Routine Activity Theory and Phishing Victimisation: Who Gets Caught in the 'Net'?

Alice Hutchings and Hennessey Hayes*

Abstract

Phishing is the use of fraudulent emails to obtain personal financial information from victims by posing as legitimate financial institutions or commerce sites. This exploratory study involved interviewing 104 participants, 50 of whom reported having received a phishing email. The theoretical foundation for this research is Routine Activity Theory, whereby crime is considered to be the consequence of the presence of a motivated offender, the presence of a suitable target, and the absence of a capable guardian. One of the findings arising from this research indicates that potential victims who undertake high levels of routine activities relating to computer use and internet banking use are more likely to be attacked by motivated offenders. However, it is proposed that high measures in these variables also act as protective factors against subsequent victimisation. Additionally, email filters, although they may be effective in blocking a large number of spam emails, are unable to differentiate legitimate emails from some phishing attacks.

Introduction

Phishing is the act of fraudulently obtaining personal information, for example, credit card details, account names, and passwords, by using emails and websites that appear to belong to a legitimate online commerce site, such as a financial institution (Australian Institute of Criminology 2005b). Phishing typically consists of attacks (that is, receiving a fraudulent email) that rely on aspects of human nature for their success. Victims are manipulated to divulge personal information – a form of social engineering. Phishing can also, however, be based on technical exploits (for example, password sniffers intercepting encrypted passwords and key loggers capturing the victim's keystrokes) or a combination of both technology and social engineering (Australian Institute of Criminology 2005b). Lynch (2005) explains the origin of the word 'phishing':

> The word "phishing" comes from an analogy to fishing; the email is bait used to lure in "fish" from the "sea" of internet users. The "f" is changed to "ph" in keeping with computer hacking tradition (Lynch 2005:259).

In order to provide an analytic view of phishing victimisation this research uses the framework provided by Cohen and Felson's (1979) Routine Activity Theory (RAT). The act

* School of Criminology and Criminal Justice, Griffith University. Address all correspondence to: Alice Hutchings, Centre of Excellence in Policing and Security, Griffith University or email a.hutchings@griffith.edu.au.

of phishing fits Felson's definition of a 'predatory crime' as 'at least one person takes or damages the person or property of others' (Felson 1994:30). Property in this situation refers to personal information, which is then used or sold to third parties in order to commit further fraudulent activities, such as abusing victims' existing financial facilities, opening new accounts and obtaining debts and liabilities in victims' names, or using the victim's identity when arrested for a crime (Lynch 2005). Therefore, phishing, examined within the RAT framework, occurs when there is: (1) the presence of a likely offender; (2) the presence of a suitable target; and (3) the absence of a capable guardian (Felson 1994:30). Grabosky (2007) and Yar (2005) both reviewed RAT in the context of cybercrime and concluded that the principles can be successfully adapted from physical to virtual space.

Prevalence and Economic Cost of Phishing Victimisation

Phishing is reported to be more common than other methods of identity theft, such as hacking, retrieving hard copy data, shoulder surfing, using insiders, and loading malicious software (Federal Deposit Insurance Corporation 2004). One study estimated that the total amount lost to phishing victimisation in the United States of America (USA) in 2007 was US$3.2 billion (Gartner 2007). AusCERT, Australia's Computer Emergency Response Team, is a not-for-profit organisation that responds to phishing websites by ensuring that they are closed down. Phishing first came to the attention of AusCERT in mid-2003. Between April 2004 and March 2007 the number of phishing sites with unique URL or domain names that were hosted by one or more hosts rose from 7 to 533, a 7,514% increase during this time period. These include sites targeting both national and international companies that have been reported to or detected by AusCERT (AusCERT 2007).

Other reports indicate that the rate of computer crime has been rising for some time. For example, Speer (2000) reported that in 1988 the American CERT Coordination team handled six incidents of computer crime compared to 3,734 ten years later in 1998, and then in just one year the rate almost doubled again, with 6,844 incidents in 1999. The Australian Computer Crime and Security Survey found that in 2006, 6% of respondent organisations detected identification theft against staff, customers or clients (it is not indicated if the identification theft was conducted through phishing attacks or other means), and eight companies reported a combined annual loss of AUD$215,103 (AusCERT 2006). This is a substantial increase from the 2005 survey, in which four companies reported an annual loss of AUD$62,000 (AusCERT 2005), however this may be due to the increased sample size of the 2006 survey. It is important to keep in mind, however, that this survey contains a number of limitations, which make it hard to apply the results to phishing in general. The survey had a low (17%) response rate (AusCERT 2006); only eight company respondents reported identity theft (resulting in an average AUD$26,888 loss per company); different companies may calculate their losses in different ways (Australian Institute of Criminology 2005a); and no specific information was provided about organisations likely to be targeted for phishing attacks, such as banks and other financial institutions, which only constituted 6% of the overall sample (AusCERT 2006).

Targeted corporations may under-report phishing incidents for a number of reasons. In 2006 the Australian Computer Crime and Security Survey found that of the respondent companies that had experienced any type of electronic attack, 69% chose not to report it to anyone outside their organisation (AusCERT 2006). Reasons for not reporting included, among others: perceived negative publicity (46%); not being aware of law enforcement interest (52%); not thinking perpetrators would be caught (57%); and not thinking law enforcement was capable (55%) (AusCERT 2006). Australia's leading banks were contacted during the current study and invited to provide data concerning the frequency of phishing

victimisation. All declined to do so, with one advising that the information was considered commercially sensitive. This is illustrative of the reluctance of financial institutions to disclose victimisation.

Reviewing the outcome of investigations reported in the Australian Computer Crime and Security Survey it is not surprising that organisations hold negative views about law enforcement action. Only 19% of law enforcement investigations resulted in criminal charges (AusCERT 2006). Other outcomes included allegations not being investigated (21%), inadequate legislation (2%), lack of evidence (49%), and jurisdictional difficulties (7%) (AusCERT 2006). These difficulties faced by law enforcement agencies emphasise the need for prevention in addition to prosecution. As Graycar and Smith (2002) note, taking no action may convey the message that phishing is tolerated by law enforcement agencies.

In addition, individuals may not report victimisation for a number of reasons. Muscat et al (2002) conducted a study on consumer fraud and found that only 35% of victims reported the incident to the police or another agency. Reasons for victims not to report phishing may include not being aware that they have become a victim due to not checking banking activity or credit rating (MacGibbon 2005), not being aware of law enforcement interest (Federal Deposit Insurance Corporation 2004), and feeling responsible for becoming a victim (Muscat et al 2002). Yar (2006) estimates that as little as 5% of computer crimes are reported to authorities.

Application of Routine Activity Theory

RAT moves the explanation of crime away from focusing solely on the offender, to also include the suitable targets, and the guardians of those targets. This theory proposes that crime occurs during every-day routines in normal life when a suitable target is in the presence of a motivated offender and is without a capable guardian (Cohen & Felson 1979).

Presence of a Likely Offender

As the quantity of people using the internet increases, so does the number of likely offenders with the technical knowledge to commit phishing offences. On the internet likely offenders have the advantages of anonymity and no geographical limitations. They may avoid detection and/or criminal charges due to law enforcement agencies being hampered by jurisdictional, legislative and evidentiary issues (AusCERT 2005). 'Phishing kits' can be acquired online and require a minimum level of expertise to utilise (Australian Institute of Criminology 2006).

The majority of phishing websites are hosted within the USA. The Anti-Phishing Working Group reported that in December 2007 the top three countries hosting phishing websites were the USA (32.5%), China (22.4%) and the Russian Federation (9.3%). The remaining countries constituting the top 10 were Thailand, Israel, Egypt, Germany, France, Republic of Korea and India (Anti-Phishing Working Group 2008). Those who obtain victims' information using phishing attacks may sell the data on the online market, therefore removing themselves from its subsequent use (Lynch 2005). There is also speculation that attacks are coordinated to a large extent, and that links to organised crime include the laundering of proceeds (Lynch 2005).

Duffield and Grabosky (2001) have compared the psychological correlates of the motivated offenders of fraud, depending on the organisational context in which it occurs and the nature of the relationship between the offender and the victim. Under their typologies, phishing would be classified as 'fraud committed against a number of individuals through print or electronic media … pitched at a relatively large number of prospective victims'

(Duffield & Grabosky 2001:1). Duffield and Grabosky (2001) describe the motivational elements common to all types of fraud to be financial strain, power over people, and the gratification obtained from mastery of a situation. Additionally, offenders may justify or rationalise their actions (Duffield & Grabosky 2001). In the context of phishing, rationalisation by an offender may incorporate the fact that the victim is usually refunded the fraudulently obtained amount by the financial institution (who can afford it), minimising the crime (as they are only obtaining a little from a lot of people), and assuming that offences will not be pursued by law enforcement. Duffield and Grabosky (2001) also claim that each of their fraud typologies have unique correlating psychological factors. In the case of phishing, which uses an indirect means to access potential victims, social cues are removed, leading 'to a reduction in the influence of social norms and constraints on the average person's behaviour' (Duffield & Grabosky 2001:5).

Presence of a Suitable Target

Suitable targets for phishing include accounts held in financial institutions and other on-line businesses, such as eBay. AusCERT (2005) notes that all of Australia's major banks have experienced theft of some of their customers' identities through phishing attacks. The Anti-Phishing Working Group (2008) reports that in the USA 91.7% phishing attacks during the month of December 2007 targeted the financial services sector. Other targeted industry sectors included retail sites (1.4%) and Internet Service Providers (1.4%), with the remaining included in a government and miscellaneous category (Anti-Phishing Working Group 2008).

The number of suitable targets increases with the behaviours of potential victims, for example, more people using the internet and internet banking. The Department of Broadband, Communications and Digital Economy (2008) identifies that both are on the rise: use of internet banking increased from 38% of Australians in 2001 to 56% as at June 2006; and 77% of Australians had accessed the internet in 2006, compared with 64% in 2001.

Absence of a Capable Guardian

The third element of RAT is the absence of a capable guardian. The term 'capable guardian' is used widely; it may include the owner of the property (in the context of phishing, the account holder), law enforcement, Computer Emergency Response Teams (CERTs), banks and financial institutions, or any other individual or agency that has the potential to discourage offenders (Yar 2005). As phishing is often based on attacks that rely on aspects of human nature rather than technical exploits, a capable guardian can be created by arming them with information and awareness, rather than security software.

The Australian Crime and Security Survey suggest that this awareness may be lacking. In 2006 it was found that although 98% of respondent companies used anti-virus software and firewalls, only 15% of general employees believed that they received adequate training in security awareness (AusCERT 2006). Similarly, the second highest factor attributed to electronic attacks was inadequate staff training and education in security practices and procedures (53% of respondent companies who experienced any type of electronic attack, the nature of which is unspecified) (AusCERT 2006).

Increasing the public's awareness of potential victimisation enhances their capacity to be capable guardians. As stated by Grabosky and Smith (2001:39), a 'key principle in the prevention of digital crime is the need to raise awareness on the part of prospective victims to the risks which they face'. In March 2005 the Australasian Consumer Fraud Taskforce

(ACFT) was established. This taskforce consists of 19 government agencies and departments who are concerned with consumer protection in relation to frauds and scams (Australasian Consumer Fraud Taskforce 2008). The aims of the ACFT include a yearly information campaign for consumers, which has been held annually since 2006. Smith and Akman (2008) evaluated the 2007 campaign and concluded that it was highly effective in raising consumer awareness. The campaign included the distribution of posters, flyers, identity fraud prevention kits, media releases, radio and television appearances, and advertisements and articles in newspapers and magazines (Smith & Akman 2008).

Banks and financial institutions may also provide public awareness to their clients. As at 30 June 2008 there were 14 Australian-owned banks, 10 foreign subsidiary banks, 34 branches of foreign banks, 12 building societies, 132 credit unions and 3 specialist credit card institutions operating in Australia (Australian Prudential Regulation Authority 2008). The websites of Australia's four main banks, namely the Commonwealth Bank of Australia, the National Australia Bank, Westpac and ANZ, were perused to identify how they advised their clients online about phishing attacks. All of these banking websites cautioned against accessing internet banking facilities from a link within an email, as well as recommending the use of email filters, providing hints on how to identify whether a website was authentic, and advising of procedures for reporting hoax emails.

However, it appears that financial institutions are not comfortable in undertaking the role of capable guardian. The Parliamentary Joint Committee on the Australian Crime Commission (2004) report on *Cybercrime* noted that a submission by the Australian Bankers' Association emphasised consumer responsibility for self-protection from fraud, rather than the banks' duty to protect their customers. While banks will usually compensate victims for their monetary losses, they are not obligated to take the matter any further. Lynch (2005) argues that there is no financial incentive for financial institutions to prevent identity theft, claiming that the cost is insignificant when compared to sales volume. However, there have been recent improvements by financial institutions, such as the use of two- and even three-factor identification, whereby account holders are required to identify themselves using multiple methods, such as a password in addition to a digital token (Smith 2007).

Target Hardening and Deflecting Offenders

While phishing offences may seem straightforward, jurisdictional or evidentiary issues hamper law enforcement agencies. Investigators must act quickly to obtain necessary evidence, with the average time online for a phishing site being three days in December 2007 (Anti-Phishing Working Group 2008). Investigation is also difficult and costly (Lynch 2005). There may be reluctance to commence an investigation into a crime that has originated from another jurisdiction, particularly within countries that do not have laws criminalising their conduct (Lynch 2005).

One of the applications of RAT is in situational crime prevention. Traditionally this application is associated with 'target hardening' whereby suitable targets are 'hardened' to discourage likely offenders by increasing risks and decreasing rewards (Clarke 1995:91). Although target hardening measures for property are usually physical, such as the implementation of locks and barriers, target hardening is also used in cyberspace, for example, the use of passwords and firewalls.

Clarke (1995:111) also discusses another technique of situational crime prevention that arises from RAT, namely 'deflecting offenders', whereby opportunities for crime are reduced. Deflecting offenders in the case of phishing attacks includes the use of email

filters. Emigh (2005) maintains that email filters are effective in blocking phishing attacks as well as combating spam. However, the sensitivity of email filters in detecting legitimate messages may allow some phishing attacks to pass undetected (Emigh 2005).

Research Questions and Hypotheses

RAT provides a framework to shed light on what routine activities make someone more vulnerable to attack, and the characteristics of a capable guardian. The questions addressed by this research are: (1) Are there behavioural risk factors for phishing victimisation? (2) Are there behavioural risk factors for being a recipient of a phishing attack? and (3) Do email filters reduce the risk of receiving a phishing attack? 'Phishing attack' refers to receiving a fraudulent email requesting personal information. Victims of this crime are the individual account holders, although the targeted financial institution will usually provide a refund for fraudulent activity if certain criteria are met (Federal Deposit Insurance Corporation 2004). Financial institutions recover these losses through higher interest rates and account fees (Lynch 2005). For the purpose of this research 'victims' are those who have provided their account details and subsequently incurred financial loss; however it is noted that this term may also be applied to those who have received a phishing email. This latter category is referred to herein as those who have been 'attacked'. In addition, this research is examining individual, rather than organisational, victims.

The first hypothesis tests the relationship of three behavioural independent variables, namely computer experience, internet experience and the use of internet banking, on the dependent variable, phishing victimisation. The second hypothesis tests the relationship of three behavioural independent variables, namely computer use, internet use and the use of internet banking, with the dependent variable, phishing attack status. The third hypothesis is that those who use email filters are less likely to receive a phishing attack. Specifically, the hypothesised directions of these variables are:

H_1 The lower the level of computer experience (IV_1), the lower the level of internet experience (IV_2), and the higher the use of internet banking (IV_3), the higher the risk for victimisation (DV_1);

H_2 The higher the level of computer use (IV_4), the higher the level of internet use (IV_5), and the higher the use of internet banking (IV_3), the higher the risk for phishing attack (DV_2); and

H_3 The use of mail filters (IV_6) reduces the risk of phishing attack (DV_2).

In relation to the first and second hypotheses, it is not predicted that the relationships are causal or deterministic relationships, but rather that these factors make the population more vulnerable to victimisation and attack. This research is examining whether those who have been victimised or attacked have these characteristics in common. If this is the case, this research proposes that these independent variables are risk factors for phishing victimisation or attack.

The purpose of this research is exploratory as it is expected that these hypotheses will expand our current knowledge of what predicts victimisation. These hypotheses test whether behaviours are risk factors for phishing attack, and whether email filters are useful in deflecting offenders. With such knowledge crime prevention efforts may be better targeted to reduce the incidence of phishing.

Participants

The population for this research included individuals aged over 18 located within the Brisbane metropolitan area who access the internet. The 104 participants in this research were randomly selected from the telephone directory and contacted by telephone. Participants were offered the chance to enter the draw to win one of five 1GB iPod Shuffles as an incentive to participate. Of the 476 potential respondents who declined to participate in the research, 100 volunteered to the researcher that they did not access the internet, and therefore were not members of the target population. Therefore, the research had an overall participation rate of 22.5%; however, the participation rate for the target population was 27.7%.

Design

This research employed a quantitative, cross-sectional survey design, examining phishing victimisation within the population at one point in time. The operational definition of prevalence is the number of phishing victims divided by the number of respondents who have been the recipient of a phishing email. The concept of phishing victimisation is defined as fraudulent activity resulting from the disclosure of account details in response to an email purporting to be from a bank or financial institution during the past five years.

Materials and Measures

The survey used for this research was constructed using exhaustive and mutually exclusive close-ended questions. The first section measured computer experience, which also included a subscale for computer use, the second measured internet experience, and included a subscale for internet use, the third measured levels of internet banking, the fourth section measured phishing victimisation, and the final section obtained demographic information, as well as computer security measures used.

The measure of computer experience utilised a survey prepared by Cassidy and Eachus (2002), which was found to have a high and significant correlation with actual computer experience ($r = 0.79$, $p < .001$). Internal reliability for Cassidy and Eachus' (2002) research was high, with a Cronbach's alpha coefficient of .97. Test-retest reliability (after one month) was also high and statistically significant ($r = 0.86$, $p < .001$) (Cassidy & Eachus 2002). Cassidy and Eachus (2002) assert that the scale is not specific to any one particular type of computer use or software, and that it is an appropriate test to use on the general adult population. Internal reliability was also found to be high in the current study, with a Cronbach's alpha coefficient of .92.

Internet experience measured reported purposes of internet use, the average number of hours spent on the internet in a week, the number of email addresses held, and whether the respondent had received training in internet use.

The internet banking scale measured how often respondents used internet banking to check their account balance, to transfer funds, to pay bills and to maintain their account, and how many bank accounts they held which could be accessed by the internet. Two items, one measuring how often in a week internet banking accounts were accessed, and the second asking whether the respondent had been employed by a bank or financial institution within the past five years, were removed from the scale due to low inter-item correlations of .14 and .01 respectively. Prior to the removal of these items the Cronbach's alpha coefficient was poor, at .66. With these items removed the Cronbach's alpha coefficient was .90.

Computer use was contained as a subscale within the computer experience scale. The items making up this scale included purposes of computer use and employment within the past five years in a computer related profession. Internet use was contained as a subscale within the internet experience scale. The items making up this scale included purpose for internet use, the average hours per week spent on the internet, and the number of email addresses held. Table 1 below presents the minimum and maximum scores attainable for each scale, as well as the Cronbach's alpha coefficient.

Table 1: Minimum and Maximum Scores and Cronbach's Alpha Coefficient for the Computer Experience, Internet Experience, Internet Banking, Computer Use and Internet Use Scales

Scale	Min	Max	Cronbach's alpha coefficient
Computer experience	0	135	.92
Internet experience	1	29	.71
Internet banking	0	21	.90
Computer use	0	10	.72
Internet use	1	34	.76

The variables measuring phishing victimisation were modelled from three crime victimisation surveys: the US Census Bureau's (2001) *Computer Crime Security Survey*; the US Census Bureau's (2004) *National Crime Victimization Survey*; and the United Nations' (2000) *International Crime Victimisation Survey*. The survey used contingency questions; therefore, respondents were directed to questions depending on the responses they had previously provided. In order to capture retrospective information the survey included an item that asked about changes in computer experience, level of internet use and level of internet banking since victimisation.

The use of email filters was captured within a survey question enquiring about computer security measures utilised, which also included virus protection, firewall, administration passwords and intrusion detection systems. In order to measure whether the respondents were representative of the general population, demographic questions such as age, income, and education status, were modelled from the 2006 census (Australian Bureau of Statistics 2008).

A focus group was conducted with the researcher and nine university students, who volunteered to participate in exchange for course credit. The focus group addressed face validity by identifying any problems with interpretation of the meaning of the question, and content validity by ensuring that the questions covered the range of logical answers.

Results

Sample Characteristics

The gender of the respondents, compared to the 2006 census data for the Brisbane region (Australian Bureau of Statistics 2008), is shown in Table 2 below.

Table 2: Respondents' Gender Compared to 2006 Census Data for the Brisbane Region

Gender	*N*	Per cent	Per cent in Census Data
Male	49	47.1	49.1
Female	55	52.9	50.9
Total	104	100.0	100.0

Respondents' ages ranged from 18 to 85 (n = 104, M = 43.44, SD = 15.40). No respondents were aged under 18, as they were not eligible to participate in the research. The age brackets for the respondents, compared to the 2006 census data for the Brisbane region (Australian Bureau of Statistics 2008), is shown in Table 3 above. It is evident that the research attracted younger participants than the general population; however, it would be expected that those in the older age bracket (65 years or older) are less likely to use computers, and therefore were not the target population for this research.

Table 3: Respondents' Age Brackets Compared to 2006 Census Data for the Brisbane Region

Age Bracket	*N*	Per cent	Per cent in Census Data
15-24 years*	11	10.6	14.9
25-54 years	68	65.4	43.1
55-64 years	18	17.3	10.5
65 years or older	7	6.7	11.2
Total	104	100.0	79.7**

* This age bracket for the 2006 Census data is 15-24 years. This bracket is compared to the 18-24 year age bracket for this research.

** The 2006 Census Data also included age brackets for 0-14 years; therefore, the total percentage does not equal 100.

All of the respondents (n = 104) resided in Queensland, 95.2% (n = 99) in urban areas and 4.8% (n = 5) in rural areas. When asked about perceived ethnic or cultural origin 69.2% (n = 72) identified as Australian, 1.9% (n = 2) as Aboriginal or Torres Strait Islander, 14.4% (n = 15) as European, 3.8% (n = 4) as New Zealander, 5.8% (n = 6) as Asian and 4.9% (n = 5) as other. The majority of respondents, or 57.7% (n = 60) had completed an education level equivalent to or above a trade certificate or apprenticeship, while 42.3% (n = 44) had achieved up to Year 12. Despite respondents being provided with the option not to respond to any survey question, the only variable containing missing data was in relation to average annual income, with 5.8% (n = 6) of participants declining to disclose this information. Income categories were adopted from the 2006 census, with 4.8% (n = 5) earning a nil income, 29.8% (n = 31) earning between $1 and $31,199, and 59.6% ($n$ = 62) earning above $31,200.

Respondents were asked what their main reasons for using computers were. They were permitted to select more than one response. Personal reasons was selected by 75.0%

(*n* = 78) of respondents, 66.3% (*n* = 69) reported using computers for work purposes, 26.0% (*n* = 27) for study purposes and 7.7% (*n* = 8) used computers for other reasons.

The home was the most common place where the internet was accessed, as reported by 62.5% (*n* = 65) of respondents. Additionally, 33.7% (*n* = 35) mainly accessed the internet from work, 1.9% (*n* = 2) from university or school, 1% (*n* = 1) from a friend or relative's home and 1% (*n* = 1) accessed the internet from another location. Internet Explorer was the most popular web browser, used by 78.8% (*n* = 82) of respondents, however 10.6% (*n* = 11) respondents reported using Firefox as their main browser, 1.9% (*n* = 2) used Netscape Navigator, 2.9% (*n* = 3) used other browsers and 5.8% (*n* = 6) of respondents were not sure.

Table 4 below details whether respondents, or their joint account holders, had received phishing attacks within the past five years. These responses were subsequently collapsed to create a dichotomous (yes/no) variable.

Table 4: Respondents' Reported Phishing Attacks Within the Past Five Years

	N	Per cent	Cumulative Per cent
Yes, I have	37	35.6	35.6
Yes, my joint account holder has	0	0.0	35.6
Yes, we both have	13	12.5	48.1
No	53	51.0	99.1
Don't know	1	1.0	100.0
Total	104	100.0	100.0

Of the 50 respondents who reported having been the recipient of a phishing attack, one reported subsequent victimisation. Therefore, the prevalence rate of phishing victimisation (operationally defined as the number of phishing victims divided by the number of respondents who have been the recipient of a phishing email) was 2% for this sample.

Hypothesis One ~ Behavioural Risk Factors for Phishing Victimisation

The first hypothesis tested whether three behavioural variables are risk factors for phishing victimisation, namely computer experience, internet experience and use of internet banking. Unfortunately, due to the low number of phishing victims surveyed, this hypothesis was unable to be tested. Instead, the details of the victim identified in this research are presented below as a case study.

Case Study

The respondent who reported phishing victimisation was a male aged 50 (0.43 standard deviations above the mean). The respondent resided in an urban area in Queensland, reported his ethnicity as Australian and his highest education level was Year 12. His average annual income was $67,600 to $83,199. He accessed the internet mostly from home; however used computers for work and personal reasons. He used Internet Explorer to browse the internet and protected his computer with anti-virus software, email filters, administration passwords and firewall.

The incident was the only fraudulent activity on the respondent's bank account in the past five years. The victim provided his account details on the one occasion, details that were then used for unauthorised transactions to the value of $1,000 to $10,000. The respondent reported the unauthorised transactions to his bank/financial institution. He provided two reasons for doing so: to recover the amount, and because he wanted the offender to be caught/punished. He was able to recover the entire amount fraudulently obtained from the bank/financial institution, but was unaware of what further action had been taken. The matter took between one week and one month to be resolved, and the respondent rated the incident as very serious. He reported no subsequent problems in relation to his account, credit rating or criminal history. When asked about subsequent precautionary actions he advised that he no longer clicked on hyperlinks presented inside emails. The victim scored 97 for computer experience (0.53 standard deviations above the mean), 17 for internet experience (0.16 standard deviations above the mean), and 14 for internet banking (0.75 standard deviations above the mean).

Hypothesis Two ~ Behavioural Risk Factors for Phishing Attack

The second hypothesis tested whether three behavioural variables are risk factors for receiving a phishing attack, namely computer use, internet use and use of internet banking. Respondents' scores for the computer use (IV_4) scale ranged from 1 to 9 (n = 104,M = 5.65, SD = 2.12. The computer use scale was significantly negatively skewed. A Kolmogorov-Smirnov test confirmed the variable was not normally distributed (K-S = .12, p < .01). The computer use scale was recoded as two dichotomous variables (low/high). The median computer use score was used as the cut-off point. Those who scored from zero to five (n = 47) were classified as having low levels of computer use, and those who scored six or above (n = 57) were classified as having high levels of computer use.

The internet use (IV_5) scale ranged from 1 to 28 (n = 104, M = 14.76, SD = 5.33). A Kolmogorov-Smirnov test confirmed the variable was normally distributed (K-S = .07, p = .20). The internet use scale was recoded as two dichotomous variables (low/high). The median internet use score was used as the cut-off point. Those who scored from one to 14 (n = 52) were classified as having low levels of internet use, and those who scored 15 or above (n = 52) were classified as having high levels of internet use.

Eight cases within the internet banking (IV_3) scale contained a score of zero, which indicated that these respondents did not use internet banking. The range for the internet experience scale was 0 to 19 (n = 104, M = 9.25, SD = 5.78). This variable was not normally distributed (K-S = .17, p < .001) and was bi-modal in appearance, with large frequencies of cases clustered at the lower, as well as the higher, ends of the scale. The internet banking scale was recoded as two dichotomous variables (low/high). The median internet banking score was used as the cut-off point. Those who scored from 1 to 10 (n = 49) were classified as having low levels of internet banking use, and those who scored 11 or above (n = 55) were classified as having high levels of internet banking use.

Forced entry logistic regression was used to determine whether computer use, internet use and internet banking use predicted phishing attack status. The dichotomised variables for these scales were used as predictor variables, as this allowed for the calculation of conditional probabilities. Without any independent variables in the model 51.9% of respondents were correctly predicted to have not received a phishing attack (-2LL = 144.02).

The full model was significantly improved with all predictor variables (-2LL = 121.48) and was statistically better at predicting phishing attack status (χ^2 (3, n = 104) = 22.54, p < .001). The full model accounted for 26.0% of the variance and accurately predicted

70.2% of phishing attack status. Of the respondents who received a phishing attack, the model accurately predicted that 66.7% would have been attacked (true positives). Therefore, 33.3% of respondents who were predicted to receive a phishing attack did not (false positives). Conversely, of respondents predicted not to receive a phishing attack, 74.5% did not (true negatives) and 25.5% did (false negatives).

Wald statistics, odds ratios and 95% confidence limits for each of the three predictor variables are contained below in Table 5. As demonstrated by the Wald statistic, computer use significantly contributed to predicting phishing attack status.

Table 5: Logistic Regression Results for Computer Use, Internet Use, Internet Banking Use and Phishing Attack Status

	B	*SE*	Wald	*df*	Sig.	odds ratio	95% CI for odds ratio	
							Lower	Upper
Computer Use	1.57	.46	11.64	1	.001	4.79	1.95	11.80
Internet Use	0.13	.47	0.07	1	.79	1.14	0.45	2.86
Internet Banking Use	0.89	.46	3.72	1	.05	2.44	0.99	6.05
Constant	-1.50	.42	12.96	1	.000	0.22		
$N = 104$								
Nagelkerke $R^2 = .26$								

Interpreting the odds of phishing attack indicated that for respondents with high computer use the odds of receiving a phishing attack was 4.79 times higher than those who had low computer use (exp(B) = 4.79, 95% CI = 1.95-11.80). The odds of receiving a phishing attack was 1.14 times higher for respondents who had high internet use than those who had low internet use (exp(B) = 1.14, 95% CI = 0.45-2.86), and 2.44 times higher for those who had high internet banking use than low internet banking use (exp(B) = 2.44, 95% CI = 0.99-6.05), all other factors being equal.

No cases exceeded ±2.5 standardised residuals, indicating that there were no multivariate outliers within the model. The average VIF statistic for the independent variables was 1.16. As this was not substantially greater than 10, it indicated that the assumption of no multicollinearity had not been violated (Field 2005). Two-tailed Pearson's product-moment correlation coefficients were conducted in order to confirm that the assumption of multicollinearity for each of the four variables had not been violated. Table 6 below presents the results of these analyses.

Table 6: Correlations among Phishing Attack Status, Computer Use, Internet Use and Internet Banking

	Phishing Attack Status	Computer Use	Internet Use	Internet Banking
Phishing Attack Status		.41**	.19	.29*
Computer Use			.29*	.27*
Internet Use				.33*
Internet Banking				

* $p < .01$ ** $p < .001$

As can be seen in the above table, the assumptions of no multicollinearity was confirmed to have not been violated, as correlations did not exceed the threshold recommended by Pallant (2005) of .90.

Hypothesis Three ~ Relationship between Email Filters and Phishing Attack Status

The third hypothesis tested whether the use of email filters reduces the risk of receiving a phishing attack. The survey captured data concerning the use of email filters within a question about general computer security measures. This survey question was recoded as eight dichotomous variables (yes/no) for each computer security measure. The responses are provided in Table 7.

Table 7: Types of Computer Security Used

	Yes		No	
	N	Per cent	*N*	Per cent
Anti-Virus Software	101	97.1	3	2.9
Email Filters	77	74.0	27	26.0
Administration Passwords	64	61.5	40	42.5
Firewall	89	85.6	15	14.4
Intrusion Detection Systems	41	39.4	63	60.6
Other	19	18.3	85	81.7
Don't Know	16	15.4	88	84.6

In order to determine whether the use of email filters was related to phishing attack status, a chi-square test for independence was conducted. It was found that there was no significant relationship between the use of email filters and receiving a phishing attack (χ^2 (1, $N = 104$) = 1.78, $p = .18$).

Chi-square tests for independence were also conducted with the other types of computer security reportedly used by participants to determine if they are related to phishing attack

status. The test with anti-virus software as the independent variable is not reported, as it was found to violate the assumption of at least five expected frequencies (Field 2005). No significant relationship was found between receiving a phishing attack and the use of administration passwords (χ^2 (1, N = 104) = 0.25, p = .62), intrusion detection systems (χ^2 (1, N = 104) = 1.77, p = .19), other types of computer security devices (χ^2 (1, N = 104) = 2.12, p = .15), or not knowing what type of computer security device(s) were in use (χ^2 (1, N = 104) = 2.15, p = .14). However, as presented below in Table 8, there was a significant relationship between firewall status and phishing attack status. Interestingly, respondents who did not have firewall were less likely to receive a phishing attack. Forty-nine of the 50 respondents who reported having received a phishing attack used firewall, and of the 15 that reported that they did not use firewall, only one had received a phishing attack.

Table 8: Contingency Table for Firewall Status and Phishing Attack Status (Expected Frequencies are Shown in Parentheses)

	Firewall Status		
Phishing Attack Status	No	Yes	Total
No	14 (7.8)	40 (46.2)	54
Yes	1 (7.2)	49 (42.8)	50
Total	15	89	104

χ^2 (1, N = 104) = 12.04

p < .01

The odds ratio indicated that respondents with firewall were 17.15 times more likely to receive a phishing attack than those who did not use firewall. Further analyses were conducted in order to ascertain the relationship between firewall status and computer use, internet use, and use of internet banking.

As computer use was significantly negatively skewed, this variable was transformed by reflection and square root to meet the assumptions of parametric tests. This significantly improved normality (Kolmogorov-Smirnov = .113, p < .01). An independent samples t-test was conducted to compare computer use scores for those with and without firewall. Those with firewall scored significantly higher in computer use (M = 2.44, SD = 0.45) than those without firewall (M = 1.95, SD = 0.51; t(102) = 3.51, p < .01). The magnitude of the differences in the means was moderate (eta squared = .11).

An independent samples t-test was conducted to compare internet use scores for those with and without firewall. Again, those with firewall scored significantly higher in internet use (M = 15.57, SD = 4.86) than those without firewall (M = 9.93, SD = 5.56; t(102) = -4.07, p < .001). The magnitude of the differences in the means was large (eta squared = .14).

Attempts were made to normalise the internet banking scale, however transformation did not significantly improve normality. In order to determine whether the use of firewall was related to use of internet banking, a chi-square test for independence was conducted with the dichotomised internet banking variable. It was found that those without firewall were significantly more likely to score low in use of internet banking than those with firewall (χ^2 (1, N = 104) = 4.84, p < .05). The contingency table presented in Table 9 presents the distribution of internet banking use according to firewall status.

Table 9: Contingency Table for Firewall Status and Internet Banking Use (Expected Frequencies are Shown in Parentheses)

	Internet Banking Use		
Firewall Status	Low	High	Total
No	11 (7.1)	4 (7.9)	15
Yes	38 (41.9)	51 (47.1)	89
Total	49	55	104

χ^2 (1, N = 104) = 4.84

p < .05

Discussion

Of the 50 respondents who reported having received a phishing attack, one reported subsequent victimisation; therefore, the prevalence rate for this sample was 2%. This incident had been reported to the financial institution where the account was held, but the victim had not notified the police or another law enforcement agency. However, due to the small sample size there is limited power to generalise this result to the larger population of internet users. Victimisation may have been underreported, as victims may not have been aware that they had been victimised if they had not checked their credit rating or banking activity (MacGibbon 2005). In addition, victims may not have disclosed to the researcher that they had provided their account details, as they may have felt responsible for victimisation (Muscat et al 2002). Those who had been victimised may also have been less likely to participate in the research, as their trust in providing personal details, even to a reputable agency, had already been compromised.

Behavioural Risk Factors for Phishing Victimisation

The first hypothesis tested whether behavioural risk factors, namely low computer experience, low internet experience and high use of internet banking, increases the risk for phishing victimisation. While this hypothesis was unable to be tested statistically, due to the low number of phishing victims surveyed, a case study for the respondent was presented.

The victim's scores for computer experience, internet experience and internet banking use did not exceed one standard deviation from the mean, indicating that in these respects he was average compared to the other respondents. The timing of the phishing attack is believed to have occurred at the time when the number of phishing sites detected by or reported to AusCERT's was increasing rapidly. The victim's levels of computer use, internet use and internet banking may have been at a level where he was likely to have received a phishing attack, but may not have been high enough to act as a protective factor against victimisation. However, as the results are limited to one participant, these analyses are conjectural only, and cannot be tested statistically.

Behavioural Risk Factors for Phishing Attack

The second hypothesis, which tested whether behavioural variables, namely high computer use, high internet use and high use of internet banking, increased the risk for receiving a phishing attack, was partially supported. Overall, these variables produced a statistically significant model, which accounted for 21.3% of the total variance. As respondents' levels

of computer use, internet use, and internet banking increased, so did the odds that they would receive a phishing attack.

However, this hypothesis was partially supported as only computer use was a significant predictor of phishing attack status, with internet banking use approaching significance ($p = .05$) and level of internet use contributing little individual variance to the model. It is likely that internet banking use would be a significant variable with a larger sample size. Therefore, it is proposed that computer use and internet banking are risk factors for phishing attack. In the context of RAT, these independent variables represent the routine activities and suitable targets that motivated offenders take advantage of when there is the absence of a capable guardian.

Another implication to consider is that while these variables are risk factors for phishing attack, they may also act as protective factors against victimisation. For example, those who regularly use internet banking may be exposed to warnings concerning phishing published on the websites of their financial institution(s). This form of public awareness informs potential victims how to act as capable guardians. This may explain why those who rated highly on these measures and who received an attack did not provide their account details.

Relationship between Email Filters and Phishing Attack Status

The third hypothesis was that email filters reduce the risk of receiving a phishing attack. This hypothesis was not supported, as it was found that there was no significant relationship between the use of email filters and receiving a phishing attack. This finding questions the sensitivity of email filters to accurately differentiate between phishing attacks and genuine email messages. This indicates that this crime prevention method, although possibly effective in preventing the majority of phishing attempts, does not deflect all motivated offenders.

The relationships with phishing attack and other computer security measures were also tested. An unexpected result was found for the use of firewall, whereby respondents who used firewall were 17.15 times more likely to receive a phishing attack than those who did not use firewall. However, this finding is likely to be spurious in nature, reflecting the relationship between firewall status, and computer use, internet use, and use of internet banking. Respondents without firewall scored significantly lower in each of these variables than respondents who did use firewall. Therefore, the relationship between firewall status and phishing attack status may in fact be reflecting the relationship between firewall status and these risk factors for phishing attack.

Recommendations for Crime Prevention

This research provides some guidance for the future directions of crime prevention initiatives. These include setting up a national database of phishing victimisation, and continuing existing public awareness campaigns.

National, centralised data collection would be one way to overcome problems relating to the real prevalence rate of phishing victimisation. At present the prevalence of phishing websites is recorded by AusCERT, while data concerning phishing victimisation may be collected by a number of different agencies, mainly the banks and financial institutions that have been targeted by phishing offenders and subsequently approached by their customers seeking restitution. Knowing the real prevalence rate of phishing victimisation is helpful for crime prevention efforts, as it allows crime prevention initiatives to be evaluated pre- and post-intervention.

The implication of these research findings is that as behavioural factors do play a role in the likelihood of receiving a phishing attack, public awareness campaigns, such as the Australasian Consumer Fraud Taskforce's annual fraud awareness month, and public awareness provided by media attention, may play an important role in countering future phishing attacks. This may make potential victims more aware of the risks that they face, enabling them to be capable guardians of their personal information.

Limitations

This research has attempted to overcome the significant difficulties associated with this challenging area of research. However, a number of limitations of the research design were identified. First, as the information was gathered for one particular time period, it is problematic to generalise from these results at a later date due to increased awareness of the part of potential victims and the use of future technology in preventing phishing attack and victimisation. Secondly, problems determining the time-order sequence due to retrospective questions may have weakened the results obtained for the victim.

Additionally, as the research design utilised a telephone survey it only consisted of respondents who had a landline telephone. Historically researchers have contemplated the associated biases with telephone surveys due to under representation in low socio-economic areas. Increasingly, however, researchers will also have to consider the impact of increased number of mobile phones replacing traditional landline telephones, particularly with the growing popularity of capped mobile telephone accounts. A study conducted in the USA found that 7% of households had mobile phones only. Those who resided in households with mobile phones only were more likely to be younger, unmarried, and renting, and it was estimated that the percentage of mobile phone households only would increase in the future (Tucker et al 2007).

A final limitation is the possibility of self-selection bias, whereas some members of the population may be more likely to complete the survey than others. While incentives were in place to increase response rates and thereby reduce self-selection bias, due to privacy issues and the anonymity of the design it was not possible to follow up participants who have not completed the survey for their responses. As discussed, this could include those who had been victimised and were unwilling to disclose further personal details.

Application of Routine Activity Theory in Cyberspace

Grabosky (2007) and Yar (2005) have suggested that RAT could provide a useful framework for conceptualising and understanding computer crime. These results confirm that RAT is a practical theoretical framework when applied to cyberspace. This theory was particularly influential in informing the analyses for this study. For example, the routine activities of computer use and internet banking use were found to be risk factors for phishing attack. It was also proposed that capable guardians score highly on these variables, which act as protective factors against providing details of personal identification.

As mentioned previously, recruiting participants is difficult, and people may not be willing to disclose victimisation. Future researchers taking a RAT approach to phishing may be better able to gain access to victims by undertaking research with the support of banks and financial institutions, at the point when victims seek restitution. However, gaining cooperation from these entities may prove to be difficult, as this research has found that they have been unwilling to disclose information that could be interpreted as commercially damaging.

Additionally, shifting the focus of future research from victims to offenders could enable the motivated offenders element of RAT to be tested. Data arising from research concerning victims and offenders could therefore be triangulated to confirm and validate findings. Again, a number of difficulties in reaching this population would be anticipated.

Further questions that could be asked of computer users include their protective behaviours when using the internet; the relationship between use of 'risky' or unprotected computers and networks, victim characteristics and victimisation; and the relationship between 'real world' victimisation and online victimisation.

References

Anti-Phishing Working Group 2008 *Phishing Activity Trends: Report for the Month of December, 2007* <www.antiphishing.org/reports/apwg_report_dec_2007.pdf> accessed 17 July 2008

AusCERT 2005 *Australian 2005 Computer Crime and Security Survey* Brisbane AusCERT

AusCERT 2006 *Australian 2006 Computer Crime and Security Survey* Brisbane AusCERT

AusCERT 2007 'Personal Communication'

Australasian Consumer Fraud Taskforce 2008 *About the Australasian Consumer Fraud Taskforce* <www.scamwatch.gov.au/content/index.phtml/itemId/725675> accessed 17 July 2008

Australian Bureau of Statistics 2008 *2006 Census QuickStats: Brisbane (Statistical Division)* <www.censusdata.abs.gov.au/ABSNavigation/prenav/ProductSelect?newproducttype=QuickStats&btnSelectProduct=View+QuickStats+%3E&collection=Census&period=2006&areacode=305&geography=&method=&productlabel=&producttype=&topic=&navmapdisplayed=true&javascript=true&breadcrumb=LP&topholder=0&leftholder=0&currentaction=201&action=401&textversion=false> accessed 10 July 2008

Australian Institute of Criminology 2005a 'Computer crime trends' *Crime Facts Info* vol 99 pp 1

Australian Institute of Criminology 2005b 'Phishing' *High Tech Crime Brief* vol 9 pp 1-2

Australian Institute of Criminology 2006 'Acquiring high tech crime tools' *High Tech Crime Brief* vol 13 pp 1-2

Australian Prudential Regulation Authority 2008 *List of Authorised Deposit-Taking Institutions* <www.apra.gov.au/adi/ADIList.cfm> accessed 17 July 2008

Cassidy S & Eachus P 2002 'Developing the Computer User Self-Efficacy (CUSE) scale: Investigating the relationship between computer self-efficacy, gender and experience with computers' *Journal of Educational Computing Research* vol 26 no 2 pp 133-153

Clarke RV 1995 'Situational crime prevention' *Crime and Justice* vol 19 pp 91-150

Cohen LE & Felson M 1979 'Social change and crime rate trends: A routine activity approach' *American Sociological Review* vol 44 no 4 pp 588-608

Department of Broadband, Communications and Digital Economy 2008 *Online statistics: Internet subscribers in Australia* <www.archive.dbcde.gov.au/2008/01/statistical_benchmarking/online_statistics> accessed 17 July 2008

Duffield G & Grabosky P 2001 'The psychology of fraud' *Trends and Issues in Crime and Criminal Justice* vol 199 pp 1-6

Emigh A 2008 *Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures* <www.antiphishing.org/Phishing-dhs-report.pdf> accessed 17 July 2008

Federal Deposit Insurance Corporation 2004 *Putting an End to Account-Hijacking Identity Theft* Washington, DC Federal Deposit Insurance Corporation

Felson M 1994 *Crime and Everyday Life* Thousand Oakes Pine Forge Press

Field A 2005 *Discovering Statistics Using SPSS* London Sage Publications Ltd

Gartner I 2008 *Gartner Survey Shows Phishing Attacks Escalated in 2007; More Than $3 Billion Lost to These Attacks* <www.gartner.com/it/page.jsp?id=565125> accessed 17 July 2008

Grabosky P 2007 *Electronic Crime* New Jersey Pearson Education Inc

Grabosky P & Smith R 2001 'Telecommunication fraud in the digital age' in Wall DS (ed) *Crime and the Internet* London Routledge

Graycar A & Smith RG 2002 'Identifying and responding to electronic fraud risks' 30th Australasian Registrars' Conference Canberra

Lynch J 2005 'Identity theft in cyberspace: Crime control methods and their effectiveness in combating phishing attacks' *Berkeley Technology Law Journal* vol 20 pp 259-300

MacGibbon A 2005 *Australian e-Commerce Safety Guide 2005* Sydney eBay

Muscat G, James M & Graycar A 2002 'Older people and consumer fraud' *Trends and Issues in Crime and Criminal Justice* vol 220 pp 1-6

Pallant J 2005 *SPSS Survival Manual* St Leonards Allen & Unwin

Parliamentary Joint Committee on the Australian Crime Commission 2004 *Cybercrime* Canberra Parliament of the Commonwealth of Australia

Smith RG 2007 'Biometric solutions to identity-related cybercrime' in Jewkes Y (ed) *Crime Online* Devon Willan Publishing

Smith RG & Akman T 2008 'Raising public awareness of consumer fraud in Australia' *Trends and Issues in Crime and Criminal Justice* vol 349 pp 1-6

Speer DL 2000 'Redefining borders: The challenges of cybercrime'*Crime, Law and Social Change* vol 34 no 3 pp 259-273

Tucker C, Brick JM & Meekins B 2007 'Household telephone service and usage patterns in the United States in 2004: Implications for telephone samples' *Public Opinion Quarterly* vol 71 no 1 pp 3-22

United Nations 2000 *International Crime Victimisation Survey* Vienna The United Nations Office on Drugs and Crime

US Census Bureau 2001 *Computer Crime Survey* Washington, DC Bureau of Justice Statistics

US Census Bureau 2004 *National Crime Victimization Survey* Washington, DC Bureau of Justice Statistics

Yar M 2005 'The novelty of "cybercrime": An assessment in light of routine activity theory' *European Journal of Criminology* vol 2 no 4 pp 407-427

Yar M 2006 *Cybercrime and Society* London SAGE Publications Ltd