No opinion
- ○ Probably not phishing
- ○ Certainly not phishing

6. What features inspired confidence or generated suspicion in authenticity?

Screenshot 4 Phish login

Tick beside each stimuli as each is noticed verbally or by mouse movement.



7. How do you rate this sample as a phishing webpage?

- ○ Certainly phishing
- ○ Probably phishing
- ○ No opinion
- ○ Probably not phishing
- ○ Certainly not phishing

8. What features inspired confidence or generated suspicion in authenticity?

9. Do you have any comments you wish to make in relation to this study?

Appendix G Consent Form

Facebook Phishing

Thank you for taking part in this phishing research study. The results are intended to be included for a Master of Science thesis in Cyberpsychology at the Institute of Art, Design and Technology. This study takes approximately 20 minutes to complete and aims to examine phishing awareness in Facebook users.

Phishing is the act of luring a user to willingly give up sensitive, personal details which can be used in identity theft, cash transfer and fraudulent credit card transactions. One way is to send a user an email in the hopes the user will reply or be directed to a website page that looks authentic but is not genuine.

Your participation in this study is voluntary and you may stop at any time. You do not have to answer any questions you do not want to answer. Your data is fully confidential and will not be identifiable as yours.

To complete this study you must:

- Be 18yrs or older
- Hold a Facebook account
- Have never taken any computer security training or studied Computer Science

Consent

I have read the above information, or it has been read to me. I have had the opportunity to ask questions about it and any questions that I have asked have been answered to my satisfaction. I agree for an audio recording to be made of the session and consent voluntarily to partake as a participant in this research.

Print Name of Participant _____

Signature of Participant _____

Date _____

Appendix H Screenshot Section Oral Instructions

(To be completed after questionnaire. Facebook screens are preloaded as individual tabs within browser. ***Ensure audio recording is ON****.)*

Read aloud:

"You are going to be shown four Facebook email and login page examples. Please examine the pages and determine if you think they genuinely belong to Facebook or are or fake (phishing). Please discuss or verbalise your observations."

Appendix I Debrief

Facebook Phishing Participant #____

Facebook Phishing Debrief

Thank you for participating in this study, your contribution is greatly appreciated. This study looked at examining phishing awareness in Irish Facebook users. Phishing is the act of luring a user to willingly give up sensitive, personal details which can be used in identity theft, cash transfer and fraudulent credit card transactions.

If you have been affected by this study, or wish to learn more about internet safety and phishing, please feel free to contact any of the following organisations:

- http://www.hotline.ie/
- http://www.wiredsafety.org/
- http://www.antiphishing.org/

If you have any complaints, concerns, or questions about this research, you may contact the researcher at kellylynnprice@gmail.com or Dr, Gráinne Kirwan, of the Institute of Art, Design and Technology, at Grainne.Kirwan@iadt.ie

Resourceful Readings

Government, U. S., & Commission, F. T. (2011). Consumer Guide to Computer Security: Fight Back Against Identity Theft, Malware, Hackers, Spyware, Spam, Botnets, Phishing - Online Privacy - Wireless, Laptop, Hotspot Security. Progressive Management.

Jakobsson, M. (2007). Phishing and Countermeasures : Understanding the Increasing Problem of Electronic Identity Theft. Hoboken N.J.: Wiley-Interscience.

Appendix J Nonparametric Correlations Personality and Ratings

Table 4

Nonparametric Correlations Personality and Ratings

		O	C	E	A	N	R1	R2	R3	R4
O	Correlation Coefficient	1.000	-.016	.187	-.298	.117	-.245	-.344	-.112	.046
	Sig. (2-tailed)	.	.951	.487	.245	.656	.344	.176	.668	.861
	N	17	17	16	17	17	17	17	17	17
C	Correlation Coefficient	-.016	1.000	.606*	.026	-.226	-.131	.111	-.093	-.461
	Sig. (2-tailed)	.951	.	.013	.921	.382	.617	.672	.723	.063
	N	17	17	16	17	17	17	17	17	17
E	Correlation Coefficient	.187	.606*	1.000	.196	-.419	-.120	.221	-.357	-.238
	Sig. (2-tailed)	.487	.013	.	.467	.106	.657	.411	.175	.374
	N	16	16	16	16	16	16	16	16	16
A	Correlation Coefficient	-.298	.026	.196	1.000	-.141	.168	.710**	.004	.049
	Sig. (2-tailed)	.245	.921	.467	.	.589	.518	.001	.987	.851
	N	17	17	16	17	17	17	17	17	17
N	Correlation Coefficient	.117	-.226	-.419	-.141	1.000	-.152	-.171	.057	.231
	Sig. (2-tailed)	.656	.382	.106	.589	.	.561	.511	.828	.372
	N	17	17	16	17	17	17	17	17	17
R1	Correlation Coefficient	-.245	-.131	-.120	.168	-.152	1.000	.216	.620**	.210
	Sig. (2-tailed)	.344	.617	.657	.518	.561	.	.374	.005	.387
	N	17	17	16	17	17	19	19	19	19
R2	Correlation Coefficient	-.344	.111	.221	.710**	-.171	.216	1.000	.109	-.064
	Sig. (2-tailed)	.176	.672	.411	.001	.511	.374	.	.656	.796
	N	17	17	16	17	17	19	19	19	19
R3	Correlation Coefficient	-.112	-.093	-.357	.004	.057	.620**	.109	1.000	.040
	Sig. (2-tailed)	.668	.723	.175	.987	.828	.005	.656	.	.872
	N	17	17	16	17	17	19	19	19	19
R4	Correlation Coefficient	.046	-.461	-.238	.049	.231	.210	-.064	.040	1.000
	Sig. (2-tailed)	.861	.063	.374	.851	.372	.387	.796	.872	.
	N	17	17	16	17	17	19	19	19	19

O=Openness, C=Conscientiousness, E=Extraversion, A=Agreeableness, N=Neuroticism, R1=Rating Phish Email, R2=Rating Genuine Web Login, R3=Rating Genuine Email, R4=Rating Phish Web Login

Appendix K Nonparametric Correlations Personality and Stimuli Count

Table 5

Nonparametric Correlations Personality and Stimuli Count

		O	C	E	A	N	S1	S2	S3	S4
O	Correlation Coefficient	1.000	-.016	.187	-.298	.117	.139	.004	-.020	-.184
	Sig. (2-tailed)	.	.951	.487	.245	.656	.594	.989	.940	.479
	N	17	17	16	17	17	17	17	17	17
C	Correlation Coefficient	-.016	1.000	.606*	.026	-.226	-.078	.168	.181	.176
	Sig. (2-tailed)	.951	.	.013	.921	.382	.766	.520	.486	.499
	N	17	17	16	17	17	17	17	17	17
E	Correlation Coefficient	.187	.606*	1.000	.196	-.419	.008	.087	.344	-.024
	Sig. (2-tailed)	.487	.013	.	.467	.106	.975	.750	.193	.928
	N	16	16	16	16	16	16	16	16	16
A	Correlation Coefficient	-.298	.026	.196	1.000	-.141	-.454	-.385	.377	.146
	Sig. (2-tailed)	.245	.921	.467	.	.589	.067	.127	.135	.576
	N	17	17	16	17	17	17	17	17	17
N	Correlation Coefficient	.117	-.226	-.419	-.141	1.000	-.248	.360	-.148	-.104
	Sig. (2-tailed)	.656	.382	.106	.589	.	.338	.155	.572	.692
	N	17	17	16	17	17	17	17	17	17
S1	Correlation Coefficient	.139	-.078	.008	-.454	-.248	-.290	-.338	.081	-.427
	Sig. (2-tailed)	.594	.766	.975	.067	.338	.229	.157	.741	.068
	N	17	17	16	17	17	19	19	19	19
S2	Correlation Coefficient	.004	.168	.087	-.385	.360	-.148	-.282	-.276	-.090
	Sig. (2-tailed)	.989	.520	.750	.127	.155	.545	.243	.253	.714
	N	17	17	16	17	17	19	19	19	19
S3	Correlation Coefficient	-.020	.181	.344	.377	-.148	-.345	-.002	-.583**	.129
	Sig. (2-tailed)	.940	.486	.193	.135	.572	.149	.993	.009	.599
	N	17	17	16	17	17	19	19	19	19
S4	Correlation Coefficient	-.184	.176	-.024	.146	-.104	-.139	.111	.023	-.704**
	Sig. (2-tailed)	.479	.499	.928	.576	.692	.571	.651	.925	.001
	N	17	17	16	17	17	19	19	19	19

O=Openness, C=Conscientiousness, E=Extraversion, A=Agreeableness, N=Neuroticism, S1= Stimuli Count Phish Email, S2= Stimuli Count Genuine Web Login, S3=Stimuli Count Genuine Email, S4= Stimuli Count Phish Web Login

Appendix L Nonparametric Correlations Impulsivity and Ratings

Table 6

Nonparametric Correlations Impulsivity and Ratings

		Impulsivity	Attention	Cognitive	R1	R2	R3	R4
Impulsivity	Correlation Coefficient	1.000	.569*	.501*	.096	.371	-.184	.467
	Sig. (2-tailed)	.	.022	.048	.724	.157	.495	.068
	N	16	16	16	16	16	16	16
Attention	Correlation Coefficient	.569*	1.000	.360	-.353	.255	-.232	.076
	Sig. (2-tailed)	.022	.	.171	.180	.340	.387	.780
	N	16	16	16	16	16	16	16
Cognitive	Correlation Coefficient	.501*	.360	1.000	.111	.175	-.076	.337
	Sig. (2-tailed)	.048	.171	.	.682	.516	.780	.202
	N	16	16	16	16	16	16	16
R1	Correlation Coefficient	.096	-.353	.111	1.000	.216	.620**	.210
	Sig. (2-tailed)	.724	.180	.682	.	.374	.005	.387
	N	16	16	16	19	19	19	19
R2	Correlation Coefficient	.371	.255	.175	.216	1.000	.109	-.064
	Sig. (2-tailed)	.157	.340	.516	.374	.	.656	.796
	N	16	16	16	19	19	19	19
R3	Correlation Coefficient	-.184	-.232	-.076	.620**	.109	1.000	.040
	Sig. (2-tailed)	.495	.387	.780	.005	.656	.	.872
	N	16	16	16	19	19	19	19
R4	Correlation Coefficient	.467	.076	.337	.210	-.064	.040	1.000
	Sig. (2-tailed)	.068	.780	.202	.387	.796	.872	.
	N	16	16	16	19	19	19	19

R1=Rating Phish Email, R2=Rating Genuine Web Login, R3=Rating Genuine Email, R4=Rating Phish Web Login

Appendix M Nonparametric Correlations Impulsivity and Stimuli Count

Table 7

Nonparametric Correlations Impulsivity and Stimuli Count

		Impulsivity	Attention	Cognitive	S1	S2	S3	S4
Impulsivity	Correlation Coefficient	1.000	.569*	.501*	-.395	.061	.224	-.228
	Sig. (2-tailed)	.	.022	.048	.130	.824	.405	.395
	N	16	16	16	16	16	16	16
Attention	Correlation Coefficient	.569*	1.000	.360	-.232	.127	-.075	.026
	Sig. (2-tailed)	.022	.	.171	.387	.639	.783	.924
	N	16	16	16	16	16	16	16
Cognitive	Correlation Coefficient	.501*	.360	1.000	-.591*	.004	.454	.242
	Sig. (2-tailed)	.048	.171	.	.016	.987	.077	.367
	N	16	16	16	16	16	16	16
S1	Correlation Coefficient	-.395	-.232	-.591*	1.000	.016	-.290	.204
	Sig. (2-tailed)	.130	.387	.016	.	.949	.228	.401
	N	16	16	16	19	19	19	19
S2	Correlation Coefficient	.061	.127	.004	.016	1.000	.148	.102
	Sig. (2-tailed)	.824	.639	.987	.949	.	.545	.677
	N	16	16	16	19	19	19	19
S3	Correlation Coefficient	.224	-.075	.454	-.290	.148	1.000	.095
	Sig. (2-tailed)	.405	.783	.077	.228	.545	.	.700
	N	16	16	16	19	19	19	19
S4	Correlation Coefficient	-.228	.026	.242	.204	.102	.095	1.000
	Sig. (2-tailed)	.395	.924	.367	.401	.677	.700	.
	N	16	16	16	19	19	19	19

S1= Stimuli Count Phish Email, S2= Stimuli Count Genuine Web Login, S3=Stimuli Count Genuine Email, S4= Stimuli Count Phish Web Login

Appendix N Nonparametric Correlations Trust in Facebook, Ratings and Stimuli Count

Table 8

Nonparametric Correlations Trust in Facebook, Ratings and Stimuli Count

		TrustFB	R1	R2	R3	R4	S1	S2	S2	S3
Trust FB	CorrCoefficient	1.000	.114	.118	.417	-.061	.113	.282	-.640**	.058
	Sig. (2-tailed)	.	.653	.640	.085	.809	.654	.256	.004	.818
	N	18	18	18	18	18	18	18	18	18
R1	CorrCoefficient	.114	1.000	.216	.620**	.210	-.290	-.148	-.345	-.139
	Sig. (2-tailed)	.653	.	.374	.005	.387	.229	.545	.149	.571
	N	18	19	19	19	19	19	19	19	19
R2	CorrCoefficient	.118	.216	1.000	.109	-.064	-.338	-.282	-.002	.111
	Sig. (2-tailed)	.640	.374	.	.656	.796	.157	.243	.993	.651
	N	18	19	19	19	19	19	19	19	19
R3	CorrCoefficient	.417	.620**	.109	1.000	.040	.081	-.276	-.583**	.023
	Sig. (2-tailed)	.085	.005	.656	.	.872	.741	.253	.009	.925
	N	18	19	19	19	19	19	19	19	19
R4	CorrCoefficient	-.061	.210	-.064	.040	1.000	-.427	-.090	.129	-.704**
	Sig. (2-tailed)	.809	.387	.796	.872	.	.068	.714	.599	.001
	N	18	19	19	19	19	19	19	19	19
S1	CorrCoefficient	.113	-.290	-.338	.081	-.427	1.000	.016	-.290	.204
	Sig. (2-tailed)	.654	.229	.157	.741	.068	.	.949	.228	.401
	N	18	19	19	19	19	19	19	19	19
S2	CorrCoefficient	.282	-.148	-.282	-.276	-.090	.016	1.000	.148	.102
	Sig. (2-tailed)	.256	.545	.243	.253	.714	.949	.	.545	.677
	N	18	19	19	19	19	19	19	19	19
S3	CorrCoefficient	-.640**	-.345	-.002	-.583**	.129	-.290	.148	1.000	.095
	Sig. (2-tailed)	.004	.149	.993	.009	.599	.228	.545	.	.700
	N	18	19	19	19	19	19	19	19	19
S4	CorrCoefficient	.058	-.139	.111	.023	-.704**	.204	.102	.095	1.000
	Sig. (2-tailed)	.818	.571	.651	.925	.001	.401	.677	.700	.
	N	18	19	19	19	19	19	19	19	19

R1=Rating Phish Email, R2=Rating Genuine Web Login, R3=Rating Genuine Email, R4=Rating Phish Web Login, S1= Stimuli Count Phish Email, S2= Stimuli Count Genuine Web Login, S3=Stimuli Count Genuine Email, S4= Stimuli Count Phish Web Login