How Contextualisation Affects the Vulnerability of Individuals to Phishing Attempts

Completed Research Paper

Farkhondeh Hassandoust **Harminder Singh** **Jocelyn Williams**

Abstract

Hackers who engage in phishing manipulate their victims into revealing confidential information by exploiting their motives, habits and cognitive biases. Drawing on heuristic-systematic processing and anchoring effects, this study examines how the contextualisation of phishing messages, by modifying their framing and content, affects individual susceptibility to phishing. This study also investigates if there is a discrepancy between how individuals believe they will react to phishing attempts and their actual reactions. Using two fake phishing campaigns and an online survey, we find that individuals are more susceptible to phishing attempts when the phishing messages they receive are specific to their context, thereby appealing to their psychological vulnerabilities. There is also a significant gap between how individuals believe they will react and their actual reactions to phishing attempts. Finally, we find that these results vary by gender.

Keywords: Information security awareness, phishing, protective practices and reactions, heuristic-systematic processing, anchoring effect, gender studies

Introduction

In 2016, more than 40% of computer users around the world were victims of cybercrimes, such as social engineering, phishing or malware attacks[1], and over half of these users were not even aware that they had been hacked (Hanus and Wu 2016). This could be because, for example, social engineering attacks carried out through phishing allow hackers to circumvent information security countermeasures. In this way, these incidents remain a persistent threat to individuals and organisations. Hackers who engage in phishing manipulate individuals into revealing their confidential information by exploiting their motives, habits and cognitive biases (Mitnick and Simon 2002).

Although Internet users have become more aware of phishing, phishing messages have also become more sophisticated, meaning that users need even more information security awareness so that they can remain secure and safe while on the Internet. Information security awareness programmes provide users with knowledge of information security threats and solutions to mitigate or avoid the impact of security

[1] Social engineering refers to psychological manipulation of users into divulging confidential information. Phishing attack is a form of social engineering. Malware is a malicious software designed to infiltrate and damage devices without users' consent.

attacks (Hassandoust and Techatassanasoontorn 2018). Despite technological developments, educating users so that they do not reveal their private information when they receive phishing messages and improve their protective security practices overall remains a significant research problem in the information security domain. This study contributes to this issue by investigating the effect of security awareness on users' information security protective behaviours in the context of phishing.

A carefully designed phishing email can trigger basic emotions that persuade individuals to comply with the disguised malicious request (Goel et al. 2017). For example, individuals may divulge their credentials to hackers if they fear losing something valuable (Kim and Kim 2013). Thus, a contextualised phishing email sent to an individual that is ostensibly from the bank s/he uses leverages fear by suggesting that the recipient will not be able to access her/his bank account unless s/he changes their banking credentials or information by clicking on a given Web link. Besides fear, phishing attacks can manipulate many other emotions related to psychological traits, such as curiosity, patriotism, friendship, authority, community and belongingness. However, few studies have experimentally investigated the influence of contextualisation or directly compared contextualised with non-contextualised phishing messages. The present study is built on Goel and colleagues' (2017) research examining how the framing of the content of a phishing message affects the susceptibility of individuals to phishing attempts. Further, we investigate if there is a discrepancy between how individuals believe they will react to phishing attempts and their actual reactions. We test these propositions by manipulating fraudulent email messages to appeal to two distinct desires among students in a tertiary institution: receiving a free iPad or finding out their academic results.

In addition to investigating whether individuals respond differently to phishing messages with different types of content, this study also examines whether these individual responses differ by demographic attributes. For example, information security practices of users, as well as their Internet attitudes and phishing practices, are known to vary by gender (Chou and Sun 2017; Goel et al. 2017; Wu 2014). Demographic factors are also known to affect users' perceived privacy risks and the extent of information sharing on social sites (Hajli and Lin 2016). Research in the U.S. and Korea suggests that information security practices will vary based on users' culture and the social hierarchy of men relative to women (Hovav and D'Arcy 2012; Turner and Monk-Turner 2007). Thus, in this study, we also examine whether males or females differed in their susceptibility to phishing messages with different types of content. Understanding which demographic groups are more susceptible to information security threats will help in the design and delivery of information security education programmes.

Drawing on the heuristic-systematic model and anchoring effects, this study tests the effects of contextualisation on individuals' susceptibility to phishing as well as the apparent discrepancy between individuals' perceived protective practices and their protective reactions. This study uses an online questionnaire to measure individuals' awareness and perceived protective practices, along with phishing campaigns to test individuals' protective reactions. The results may shed light on important factors that should be considered in promoting protective security practices and encouraging more discriminating responses to phishing attempts.

Theoretical Background – The Heuristic-Systematic Model and Anchoring Effect

In this section, we introduce the theoretical framework in which we set our research. Previous phishing studies have mostly focused on two areas: a) how individual susceptibility to phishing varies by individual attributes, such as cognitive limitations, personality traits, identity, and demographics; and b) how interventions such as training can decrease susceptibility to phishing (Goel et al. 2017). Researchers have found that if individuals are exposed to general scams, they can usually protect themselves by comprehending the nature of the scams. However, individuals are less able to defend themselves when they are exposed to sophisticated deception or contextualised messages. These findings reveal that heuristic modes would increase the individual's susceptibility to phishing scams and guide her/his reactions to email requests (Downs et al. 2006). For example, most Internet users are familiar with Amazon, as it is a reputable company, and they may have already given Amazon their personal information when they transact with it. So, if they receive a phishing email that claims to be from Amazon and it asks for their personal information, they would most probably provide the

information willingly (Downs et al. 2006). Halevi and her colleagues (2015) found that 63% of employees who received an email addressed to them individually that was purportedly from their company's IT manager would click on a link embedded in that email, as they judged it to come from a reliable source. Another study that applied principles of persuasion to design simulated phishing emails found that such messages were highly effective in that they increased the susceptibility of recipients to phishing (Wright et al. 2014).

Successful phishing attacks take advantage of the human willingness to make intuitive judgments based on initial impressions of the context. Although phishing messages include false information that an individual may notice with careful scrutiny, a well-designed phishing message activates motivations that push victims toward accepting the message (Goel et al. 2017). Countermeasures to reduce the vulnerability of individuals to phishing include learning designs based on learning science principles (Kumaraguru et al. 2007; Sheng et al. 2007) and games (Arachchilage and Love 2013), as well as browser add-ons and toolbars (Wu et al. 2006).

The prior research on individual responses to phishing and phishing countermeasures discussed above points to the need to focus on how individuals make judgements about messages they receive. According to the heuristic-systematic model (HSM), individuals apply a combination of heuristic (quick) and systematic (deliberate) processing models to make judgements (Chen and Chaiken 1999). When individuals are engaged in the heuristic processing mode, they rely on judgmental and cognitive shortcuts that lead to quick decisions based on their immediate emotion; however, these decisions are subject to cognitive biases. On the other hand, when individuals are engaged in the systematic processing mode, they attentively inspect information and deal with messages analytically (Chaiken 1987; Chen and Chaiken 1999). HSM argues that individuals tend to choose actions that need less effort; thus, they use the heuristic processing mode more often than the effortful systematic processing mode. "Sufficiency threshold" is a critical concept in HSM and refers to the acceptable level of confidence an individual has in her/his judgement (Eagly and Chaiken 1993). Thus, individuals continue processing a message until they are confident that they have exceeded the sufficiency threshold. Individuals using heuristic processing stop processing information once they reach their sufficiency threshold. If they do not reach it, they will continue their decision-making by using systematic processing until they reach their sufficiency threshold. According to HSM, individuals adjust their sufficiency threshold based on contextual factors, such as the importance of the decision, purported authority figures involved (e.g., school administrators and bank officials), and time pressures. The presence of any of these contextual factors may lead individuals to lower their sufficiency threshold so that they can use only heuristics processing to make decisions. In the phishing scenario, attackers succeed if they can reduce the sufficiency threshold of the recipients of phishing messages; in this way, recipients do not shift to systematic processing when judging the validity of a phishing message, using heuristic processing to do so quickly and inaccurately (Luo et al. 2013). One way of lowering the sufficiency threshold of recipients is to contextualise the message to quickly trigger their motivational concerns. For example, course registration is important to college students, and a course-related message can create a sense of urgency that needs quick action (Goel et al. 2017).

A related heuristic that is relevant to the HSM is the anchoring effect, which is the disproportionate impact of initially presented values on individuals when they make decisions and judgments (Tversky and Kahneman 1974). Thus, individuals who are presented with a particular parameter or value make insufficient adjustments when making their final decision. Individuals who are exposed to a higher anchor make more insufficient adjustments downward (Tversky and Kahneman 1974). This bias can be considered an outcome of the arduous adjustment processes that are insufficient and based on an initially presented parameter (Epley and Gilovich 2001; Tversky and Kahneman 1974). In a decision-making process, anchoring effects are stronger when the source of the initial value is more ambiguous, less familiar, or more trustworthy (Furnham and Boo 2011). For example, a message from a trustworthy source such as a school administrator presents a strong anchor, and individuals may make insufficient adjustments from the information provided by that source when making a final decision.

While the need for research on security awareness among users has been suggested, most previous studies have focused on organisational security policies to deter information security threats (e.g., D'Arcy et al. 2009). According to previous information security studies, providing effective

information security awareness is considered the most cost-effective solution to encourage users in adopting more protective approaches (Hanus and Wu 2016). Previous researchers suggested the investigation of information security awareness in relation to protection and prevention strategies (Dinev and Hu 2007). Therefore, according to HSM, information security awareness can increase users' sufficiency threshold level, where users would pass the heuristic quick processing and get into the systematic deliberate processing in their judgements. In addition, knowledgeable users are less impacted by presented anchors (Wilson et al. 1996). Forewarnings such as training programmes are an effective way to decrease the anchoring effects and heuristics judgments. It should be considered that anchoring effects can be diminished, but not fully eliminated even with forewarnings, incentives and training programmes (Tversky and Kahneman 1974; Wilson et al. 1996). Previous studies suggested including users' information security awareness in information security models in order to better examine users' information security awareness intentions in relation to their security protective practices (Hanus and Wu 2016). Moreover, the user's self-perception about their information security awareness is another aspect of information security awareness. Users' lack of awareness is considered the main issue to cause their vulnerability against security threats. Previous studies argue that users' lack of awareness of security best practices is a significant reason for risky security reactions and their consequences (Haeussinger and Kranz 2017; Siponen 2000). Although the significance of users' phishing awareness has been mostly recognised, recent research indicates that awareness remains a substantial topic and that most users lack an awareness of phishing issues and procedures (Lim et al. 2010; Goel et al 2017). As a result, it may be inferred that increasing users' levels of information security or phishing awareness would diminish users' anchoring effects and increase their sufficiency level to reach systematic processing for judgement as well as minimise the likelihood of risky information security behaviour, and enhance the efficiency of protective security techniques and countermeasures in workplaces and personal lives (Haeussinger and Kranz 2017).

The sufficiency threshold of individuals is also affected by their personal attributes such as their gender and personality, which consequently impacts their heuristic and systematic decision-making processes. For example, users who score highly in agreeableness and conscientiousness are more susceptible to anchoring effects and more inclined to use heuristics to make quick judgements (Eroglu and Croxton, 2010). Demographic characteristics (e.g., gender, age, and education level) also influence phishing susceptibility (e.g., Flores et al. 2015; Halevi et al. 2013; 2015; Jagatic et al. 2007; Sheng et al. 2010). They found that women were more susceptible to phishing than men, and individuals aged 18 to 25 years old formed the most susceptible age group (Sheng et al. 2010). There is a significant difference between female and male users in relation to their information security privacy concerns and sharing their personal information in social sites (Chou and Sun 2017). It is thought that gender may be related to differences in users' perceptions and utilisation of the Internet (Wu 2014). In addition, gender differences exist in terms of online privacy protection practices and privacy importance (Chai et al. 2009). A previous study validated the role of gender in perceived control of information and perceived privacy risks on college students' attitudes toward information sharing on social sites (Hajli and Lin 2016). Goel and colleagues (2017) found that female students are more likely than male students to open a phishing message but not necessarily click on the malicious links. On the other hand, Flores and colleagues (2015) investigated individuals' personal and cultural determinants of phishing. However, they did not report a significant correlation between individuals' demographic characteristics (age and gender) and phishing behaviours.

Research Model and Hypothesis Development

Most previous studies focused on individuals' susceptibility to generic phishing messages without contextualisation. Contextualising messages increases the effectiveness of phishing. Phishing messages designed for a particular group of users will be effective if users identify group-relevant concerns and provoke particular emotions that trigger the desired response (Goel et al. 2017; Luo et al. 2013). In addition, studies comparing users' perception and their actual reactions to phishing attempts are lacking. Drawing on HSM and anchoring effect, contextualised phishing attacks make users more likely to engage in heuristic processing and repress their systematic processing, leading to the successful phishing attacks. Previous researchers argued that contextualising a message to quickly trigger users'

motivational concerns in a context specific to her/him would reduce the sufficiency threshold, encourage heuristic processing, and avoid the careful scrutiny of the message (Luo et al. 2013). For example, an email from a university support centre or administration office that is considered a trustworthy source presents a strong anchor, which can create a sense of urgency for quick action. Students who receive such messages may make insufficient adjustments and judgments based on the initially presented parameter of the reliable source. If there is a high anchor such as a reliable email sender, more heuristic processing will occur, and judgments will be made quickly. On the other hand, when initial values or parameters are too extreme, individuals ignore the values or question their validity, leading to a smaller anchoring effect being generated (Wegener et al. 2001). For example, a message which tells the recipient they have won an expensive device (such as an iPad mini) may seem too good to be true; thus, its anchoring effect will be minor, and the recipient will engage in less heuristic processing. Therefore, we hypothesise:

H1: Contextualised email messages that relate to a recipient's specific concerns increase vulnerability to phishing compared to non-contextualised email messages in relation to general concerns.

Another factor that is likely to influence the heuristic, systematic processing or anchoring effects in the context of phishing, is users' awareness level. Heuristic processing as a quick procedure mostly relies on judgmental rules and cognitive shortcuts that would likely cause risky reactions. On the other hand, systematic processing that contains careful scrutiny of information and analytical viewing of the messages would likely lead to protective reactions. Users need to be aware of security threats such as phishing and also need to be aware of countermeasures that could be performed against such threats. Users' threat awareness can enhance their protective reactions and minimise their risky approach against information security threats (Hanus and Wu 2016). Users' awareness regarding phishing threats and suggested countermeasures would likely increase their sufficiency threshold that lead them to pass the quick heuristic judgment process and reach the systematic mode. By decreasing the anchoring effect and reaching the systematic process stage, users would deliberately analyse the phishing messages, which is likely to improve their protective security reactions. According to previous studies, knowledgeable users with high expertise are less impacted by presented anchors and less uncertain in making relevant decisions (Wilson et al. 1996). Forewarnings such as training programmes are an effective way to decrease the anchoring effects, which leads to less heuristic quick judgments and more systematic deliberate decisions. Thus, we hypothesise:

H2: Users' phishing awareness positively influences their perceived protective practices and reactions.

Both users' sufficiency thresholds and their information security practices vary by gender (Chou and Sun 2017; Goel, Williams and Dincelli 2017). Thus, this study examines how phishing susceptibility varies across gender. Previous studies have suggested that female users are more susceptible to phishing than male users (e.g., Halevi et al. 2015; Jagatic et al. 2007). This could be because females and males have different information security reactions (Flores et al. 2015; Halevi et al. 2013) and different levels of willingness to engage in information security protective reactions (Lwin et al. 2012). There is also an apparent gender gap on information security awareness and Internet usage. For instance, male students have greater Internet skills, a higher level of Internet experience, and more familiarity with Internet threats, while female students have a less positive attitude towards the Internet and experience more Internet anxieties (e.g., Hu et al. 2012; Sun et al. 2016). There is also a significant difference between female and male users in relation to their information security privacy concerns and the extent to which they share their personal information on social media sites (Chou and Sun 2017). According to HSM, less expertise and higher Internet anxiety would decrease the sufficiency threshold, thus users are most likely make their judgement in the heuristic quick mode before reaching the systematic deliberate mode. Personality characteristics are also related to anchoring, in that users with high agreeableness and low extraversion are more vulnerable to the anchoring effect (Eroglu and Croxton, 2010). However, females score significantly higher on both agreeableness and extraversion than males (Goodwin & Gotlib, 2004). We hypothesise that:

H3: Female users are more vulnerable to phishing than male users.

Previous research stated that students in higher education are technologically literate but possess little knowledge to help them protect their information and assets (Kim 2014). Another study reported a

conflicting result between users' beliefs about information security and their information security reactions. For example, users believe that they can protect their computers from hackers, while they are not familiar with different types of security threats such as phishing, and countermeasures (e.g., installing a firewall) (Stanciu and Tinca 2016). Skillful information security users might be good at handling some technical issues, but they still fall victim to online safety incidents (Chou and Sun 2017). Users may be competent in technical skills that give them self-confidence in their protective reactions. On the other hand, according to HSM and anchoring effects, users with higher IT literacy present more self-confidence in their security reactions, which along with well-designed phishing messages would lower their sufficiency threshold, increase their anchoring effects and cause them to respond in heuristic processing mode and overlook the risks associated with phishing messages. In addition, industry best practices as well as academic studies show there is a discrepancy between users' perceived level of information security and their actual security reactions (Stanciu and Tinca 2016). Therefore, we presume the following hypothesis:

H4: Users express confidence in their perceived phishing practices which conflicts with their actual phishing reactions.

Research Design

To test the hypotheses, simulated phishing emails were sent to a sample of students in a tertiary institution. An academic setting has been used for this study because students often fall victim to similar online threats, and they fit in the age bracket of most susceptible to phishing threats (Johnston and Warkentin 2010). Although phishing experiments arguably contravene informed consent requirements and involve deception, these experiments can be conducted ethically if risks are minimised, privacy and confidentiality are protected, potential participants have an opportunity to opt in/out to the research before it begins, and subjects are debriefed after their participation ends (Resnik and Finn 2018).

Thus, potential participants received an email including brief explanations about this information security research along with the attached participants' information sheet and consent form, and those who wished to participate in the study signed the consent form and sent it back (through email or hand over) to the researchers. Individuals who did not want to participate in this research were excluded from the study. The remaining participants were sent simulated phishing emails to evaluate how they would respond to them. The phishing emails were designed to test the effects of contextualisation in two ways. First, we varied the content of the message so that it could be relevant specifically to tertiary students (e.g., obtaining their course results) or to anyone (e.g., winning an iPad mini). Second, we characterised the message sender as being from within the college/university (e.g., student support manager) or outside the college/university (e.g., the Apple research team). We used Gophish, an open-source phishing framework to run the study. For the simulated phishing email, the sender's name appeared as 'college admin'; however, the email address did not have a university domain, but instead was a personal Gmail address. In addition, there was a typo in the sender's email address (***addmin@gmail.com). The simulated phishing email also contained three misspellings such as 'attendence', a URL that was redirected to another page, and the wrong domain for the sender's email address was '@***.com' instead of '@***.ac.nz'.

We debriefed the participants after the event. Debriefing in a phishing experiment has the potential of having a long-lasting positive impact, if debriefing is structured in such a way that the subject learns how to avoid being a victim of future real phishing attacks (Finn and Jakobsson 2007). Upon completion of the experiment, students received a debriefing email informing them about the purpose of study, how phishing works and advice about how to avoid phishing attempts.

Once their responses to the phishing attempt had been recorded, an online survey was conducted. The measurement items of the survey have been validated in previous studies (Bailey et al. 2008; Stanciu and Tinca 2016). In the first section of the survey, the participants were asked to provide demographic information. In the second section, they were asked to indicate their awareness and familiarity (scale 1 to 7) with security threats such as phishing. In the third section, participants were asked to rate their perception of their information security practices on a five-point Likert scale.

The questionnaire was refined in two stages: pre-test and pilot study (Straub et al. 2004). The pilot study had 35 respondents and the findings indicated that there were no major difficulties in understanding the questionnaire items and instructions. The data collection process was conducted for five weeks during July - August 2018. In total, we sent the survey to 550 students and received 293 responses. After removing incomplete responses, 269 responses remained.

Data Analysis and Findings

The demographic profile of respondents included information about their gender, age, level of study, and ethnicity. Out of 269 respondents, 51.3% were female students and 46.5% male students. The majority of the respondents (64.3%) were aged between 24 – 32 years old. Most of the respondents were from postgraduate degrees (88%), and 11.9% from undergraduate studies. Over 71% of the participants were Asian international students.

The findings revealed vast differences between message conditions in the rates at which the emails were opened, the links in the emails were clicked on and submit data rates (Table 1). For example, 63.9% of those who received the phishing email related to coursework submitted their credentials (e.g., college username and password), compared to only 3% for those who received the phishing email about winning an iPad. Similarly, only 9.3% of the respondents in the first group did not open the email, compared to 67% of those in the second group. These results suggest that highly contextualised emails capture recipients' attention, supporting Hypothesis 1. This hypothesis was tested with a chi-square test, which revealed a significant association between the contextualization of a phishing email message and the recipients' vulnerability to phishing (χ^2 (3) = 269.00, p = .000).

Table 1. Proportion of Respondents who Opened the Phishing Email, Clicked on the Link and Submitted Data

Phishing Email	% Did Not Open	% Open	% Clicked	% Submitted Data
Course Related	9.3%	19.3%	7.4%	63.9%
Winning iPad	67%	27.2%	2.9%	3%

To test Hypothesis 2, we examined the correlation between users' phishing awareness and their perceived protective practices. Table 2 below indicates a positive significant relationship (0.51**) between phishing awareness and perceived protective practices (p<0.05, one-tailed), supporting Hypothesis 2. These results suggest that greater phishing awareness is associated with a higher perception that the appropriate phishing security practices will be carried out. The results also indicate inverse relationships between users' phishing awareness and their actual phishing reactions (-0.76***, -0.13*). This finding suggests that individuals with higher levels of phishing awareness were less likely to engage in risky reactions, such as clicking on either type of phishing email.

Table 2. Correlations Between all Constructs

	Phishing awareness	Perceived phishing practices	Course-related phishing reaction	iPad mini phishing reaction
Phishing awareness	1			
Perceived phishing practices	0.51**	1		
Course-related phishing reaction	-0.76**	-0.43**	1	
iPad mini phishing reaction	-0.13*	-0.10*	0.14**	1

Note: **. Correlation is significant at the 0.01 level, *. Correlation is significant at the 0.05 level

To test Hypothesis 3, we tested users' phishing awareness, perceived protective practices and actual phishing reaction by gender (Table 3). First, we compared participants' phishing awareness based on their gender. The result was statistically significant with p = 0.000 (Table 3). Therefore, we reject the null hypothesis and conclude that phishing awareness among female students is significantly lower than male students.

Table 3. Respondents' Awareness of Phishing

		N	Mean	Std. Deviation	Std. Error Mean	t	Df	Sig. (2-tailed)
Gender	Female	135	3.30	2.10	.18	45.89	268	.000
	Male	128	3.45	2.05	.18			
Total Sample		269	3.35	2.06	.13	26.60	268	.000

Next, we examined participants' perceptions of how they would react to phishing attempts. This was captured in five questions in the survey on a 5-point Likert scale ('1=never', '2=rarely' '3=sometimes', '4=often' and '5=always'). Participants who 'never' or 'rarely' engaged in risky security behaviours were considered to have "protective practices", while those 'sometimes' or 'often' or 'always' engaged in risky behaviours, were considered to have "risky practices". Participants who engage in risky practices are at risk of being hacked, while participants who engage in protective practices are more likely to recognise the phishing threats and not fall victim to phishing attempts.

Table 4 presents the findings based on the mean for each gender (1 to 5) and the probability of perceived protective practices. The protective practices percentages indicate the percentage of participants (both male and female) who claimed they would engage in protective practices. Therefore, a higher percentage represents lower risk to the users as well as organisations that the participants engage with. The findings reveal that male participants believed they would engage in more protective practices than female participants, indicating that the latter group are more vulnerable to phishing.

Table 4. Participants' Perception on Their Phishing Practices

	Mean	t	Gender (Mean)		%Perceived protective practice
Context of messages			Female	Male	
If you received an email containing the logo and web address of your bank or one of your credit card companies requesting that you should verify information such as your date of birth, account number, address, etc., and the email was addressed to you personally – would you click on the link and provide the requested information?	2.43	29.57***	2.49	2.37	79.1%
If you received an email containing the logo and web address of your bank or one of your credit card companies requesting that you should verify information such as your date of birth, account number, address, etc., and the email was addressed to "Dear customer" – would you click on the link and provide the requested information?	2.69	33.80***	2.72	2.67	78.4%

Would you fill out an email form asking for personal financial information if the email appeared to be from a trusted site and was addressed to you personally?	2.34	28.87***	2.34	2.38	75.5%
If you received an email containing the logo and web address of your college/university requesting that you should verify information such as your name, student ID, date of birth, address, etc., and the email was addressed to you personally –would you click on the link and provide the requested information?	2.60	32.65***	2.67	2.55	65.1%
I click on email links or posts with touching winning messages such as winning an Apple iPad.	1.92	29.42***	1.94	1.87	81.4%

Third, to examine users' actual phishing reactions for Hypothesis 3, we tested the proportion of males and females who opened, clicked on the link, and submitted data for both message conditions. We found a main effect for gender: collapsing across both message conditions, females were more likely to open the email message, click on the malicious link and submit their credential data than males. We found significant gender differences in the rates at which the iPad mini and course registration emails were opened. Details are presented in Table 5. This hypothesis was tested with a chi-square test, which revealed a significant difference between female and male phishing reactions (X^2 (9) = 289.48, p = .000).

Table 5. Breakdown of the Phishing Results Based on Gender

	Context of Phishing Email	Mean	t	% Did Not Open	% Open	% Clicked	% Submitted Data
Female	Course Related	3.30	37.70***	3.7%	10.4%	3.7%	33.5%
	Winning iPad	1.48	23.21***	31.6%	14.9%	1.9%	1.9%
Male	Course Related	3.18	31.65***	5.6%	8.9%	3.7%	28.3%
	Winning iPad	1.35	25.09***	33.5%	12.3%	1.1%	0.7%

Hypothesis 4 proposed a discrepancy between users' perceptions of how they would react to phishing messages and their actual reactions. Based on the findings from the survey (Table 4) and the actual responses to phishing emails (Table 5), there is a significant gap between participants' perceived phishing practices and their actual phishing reactions for the context-specific course-related phishing messages: while 65.1% of the participants reported that they would engage in protective practices, 69.1% of them carried out a risky action (i.e. either clicking the link in the email, or submitting data). However, there was not much difference in the other message context, which offered a free iPad mini: 81.4% of the participants reported that they would carry out protective practices, and only 5.9% of them engaged in a risky action when they actually received the phishing email. Therefore, students' perceptions about their phishing practices is more in line with their actual phishing reaction in the non-contextualised messages. Hence, Hypothesis 4 was supported only for contextualised messages.

Discussion and Contributions

In this study, we investigated the impact of content and framing of phishing attempts on users' vulnerability; users' phishing awareness on their perceived protective practices as well as actual

phishing reactions by gender; and the difference between users' perceived phishing practices and their actual phishing reactions.

In support of Hypothesis 1, in line with findings of Goel and colleagues (2017), users were more susceptible to a highly contextualised message pertaining to course results than to another generic message of winning an iPad mini. Almost three-quarters (71.3%) of participants who opened the course related message, clicked on the simulated phishing link and 63.9% of them submitted their credential username and password. Therefore, the contextualised message channeled participants through the first two steps of the phishing process and led them to read the message, click on the embedded link and submit the data, which is consistent with the heuristic-systematic model (Eagly and Chaiken 1993). In the course related message, cues such as an important college matter and a credible sender can make a stronger anchoring effect that leads people to act without carefully deliberating on the outcome of their actions. The highly contextualised email may have deterred the initial scrutiny of the users' systematic processing system. Researchers suggest that best effective phishing messages would function on both the heuristic and systematic processing systems (Goel et al. 2017; Luo et al. 2013). The importance of checking the course final results may have lowered the sufficiency threshold in students and pushed them toward quick action, despite some spelling mistakes and the use of an incorrect college domain name.

Hypothesis 2 states that students' phishing threat awareness positively impacts their perceived protective practices and reactions. The results suggest that there is a positive significant relationship between students' phishing awareness level and their protective practices as well as an inverse relationship between users' awareness and their phishing reactions. Accordingly, the need for effective security awareness, robust solutions and training in regard to information security in order to improve users' protective behaviours is dramatically proved (Stanciu and Tinca 2016). Thus, students have to be trained in regard to this important issue. We infer that information security training is likely to result in more employable graduates who are better prepared for contemporary professional practice. Users who are aware of threats are also more engaged in protective practices (Hanus and Wu 2016). Therefore, effective security training and education programmes should take a systematic approach by making sure that they address the multiple dimensions of security awareness. Effective information security awareness and training programmes should lead to improvement in graduates' capability to exercise protective reactions. Training would improve users' awareness and increase their sufficiency threshold, which would equip them to pass the heuristic mode and better engage in systematic processes. Awareness may also lower the anchoring effect, leading knowledgeable users to more deliberate judgements, decisions and protective reactions. Additionally, it appears that such programmes should also pay more attention to educating users about the risks caused by security threats.

Hypothesis 3 states that students' vulnerabilities and practices change across different student populations based on gender. Individuals' differences such as gender affect their performance, especially the cognitive processing of the judgmental decisions (Brandstätter 1993). The findings of the present study are in line with previous studies suggesting female users are more susceptible to phishing than male users. Previous studies found that before training, female users were more likely to click on the simulated phishing links and enter their information, which was mostly due to lack of technical experience and skills (e.g., Flores et al. 2015; Sheng et al. 2010). Researchers also reported that training reduced female users' tendency to enter information into phishing links by 40% (Sheng et al. 2010). Therefore, this variation can be bridged by providing customised training in order to improve the security awareness and protective reactions among users. Users' demographic characteristics are related to the anchoring effect and female users with higher agreeableness, and lower extraversion are more vulnerable to the anchoring effects. Findings revealed that female users reported lower expertise than males. According to HSM, less expertise and higher Internet anxiety would decrease the sufficiency threshold; thus female users may make their judgements in the heuristic quick mode before reaching the systematic deliberate process. Although we can make no assumptions about why these gender differences exist, any information security intervention strategy should consider them.

Beyond findings from Goel and colleagues (2017), hypothesis 4 of this study suggests that there is a big discrepancy between students' perceived phishing practices and their actual reactions to contextualised phishing messages. This hypothesis has been supported for highly contextualised

messages like course-related emails. Our findings revealed that students' perceived phishing practices through survey questions were in line with their actual phishing reactions in iPad mini context. Students were less susceptible to the phishing message geared toward free goods (an iPad mini) than for course-related messages. Perhaps these types of messages were not as believable, or students are quite familiar with free gift/winning phishing messages due to the dramatic increase in these types of messages. It seems that the deception of offering free goods does not lower the sufficiency threshold in students or cause them to pass the heuristic processing mode to reach the systematic processing system and analyse the risks associated with phishing emails. On the other hand, students reported high confidence in their perceived phishing practices which conflicted with their phishing reactions in the course related context. Drawing on HSM and anchoring effects, the deception of course -elated messages from reliable sources would lower users' sufficiency threshold and higher anchoring effects that lead them to make quick uncertain judgments in the heuristic mode.

This study provides important theoretical contributions to the information security domain. It establishes that contextual factors modify the effectiveness of phishing attempts. Heuristics would likely reduce rational logic processes and increase vulnerability to fraudulent messages. The findings of this study offer support to the heuristic-systematic processing model (HSM) and anchoring effects. A contextualised message from a reliable source may likely prompt individuals to act quickly without carefully considering the possible consequences of the action. Contextualised social engineering threats such as emails to students related to their academic results, may lead them to overlook cues of deception that they might normally catch in non-contextualised messages. Although initial suspicion causes recipients to more systematically process a message, the contextualised message from a strong, trustworthy source as an anchor would likely convince them that the message is legitimate. The survey results support this assertion by showing that respondents who clicked on the embedded link were suspicious of the email but clicked on the link, nonetheless. Perhaps the emotion elicited by the message as well as a strong anchor lowered the user's sufficiency threshold, thus influencing their appraisal of or their response to the legitimacy of the message.

Based on the overall findings of this study, in order to improve the impact of information security training, we contend that it is necessary to provide highly focused and contextualised awareness training (e.g., workshops, campaigns) targeted to different audiences. Given that students take emails from school administration and lecturers seriously, such interventions may provide students with more effective ways to distinguish phishing emails from legitimate emails. There are several ways to do so such as: checking that emails are from the school domain; understanding the importance of verifying emails, especially those that require credential information; and providing students with a procedure to verify the authenticity of messages either by web or phone. Students should also be educated in ways to identify the legitimacy of messages. In order to make contextualised strategies, the individuals' demographic characteristics should be taken into account to counteract user vulnerabilities (Goel et al. 2017). Training improves users' phishing susceptibility through seeking ways to raise their sufficiency threshold and lower anchoring affects, to stop heuristic processing, which subsequently increases the chance of systematic processing of messages.

We suggest it is highly important that higher education institutions not only develop security training programmes, but students' enrollment in such training, their security awareness as well as their actual security practices (e.g., through utilising phishing campaigns) should be monitored regularly. In order to prepare and motivate students to build up their security awareness level appropriately, instructors should integrate learning activities showing how to recognise the security threats such as phishing, how to react and report these threats and what are the magnitude and cost of these threat issues. In addition, students should be educated on what to do after falling victim to a security threat. Over-reliance on technical skill/knowledge for protection is common but unsafe. We consider this an important issue in a world increasingly being harmed by malicious internet practices. Graduates entering employment require a high level of security awareness and the skills to function online in a defensive manner, to protect both themselves and the organisations for which they work.

Limitations and Future Research

The present study was conducted in one higher education institution, in New Zealand, so its generalisability is limited, and users with different cultures from different countries may behave differently regarding phishing messages (Flores et al. 2015). This study focuses on general phishing attacks through emails and does not investigate users' practices through spear phishing or phishing via online social media platforms. Future research should examine the influence of contextualised messages to these other forms of phishing. We sent both types of emails to the same sample of students, so their responses to the later email (winning an iPad mini) may be influenced by their response to the first email (course-related). For a future study, separate samples are recommended to receive different phishing emails. We applied only two frames for the phishing emails. However, comparisons between these two scenarios provide interesting insights into the influence of framing and contextualisation. Further studies can expand on our findings and investigate the effects of several different scenarios in an experimental setting. In addition, future research can investigate the factors impacting anchoring effects in order to decrease the vulnerability to phishing attempts.

Conclusions

We tested the proposition that successful phishing attacks take advantage of internet users by reducing the sufficiency threshold, strengthening anchoring effects and luring the recipients to quickly and intuitively judge the validity of the message based on initial impressions of the immediate context. We also investigated the premise that susceptibility to phishing is significantly associated with the contextual setting of a phishing message through an experiment with emails framed based on the proposed hypotheses to evoke user reactions. We also found that phishing awareness is associated with users' protective practices and reactions related to phishing. Our findings revealed that the different demographics were associated with susceptibility to phishing. Therefore, the study suggests the need for context-based and targeted education based on demographic features (e.g., gender). We also tested the assertion that there is a discrepancy between users' perception on their phishing practices and their actual phishing reactions. We found that the there is a big gap between users' perception and their actual reaction in contextualised phishing message, while not much difference of such perception and reaction exists in non-contextualised general message.

Acknowledgement

We acknowledge InternetNZ, who provided funding support for this paper.

References

Arachchilage, N. A. G., & Love, S. 2013. "A game design framework for avoiding phishing attacks," *Computers in Human Behavior* (*29*:3), pp. 706-714.

Bailey, J.L., Mitchell, R.B. and Jensen, B.K. 2008. "Analysis of student vulnerabilities to phishing," *in Proceeding of AMCIS,* pp. 271-282.

Brandstätter, H. 1993. "Should economic psychology care about personality structure?," *Journal of Economic Psychology* (14:3), pp. 473–494.

Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H.R. and Upadhyaya, S.J., 2009. "Internet and online information privacy: An exploratory study of preteens and early teens," *IEEE Transactions on Professional Communication* (52:2), pp.167-182.

Chaiken, S. (1987). "The heuristic model of persuasion," in M. P. Zanna, J. M. Olson, and C. P. Herman (Eds.), *Social influence: The Ontario symposium* (5), pp. 3-39. Hillsdale, NJ: Lawrance Erlbaum Associates.

Chou, H.L. and Sun, J.C.Y. 2017. "The moderating roles of gender and social norms on the relationship between protection motivation and risky online behavior among in-service teachers," *Computers & Education* (*112*), pp. 83-96.

Chen, S., and Chaiken, S. 1999. "The heuristic-systematic model in its broader context," in S. Chaiken and Y. Trope (Eds.), *Dual-process theories in social and cognitive psychology,* pp. 73-96. New York: Guilford.

Dinev, T. and Hu, Q. 2007. "The centrality of awareness in the formation of user behavioral intention toward protective information technologies," *Journal of the Association for Information Systems* (8:7), pp. 386-408.

Downs, J.S., Holbrook, M.B. and Cranor, L.F. 2006. "Decision strategies and susceptibility to phishing," in *Proceedings of the second symposium on Usable privacy and security*, ACM, July, pp. 79-90.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79-98.

Eagly, A. H., and Chaiken, S. 1993. *The psychology of attitudes*, Fort Worth, TX: Harcourt.

Epley, N. and Gilovich, T. 2001. "Putting adjustment back into the anchoring and adjustment heuristic: differential processing of self-generated and experimenter-provided anchors," *Psychological Science* (12:5), pp. 391–396.

Eroglu, C. and Croxton, K.L. 2010. "Biases in judgmental adjustments of statistical forecasts: the role of individual differences," *International Journal of Forecasting* (26:1), pp.116–133.

Finn, P. R., and Jakobsson, M. 2007. "Designing ethical phishing experiments," *IEEE Technology and Society* (26:1), pp. 46–58.

Flores, W. R., Holm, H., Nohlberg, M., and Ekstedt, M. 2015. "Investigating personal determinants of phishing and the effect of national culture," *Information & Computer Security* (23:2), pp. 178-199.

Furnham, A. and Boo, H.C. 2011. "A literature review of the anchoring effect," *The journal of socio-economics* (40:1), pp.35-42.

Goel, S., Williams, K. and Dincelli, E. 2017. "Got phished? Internet security and human vulnerability," *Journal of the Association for Information Systems* (18:1), pp. 22-44.

Goodwin, R. D., & Gotlib, I. H. (2004). "Gender differences in depression: the role of personality factors," *Psychiatry Research*, (126:2), pp. 135-142.

Grover, M., Reinicke, B. and Cummings, J. 2016. "How secure is education in Information Technology? A method for evaluating security education in IT," *Information Systems Education Journal* (14:3), pp. 29-44.

Haeussinger, F. and Kranz, J. 2017. "Antecedents of employees' information security awareness – review, synthesis, and directions for future research," in *Proceedings of the 25th European Conference on Information Systems (ECIS),* Guimarães, Portugal, pp. 12-32.

Hajli, N. and Lin, X., 2016. "Exploring the security of information sharing on social networking sites: The role of perceived control of information," *Journal of Business Ethics* (133:1), pp.111-123.

Halevi, T., Lewis, J., and Memon, N. 2013. *Phishing, personality traits and Facebook,* arXiv preprint arXiv:1301.7643v2.

Halevi, T., Memon, N., and Nov, O. 2015. Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks.

Hanus, B., and Wu, Y.A. 2016. "Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective," *Information Systems Management* (33:1), pp. 2-16.

Hassandoust, F. and Techatassanasoontorn, A., 2018. "Understanding Users' Information Security Awareness and Intentions: A full Nomology of Protection Motivation Theory," in *Proceedings of the 22nd Pacific Asia Conference on Information Systems.*

Hovav, A. and D'Arcy, J., 2012. "Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea," *Information & Management* (49:2), pp.99-110.

Hu, T., Zhang, X., Dai, H. and Zhang, P. 2012. "An examination of gender differences among college students in their usage perceptions of the internet," *Education and Information Technologies* (17:3), pp. 315-330.

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

Johnston, A. C., and Warkentin, M. 2010. "Fear appeals and information security behaviors: An emprical study," *MIS Quarterly* (34:3), pp. 549-566.

Kim, B.E. 2014. "Recommendations for information security awareness training for college students," *Information Management & Computer Security* (22:1), pp. 115-126.

Kim, D., and Kim, J. H. 2013. "Understanding persuasive elements in phishing e-mails: A categorical content and semantic network analysis," *Online Information Review* (37:6), pp. 835-850.

Kiss, G. and Szasz, A., 2016, November. "Analysing of the information security awareness of the economic information technology students," in *Computational Intelligence and Informatics (CINTI), 2016 IEEE 17th International Symposium on* (pp. 000213-000218). IEEE.

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F., and Hong, J. 2007. "Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer," in *Proceedings of the Anti-phishing Working Groups 2nd Annual eCrime Researchers Summit,* pp. 70-81.

Lim, J. S., Ahmad, A., and Maynard, S. 2010. "Embedding Information Security Culture Emerging Concerns and Challenges," in *Proceedings of the 15th Pacific Asia Conference on Information Systems (PACIS),* Australia, Brisbane.

Luo, X., Zhang, W., Burd, S., and Seazzu, A. 2013. "Investigating phishing victimization with the heuristic-systematic model: A theoretical framework and an exploration," *Computers & Security*, (38), pp. 28-38.

Lwin, M. O., Li, B., and Ang, R. P. 2012. "Stop bugging me: An examination of adolescents' protection behavior against online harassment," *Journal of Adolescence* (35:1), pp. 31-41.

Mitnick, K. D., & Simon, W. L. 2002. *The art of deception: Controlling the human element of security*, New York: John Wiley & Sons.

Ndiege, J.R. and Okello, G.O., 2018. "Information security awareness amongst students joining higher academic institutions in developing countries: Evidence from Kenya," *The African Journal of Information Systems* (10:3), pp. 204-222.

Resnik, D. B., and Finn, P. R. 2018. "Ethics and Phishing Experiments," *Science and engineering ethics* (24:4), pp. 1241-1252.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., and Downs, J. 2010, April. "Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions," *in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, pp. 373-382).

Siponen, M. 2000. "A conceptual foundation for organizational information security awareness," *Information Management and Computer* Security (8:1), pp. 31-41.

Stanciu, V., and Tinca, A. 2016. "Students' awareness on information security between own perception and reality–an empirical study*," Accounting and Management Information Systems* (15:1), pp. 112-130.

Sun, J.C.Y., Yu, S.J., Lin, S.S. and Tseng, S.S. 2016. "The mediating effect of anti-phishing self-efficacy between college students' internet self-efficacy and anti-phishing behavior and gender difference," *Computers in Human Behavior* (59*)*, pp. 249-257.

Turner, C.G. and Monk-Turner, E., 2007. "Gender differences in occupational status in the South Korean labor market: 1988-1998," *International journal of social economics* (34:8), pp.554-565.

Tversky, A. and Kahneman, D., 1974. "Judgment under uncertainty: heuristics and biases," Science (185), pp. 1124–1131.

Wegener, D.T., Petty, R.E., Detweiler-Bedell, B. and Jarvis, W.B.G. 2001. "Implications of attitude change theories for numerical anchoring: anchor plausibility and the limits of anchor effectiveness," *Journal of Experimental Social Psychology* (37:1), pp. 62–69.

Wilson, T.D., Houston, C.E., Etling, K.M. and Brekke, N. 1996. "A new look at anchoring effects: basic anchoring and its antecedents," *Journal of Experimental Psychology: General* (125:4), pp. 387–402.

Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., and Marett, K. 2014. "Influence techniques in phishing attacks: An examination of vulnerability and resistance," *Information Systems Research* (25:2), pp. 385-400.

Wu, J. Y. 2014. "Gender differences in online reading engagement, metacognitive strategies, navigation skills and reading literacy," *Journal of Computer Assisted Learning* (30:3), pp. 252-271.

Wu, M., Miller, R. C., and Garfinkel, S. L. 2006. "Do security toolbars actually prevent phishing attacks?," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 601-610).