The Role of Contextualization in Users' Vulnerability to Phishing Attempts

Farkhondeh Hassandoust
Auckland University of Technology
New Zealand
Ferry@aut.ac.nz

Harminder Singh
Auckland University of Technology
New Zealand

Jocelyn Williams
Manukau Institute of Technology
New Zealand

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 the anchoring effect, this study examines how the contextualization of phishing messages, in the form of modifications to their framing and content, affects individuals' susceptibility to phishing. This study also investigates if there is a discrepancy between the way 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.

Keywords: word; information security, phishing, contextualization, heuristic-systematic processing

1 Introduction

With the spread of technology and the global reach of the internet, cybercriminal activities are occurring more frequently (Nouh, Nurse, Webb, & Goldsmith, 2019). For example, New Zealand's national Computer Emergency Response Team (CERT NZ) announced that the highest number of cybersecurity incidents ever were reported in the third quarter of 2019, with a 27% increase in reports of phishing and credential harvesting (CERTNZ, 2019). Phishing, a type of social engineering attack carried out by hackers who send spoof emails to trick individuals into giving up sensitive information, is a particular worry because it enables hackers to circumvent information security countermeasures.

Hackers who engage in phishing manipulate individuals into revealing their confidential information by exploiting their motives, habits and cognitive biases (Mitnick & Simon, 2003). Although Internet users have become more aware of them, 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 programs provide users with knowledge of information security threats and

solutions to mitigate or avoid the impact of security attacks (Hassandoust & Techatassanasoontorn, 2020). Despite the increased number of such programs, convincing individuals not to reveal their private information when they receive phishing messages and to improve their protective security practices overall remains a significant research challenge (Hassandoust & Techatassanasoontorn, 2020).

Although phishing has attracted a great deal of academic and practitioner attention, it remains a major IT security problem. One reason for this is that phishing emails can trigger emotions that over-ride individuals' training and awareness so that they comply with the disguised malicious request (Goel, Williams, & Dincelli, 2017). These emotions include fear, curiosity, patriotism, friendship, authority, community, and belongingness. For example, phishing practitioners may scare potential victims into divulging their private credentials by implying that if they do not do so, they will lose something valuable (Kim & Kim, 2013). A common scenario is in the banking context: customers are sent contextualized[1] phishing emails that are ostensibly from the bank they use. These phishing attacks leverage 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 URL.

Hence, it is important to consider the phishing attack context when interpreting recipients' responses, because the context can elicit certain emotions. However, few studies have investigated the influence of contextualization in phishing or compared the impact of contextualized against non-contextualized phishing messages. While Goel and his colleagues (2017) studied how the framing of a phishing message affects the susceptibility of message recipients to phishing attempts, less is understood about how this vulnerability interacts with receivers' attributes. We build on that study in three ways. First, we expand its theoretical explanation to include the role of anchoring. Second, we investigate if there is a discrepancy between how individuals believe they will react to phishing attempts and their actual reactions. Third, we examine if individuals' reactions to phishing are influenced by their prior experiences. We test these propositions by manipulating fraudulent email messages to appeal to two distinct motivations among tertiary students: receiving a free computing device or finding out their academic results.

While this study investigates whether individuals respond differently to phishing messages with different types of content, it also examines whether individual responses differ by demographic attributes. Understanding which demographic groups are more susceptible to information security threats will help in designing and delivering relevant education programs. For example, information security practices, as well as Internet attitudes and phishing practices, are known to vary by gender (Chou & Sun, 2017; Goel et al., 2017; Wu, 2014). Demographic factors also affect individuals' perception of their privacy risk and the extent of information sharing on social sites (Hajli & Lin, 2016). Research in the U.S. and Korea suggests that information security practices vary across cultures and the position of men relative to women in the social hierarchy (Hovav & D'Arcy, 2012; Turner & Monk-Turner, 2007). For instance, in South Korea, gender and age are associated with social status, meaning that older people and males retain a higher position in the social hierarchy.

[1] Contextualization may refer to adapting extent theories to account for relevant contextual conditions (Whetten, 2009). However, in this paper, contextualization means adapting phishing instruments to fit recipients' characteristics or background settings.

The next section describes the theoretical perspective of the heuristic-systematic model. Following that, prior research on phishing, contextualization and information security awareness is discussed. Our research model and hypotheses are then presented. This is followed by an explanation of the methodology, which comprised two phishing campaigns and an online questionnaire, and an analysis of the results. The paper concludes with a discussion of the findings and their implications for researchers and practitioners. The results shed light on factors that should be considered in promoting protective security practices and encouraging more prudent responses to phishing attempts.

2 Theoretical Background

The dominant assumption in information security research is that individuals are rational actors who deliberately plan their behaviours in advance and are aware of the benefits and costs of their responses (Dennis & Minas, 2018). While this assumption may hold true in some information security contexts, it is less appropriate for situations where individuals react automatically, such as in phishing attacks. Instead of using carefully deliberated actions, individuals' responses to phishing emails are immediate, reactive, nonconscious and automatic (Dennis & Minas, 2018). The next section describes a dual process theory related to such behaviours - the heuristic systematic model - and explains how it can be used to understand individuals' security behaviours as instant cognitive responses, instead of solely being the outcome of deliberate judgements.

2.1 The Heuristic-Systematic Model

Chen and Chaiken (1999, p. 74) argue that individuals apply a combination of heuristic (quick) and systematic (deliberate) processing models to make judgments:

> "Heuristic processing entails the activation and application of judgmental rules and 'heuristics' that are presumed to be learned and stored in memory…. Heuristic processing make[s] minimal cognitive demands on the perceiver" whereas "Systematic processing entails a relatively analytic and comprehensive treatment of judgment-relevant information…. Given its nature, systematic processing requires both cognitive ability and capacity".

Heuristic processing uses readily apparent cues embedded within a message, such as its source, format, and subject, to quickly generate an assessment of validity. On the other hand, systematic processing makes such an assessment by cautiously examining the information content in a message (Luo, Zhang, Burd, & Seazzu, 2013). When individuals use heuristic processing, they rely on judgmental and cognitive shortcuts that lead to quick decisions based on their immediate emotion/s; however, these decisions are subject to cognitive biases. On the other hand, individuals engaged in systematic processing inspect information attentively and deal with messages analytically (Chaiken, 1987; S. Chen & Chaiken, 1999).

This theory, referred to as the Heuristic-Systematic Model (HSM), argues that since individuals tend to choose actions that require less effort, they use the heuristic processing mode more often than the systematic processing mode. Information systems researchers have used the HSM to evaluate users' reactions and behaviours in various contexts (Hilligoss & Rieh, 2008; Wirth, Böcking, Karnowski, & Von Pape, 2007), including phishing (Goel et al., 2017; Luo et al., 2013). For example, Luo and his colleagues (2013) adopted HSM to investigate the psychological mechanism underlying the effectiveness of phishing attacks. They argued

that when systematic processing occurs, individuals' high-quality arguments lead to appropriate assessments of phishing messages. The question then arises as to when individuals move from one mode to the other. Since individuals are essentially satisficers (Simon, 1965), that is, they do not strive to make validity assessments with the highest accuracy or reliability, they stop processing when they think their assessments are good enough. The point at which they stop processing is referred to as the "sufficiency threshold" (Luo et al., 2013). The "sufficiency threshold" refers to the acceptable level of confidence an individual has in her/his judgment (Eagly & Chaiken, 1993). 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. These include the importance of the decision, the involvement of purported authority figures (e.g., school administrators and bank officials), social pressures, cognitive resources, their own skill levels, and time pressures. The presence of any of these contextual factors stresses a need for urgent action. They also act as cues that direct individuals towards the peripheral route of persuasion, instead of the central route, so that they do not focus on the content of the information being presented to them (Petty & Cacioppo, 1984). This, in turn, leads individuals to lower their sufficiency threshold so that they use only heuristics processing to make decisions (Chaiken, 1982). In the phishing scenario, attackers have a higher chance of convincing recipients of phishing messages to open them if they can reduce the recipients' sufficiency threshold. In this way, recipients do not shift to systematic processing when they receive a phishing message, using heuristic processing to quickly and inaccurately judge its validity (Luo et al., 2013). One way of lowering the sufficiency threshold of recipients is to contextualize the message to quickly trigger their motivational concerns in a context that seems important and inhibits them from inspecting the message. For example, registering for courses is important for college students, so receiving a message about course registration is likely to create a sense of urgency that needs quick action (Goel et al., 2017).

In some instances, heuristic and systematic processing modes can happen simultaneously (Luo et al., 2013). These conditions are when: 1) heuristic and systematic processing cause the same decision, and confidence in that decision would be higher than either process alone (i.e., the modes reinforce each other, thereby strengthening the decision); 2) heuristic processing may create an initial conclusion that biases the nature and scope of the systematic processing mode (i.e., biased short-cut actions); and 3) systematic processing may generate conclusions that overturn or limit those of heuristic processing mode (i.e., attenuation processing).

3 Literature Review

3.1 Phishing

Online social engineering attacks include phishing e-mails that spoof legitimate institutions in order to defraud users, and others that aim to commit advance-fee fraud. E-mail spoofing (phishing), the focus of our study, targets individual users as well as potentially bypassing the best technical security systems to gain access to an organization's critical information. One of the most well-known deceptive techniques in online communications (CERTNZ, 2019), email phishing involves credible-looking emails that are sent to individuals to fool them into

providing their sensitive personal information. Specific forms include spear phishing - malicious emails sent to a specific person, and whaling - phishing attacks targeting senior executives (Irwin, 2020; Pienta, Thatcher, & Johnston, 2020).

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 individuals' susceptibility to phishing (Goel et al., 2017). Researchers have found that individuals can usually protect themselves when they are exposed to social engineering attacks online because they know that Internet use has some inherent risk and they are familiar with how to manage such risks (Downs, Holbrook, & Cranor, 2006). However, they are less able to defend themselves when exposed to sophisticated deception or contextualized messages. These findings indicate that messages limiting individuals to heuristic processing would increase their susceptibility to phishing scams (Downs et al., 2006).

Most previous studies were based on theories which assumed that individuals consider their security intentions and behaviours deliberately. However, individuals confronted with phishing attacks are unlikely to follow that conceptualization and think carefully about the issue facing them (Dennis & Minas, 2018). Phishing messages include at least some false content that can usually be recognized with some amount of systematic processing. To improve the success rate of phishing attacks, hackers mislead their targeted victims into making a quick but incorrect validity assessment of the message. This demonstrates the link between heuristic processing modes and the nonconscious automatic cognition found in phishing victimization (Dennis & Minas, 2018; Luo et al., 2013).

The heuristic processing mode depends on available heuristic cues such as source credibility and catchy message content. 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 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 found that use of persuasion principles in the design of phishing emails was highly effective through increasing the susceptibility of recipients to phishing (Wright, Jensen, Thatcher, Dinger, & Marett, 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). However countermeasures including learning designs based on learning science principles (Kumaraguru et al., 2007; Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010) and games (Arachchilage & Love, 2013), as well as browser add-ons and toolbars (Wu, Miller, & Garfinkel, 2006) can be used to reduce the vulnerability of individuals to phishing. The research discussed above on individual responses to phishing and phishing countermeasures indicates a need to explore how individuals make judgments about messages they receive.

Studies on the behavioural aspects of phishing try to ascertain why phishing works and how it can be detected and prevented. This has been done by investigating the impact of email

recipients' individual attributes, and the attributes of the email itself (e.g., Anderson, Vance, Kirwan, Jenkins, & Eargle, 2016; Arachchilage, Love, & Beznosov, 2016; Wang, Li, & Rao, 2017; Wright et al., 2014). For example, Moody, Galletta, and Dunn (2017) used the Delphi method to determine the effect of personality and situational factors on individuals' susceptibility to phishing attacks. Most studies in this domain use theories such as protective motivation theory, routine activity theory and technology threat avoidance theory. The default assumption here is that individuals are engaged in systematic, theoretical reflection (Arachchilage & Love, 2014; Blythe, Petrie, & Clark, 2011; Jansen & Van Schaik, 2018; McElwee, Murphy, & Shelton, 2018). By using the lens of these theories, the previous studies empirically tested and tracked subjects' actual clicking behaviour. The challenge here is that responses to security threats do not take place after systematic reflection. While these theories can provide a framework for interpreting the cognition and behaviours of phishing email recipients, they cannot fully predict and interpret users' automatic cognition based on their reactive and immediate emotions, which are arguably a better fit with responses to phishing. Therefore, theories such as HSM are needed to evaluate individuals' immediate responses to phishing attacks. The table in Appendix A summarizes the objectives, theoretical background, and findings of the literature related to this domain.

3.2 Information security awareness

While it has been suggested that research on individuals' security awareness is needed, most previous studies have focused on organizational security policies to deter information security threats (D'Arcy, Hovav, & Galletta, 2009). This is because providing effective information security awareness is the most cost-effective way to encourage users to adopt more protective (Hanus & Wu, 2016) and preventive strategies (X. Chen, Chen, & Wu, 2018; Dinev & Hu, 2007). Prior research has suggested utilizing individuals' information security awareness to examine their intentions in relation to information security protective practices (Hanus & Wu, 2016).

From an HSM perspective, information security awareness can increase individuals' sufficiency threshold level, meaning that individuals would move beyond heuristic quick processing to systematic deliberate processing when making judgments about potential information security threats. In addition, activities to enhance individual alertness, such as training programs, are an effective way of decreasing heuristic-based judgments.

Individuals' lack of awareness is considered to be the main predictor of their vulnerability to security threats, by, for example, engaging in risky security behaviour (Haeussinger & Kranz, 2017; Siponen, 2000). Although the significance of individuals' phishing awareness has been mostly recognized, recent research indicates that awareness remains a substantial topic since most users lack awareness of phishing and how it occurs (Goel et al., 2017; Lim, Ahmad, Chang, & Maynard, 2010). As a result, it may be inferred that an increase in individuals' awareness of information security or phishing would increase their sufficiency level, so that they will be more likely to use systematic processing to make decisions about information security threats. This would minimize the likelihood of risky information security behaviour and enhance the efficacy of protective techniques and countermeasures in their workplaces and personal lives (Haeussinger & Kranz, 2017).

3.3 Individual Differences in Susceptibility to Phishing

Individuals' sufficiency threshold is also affected by their personal attributes such as age, gender, and personality, which consequently have an impact on their heuristic and systematic

decision-making processes. For example, users who score highly in agreeableness and conscientiousness are more inclined to use heuristics to make quick judgments (Eroglu & Croxton, 2010). The experiences, current contextualization, personality, culture and demographic characteristics of individuals have a profound impact on their behaviour (Dennis & Minas, 2018). Demographic characteristics (e.g., gender, age, education level and technical skills) also influence phishing susceptibility (Flores, Holm, Nohlberg, & Ekstedt, 2015; Halevi, Lewis, & Memon, 2013; Halevi et al., 2015; Jagatic, Johnson, Jakobsson, & Menczer, 2007; Sheng et al., 2010). Demographic aspects include characteristics such as gender and social identities inherited from ancestors, such as ethnicity (Dennis & Minas, 2018). Females and males differ significantly in relation to their information security privacy concerns and the sharing of personal information on social networking sites (Chou & Sun, 2017; Hajli & Lin, 2016). Gender may also be related to differences in individuals' perceptions and use of the Internet (Wu, 2014). Males have been found to be less concerned about unethical computer practices, such as using unlicensed programs (Beycioglu, 2009), and more likely to correctly recognize phishing and legitimate websites than females (Kumaraguru, Sheng, Acquisti, Cranor, & Hong, 2010). Similarly, Goel and his 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. The higher susceptibility of females to phishing may be due to their lack of technical experience (Sheng et al., 2010). However, Pattinson et al (2015) did not find significant correlations between individuals' demographic characteristics (age and gender) and phishing behaviours. They did find a significant positive relationship between age and security behaviour, indicating that older adults show safer behaviour. Flores and his colleagues (Flores et al., 2015) investigated individuals' personal and cultural determinants of phishing. They found phishing behaviour differs across Indian, Swedish and American employees from nine different firms.

4 Research Model and Hypothesis Development

The preceding sections described how phishing researchers have explored the impact of the contextualization of phishing emails, and individual differences on individual susceptibility to phishing. This paper uses a heuristic perspective to explain those findings, as well as explain the role of security awareness training as a possible preventive mechanism. In this section, we describe the hypotheses we will use to examine the validity of our theorizing.

4.1 Hypothesis 1: Trustworthiness as an anchor

Contextualized phishing attacks make individuals more likely to engage in heuristic processing and repress their systematic processing, leading to successful phishing attacks. Previous researchers argued that contextualizing a message to quickly trigger individuals' motivational concerns in a context specific to them would reduce their sufficiency threshold, encourage the use of heuristic processing, and avoid 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 can create a sense of urgency for quick action. Students who receive such messages may make insufficient adjustments and judgments based on the parameter of the reliable source initially presented. If the email sender is known to be a reliable source, heuristic processing will occur, and judgments will be made quickly.

We postulate that reliable sources act as anchors that affect individual decision-making. The anchoring effect is a cognitive bias that explains why individuals' behaviour and judgments

are impacted by the initial value, perspective or impression they receive (Epley & Gilovich, 2006). For example, Jacowitz and Kahneman (1995) found that participants gave higher estimates of the length of the Mississippi River after they first considered whether it is shorter or longer than 5000 miles than when they considered whether it is shorter or longer than 200 miles. The judgement influenced by an anchor can also be based on non-numeric values and information (Cohen & Reed, 2006; Esch, Schmitt, Redler, & Langner, 2009). For example, Iuga et al. (2016) examined whether the first three webpages that individuals saw during a phishing experiment influenced the zones that their participants inspected on the fourth webpage they saw. 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 & Boo, 2011; Iuga, Nurse, & Erola, 2016). For example, a message from a trustworthy source such as a school administrator presents a strong anchor, which lowers the individual's sufficiency threshold. Therefore, individuals do not proceed to systematic, deliberate processing when making their decision; instead, they use quick heuristic adjustments from the information provided by that source.

Thus, in the context of phishing, drawing on HSM and the anchoring effect, we infer that messages from reliable email senders, which are perceived to be strong anchors, will lead to greater heuristic processing 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, Petty, Detweiler-Bedell, & Jarvis, 2001). For example, a message which tells the recipient they have won an expensive computing device 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 hypothesize:

> *H1: Contextualized email messages from strong anchors increase the vulnerability of recipients to phishing compared to non-contextualized email messages.*

4.2 Hypothesis 2: Information security awareness

Another factor that is likely to influence the relative extent of heuristic versus systematic processing in the context of phishing is the individual's awareness of information security issues. These include phishing and the countermeasures that could be performed against phishing. Individuals with higher levels of threat awareness can enhance their protective reactions and minimize their risky responses to information security threats (Hanus & Wu, 2016). Knowledgeable users with high expertise are less affected and less uncertain in making relevant decisions (Wilson, Houston, Etling, & Brekke, 1996).

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, where individuals carefully scrutinize and analyse information, is likely to lead to protective reactions. Being aware of phishing and countermeasures to phishing would likely increase the sufficiency threshold of individuals, leading them to bypass the quick heuristic judgment process and use systematic processing. At this stage, individuals would deliberately analyse phishing messages, which is likely to improve their protective security reactions.

Activities that enhance individual alertness to information security attacks, such as training programs, are an effective way to increase individuals' knowledge, which leads to fewer quick heuristic judgments and more systematic deliberate decision-making. Thus, we hypothesize:

H2a: Users' phishing awareness positively influences their perceived protective practices.

H2b: Users' phishing awareness positively influences their phishing reactions.

4.3 Hypothesis 3: Prior experiences

Demographic characteristics and personality traits are associated with an individual's prior experience with information security threats. Drawing on the Big Five Model (personality traits are assumed to represent the basic structure behind all personality traits), if a person high in agreeableness had fallen victim to cybercrime previously, it is likely that heuristics associated with the prior bad experience would dominate the person's fundamental personality trait, when s/he is in a context that triggers cognitive heuristics based on that experience (Dennis & Minas, 2018). Individuals tend to use heuristics that are often motivated by proximity and vividness (Loewenstein, O'Donoghue, & Bhatia, 2015). Thus, prior bad experiences that are rather vivid, such as identity theft, are expected to outweigh personality traits, such as agreeableness (Dennis & Minas, 2018). Moreover, avoidance responses overcome appetitive responses (to reach for a presented stimulus), because humans have evolved to avoid danger (Kahneman, 2011). For example, an appetitive response can be compliance with a request, whether the request is to comply with an organization's security policies or react to a phishing message. Hence, based on an avoidance heuristic, a prior bad experience would often replace a set of good experiences. If the prior experience happened recently, then the associated avoidance heuristic with it would be even stronger. Therefore, we theorize the following proposition:

H3: Users with prior phishing experiences are less likely to fall for a phishing attack.

5 Research Design

Although phishing experiments arguably contravene informed consent requirements and involve deception, they can be conducted ethically if risks are minimized, 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 & Finn, 2018).

To test the hypotheses, simulated phishing emails were sent to a sample of students in a tertiary institution. The participants in this study were undergraduate and postgraduate students enrolled at a higher education institution in New Zealand. In this study, we used an education setting, as students are a frequent target of online attacks, and they fit in the age bracket of those most susceptible to phishing threats (Johnston & Warkentin, 2010) and are thus a suitable group for applied behavioural research on information security. All the students at the educational institution were sent an email that included a brief explanation about this information security research project, along with an information sheet and consent form. Key aspects such as the opt-out option and completely voluntary nature of participation have been clearly explained to the students. Those who wished to participate in the study signed the consent form and sent it back (through email or personal hand over) to the researchers. Individuals who did not want to participate in the research were excluded from the study. Consenting participants were sent simulated phishing emails to evaluate how they would respond to them. These were designed to test the effects of contextualization 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 characterized 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). An Apple-related email was used as a general context because some students had used "*Apple Educational Benefits/Pricing*" as a case study for a course before this research project, indicating that this topic interested them at that time.

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`'.

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. Debriefing in a phishing experiment has the potential to deliver a long-lasting positive impact, if it is structured in such a way that the subject learns how to avoid being a victim of future real phishing attacks (Jakobsson & Ratkiewicz, 2006).

The phishing responses were coded 1/2/3/4, where 1 represents that respondents did not open the email, 2 that respondents opened the email only, 3 that respondents opened the email and clicked the link, and 4 that respondents opened, clicked the link and submitted data. Once their responses to the phishing attempt had been recorded, an online survey was conducted in order to capture their perceptions on phishing messages. The survey measurement items had been validated in previous studies, as shown in Appendix B (Bailey, Mitchell, Robert, & Bradley, 2008; Dinev & Hu, 2007; Stanciu & Tinca, 2016; Wang, Li, & Rao, 2016). In the first section of the survey, participants were asked to provide their demographic information and in the second section, to indicate their awareness of and familiarity with (scale 1 to 9) security threats such as phishing. Individuals' overall prior experience of online security threats was assessed using six items, using yes/no responses for each. The ratings for each respondent on each item sum were summed to provide an overall score. In a third section, participants were asked to rate their perception of their information security practices on a five-point Likert scale. For perceived protective practices, the ratings for each respondent on each scenario were averaged to provide an overall score.

The survey questionnaire was refined in two stages: a pre-test and a pilot study (Straub, Boudreau, & Gefen, 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 over five weeks during July-August 2018. In total, we sent the survey to 550 students and received 293 responses. After removing incomplete responses, 269 valid responses remained.

6 Data Analysis and Findings

We used IBM SPSS for correlation and chi-square analysis to test the proposed hypotheses. The chi-square statistic is a non-parametric technique for analysing group differences when the dependent variable is measured at a categorical level (McHugh, 2013). The demographic attributes of participants that were collected included their gender, age, level of study, and ethnicity. Analysis showed that out of the 269 student respondents, 50.3% were female and

47.6% male. Most respondents (66%) were aged between 24 and 32 years old; most were studying for undergraduate degrees (69.9%), and 30.1% for postgraduate qualifications. 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, whether the links in the emails were clicked on, and submit data rates (Table 1). For example, 71.3% (63.9% + 7.4%, as shown in Table 1) of those who received the "course-related" phishing email engaged in risky behaviour[2] by either clicking on the malicious link or submitting their credentials (e.g., college username and password), compared to only 5.9% for those who received the "winning iPad" phishing email. Similarly, only 28.6% of the respondents in the "course-related" group showed safe behaviour through either not opening the email (9.3%) or simply opening the email without clicking on the link and then submitting confidential data (19.3%) compared to 94.2% of those in the "winning iPad" group. These results suggest that highly contextualized 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).

Type of Phishing Email[3]	Safe Behaviors		Risky Behaviors	
	% 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%

Table 1. Proportion of respondents who opened the phishing email, clicked on the link and submitted data

To test Hypotheses 2a and 2b, we examined the Pearson product-moment correlation coefficient between users' phishing awareness, their perceived protective practices and their actual phishing reactions. Table 2 below indicates a positive significant relationship (0.51**) between phishing awareness and perceived protective practices ($p<0.01$, one-tailed), supporting Hypothesis 2a. 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*), which supports Hypothesis 2b. This finding suggests that individuals with higher levels of phishing awareness are less likely to engage in risky reactions, such as clicking on either type of phishing email.

[2] In this study, "Did not open" and "Open" the emails (as no further action followed) were considered as safe behaviors, while clicking on the malicious link and submitting the data were considered as risky behaviors.

[3] In this study, the "Did not open" group refers to those participants who did not open the email; the "Open" group refers to those who opened the email but neither clicked on the link nor submitted their data"; the "Clicked on the link" group refers to those who opened the email and clicked on the link but did not submit their data; and the "Submitted data" refers to those participants who opened the email, clicked on the link and submitted their confidential information.

	Phishing awareness	Perceived protective practices	Course-related phishing reaction	Winning iPad phishing reaction
Phishing awareness	1			
Perceived protective practices	0.51**	1		
Course-related phishing reaction	-0.76**	-0.43**	1	
Winning iPad 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*

Table 2. Correlations between phishing awareness, perceived and actual practice constructs

To test Hypothesis 3, chi-square analysis revealed a significant association between users' prior experience and their perceived protective practices as well as their contextualized phishing reactions. In our study, users with prior experience of security threats, such as phishing, used more protective phishing practices (χ^2 (12) = 807.0, p = .000) and showed protective reactions (χ^2 (68) = 147.78, p = .000) by neither clicking on the link nor submitting their credential information through simulated phishing attacks. We also examined the correlation between users' prior experience and their perceived and actual protective practices. Table 3 below indicates a positive significant relationship (0.41**) between prior experience and perceived protective practices (p<0.01).

	Prior experience	Perceived protective practices	Course-related phishing reaction	Winning iPad phishing reaction
Prior experience	1			
Perceived protective practices	0.41**	1		
Course-related phishing reaction	-0.97**	-0.43**	1	
Winning iPad phishing reaction	-0.15*	-0.10*	0.14**	1

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

Table 3. Correlations between prior experience, perceived and actual practice constructs

These results suggest that prior experiences with phishing or other security threats are associated with a stronger perception that the individual would use appropriate phishing security practices. The results also indicate an inverse relationship between users' prior experience and their actual phishing reactions (-0.97***, -0.15*). This finding suggests that individuals with more prior experience of phishing or other security threats are less likely to

engage in risky reactions, such as clicking on either type of phishing emails. Users identified prior experiences with security threats that included examples such as a cyber-attack from visiting a website, important personal information such as a social security number being stolen, or being the victim of an online scam and losing money.

6.1 Post-hoc analysis

We also tested users' phishing awareness, perceived protective practices and actual phishing reactions by gender (Table 4). First, we compared participants' phishing awareness based on their gender. The result was statistically significant with $p< 0.005$. Therefore, we conclude that phishing awareness among female students is significantly lower than male students.

		N	Mean	Std. Deviation	Std. Error Mean	t	Df	Sig. (2-tailed)
Gender[4]	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

Table 4. Respondents' awareness of phishing

Next, we examined participants' perceptions of how they would react to phishing attempts. This was captured in five questions in the follow-up 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 use "protective practices", while those who 'sometimes', 'often' or 'always' engaged in risky behaviours were considered to engage in "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 recognize phishing threats and not fall victim to phishing attempts.

Table 5 presents our 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 organizations 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.

[4] Female and male respondents made up 97.9% of the sample, with around 2.1% of respondents preferring not to reveal their gender.

Context of messages	Mean	t	Gender (Mean)		%Perceived protective practice
			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%

Table 5. Participants' perception of their protective practices

Third, to examine users' actual phishing reactions by gender, we tested the proportion of males and females who opened, clicked on the link, and submitted data for both message conditions. We found a principal 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 6 with a chi-square test, which revealed a significant difference between female and male phishing reactions χ^2 (9) = 289.48, p = .000).

	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%

Table 6. Breakdown of the Phishing Results Based on Gender

Regarding other individual differences, we also found a significant age difference in the frequency of clicking on the malicious link and submitting sensitive information (χ^2 (18) = 68.33, p = .000). The results of the chi-square test presented a main effect of individuals' technical skills on the frequency of engaging in risky practices, i.e. clicking on the link and submitting data (χ^2 (9) = 86.90, p = .000). The chi-square test also revealed a significant main effect of individuals' study level on the frequency of clicking on the link and submitting the confidential information (χ^2 (12) = 87.50, p = .000). Appendix D presents the frequency of opening, link clicks and submitting data by study level.

7 Discussion

In this study, we investigated the impact of the content and framing of phishing attempts on users' vulnerability, and of users' phishing awareness on their perceived protective practices as well as on their actual phishing reactions by analysing the difference between users' perceived protective practices and their actual phishing reactions.

In support of Hypothesis 1, and in line with Goel and colleagues (2017), users in the present study were more susceptible to a highly contextualized message that appeared to pertain to their course results than to another generic message about winning an iPad mini. Almost three-quarters (71.3%) of our participants who opened the course-related message then clicked on the simulated phishing link, while 63.9% of them submitted their credential username and password. Therefore, the contextualized message channelled 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, actions which are consistent with the heuristic-systematic model (Eagly & Chaiken, 1993). In the course- related message, cues such as an important college matter and a credible sender as a reliable anchor led individuals to act without carefully considering the outcome of their actions. The highly contextualized email may have deterred the initial scrutiny of the users' systematic processing system. Existing research suggests that the most effective phishing messages function on both the heuristic and systematic processing systems (Goel et al., 2017; Luo et al., 2013). Drawing on anchoring effect, for our student participants, the importance of checking final course results may have lowered their sufficiency threshold and pushed them toward quick action, despite some spelling mistakes and the use of an incorrect college domain name.

Hypothesis 2a and 2b states that students' phishing threat awareness has a positive impact on their perceived protective practices and reactions. The results suggest that there is a significant positive 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 (Y. Chen, Ramamurthy, & Wen, 2015; Stanciu & Tinca, 2016; G. White, Ekin, & Visinescu, 2017). Thus, students must 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 & Wu, 2016). Therefore, effective security training and education programs should take a systematic approach by making sure they address the multiple dimensions of security awareness (G. L. White, 2015). Effective information security awareness and training programs should lead to improvement in graduates' ability to exercise protective reactions. Training would improve users' awareness and increase their sufficiency threshold, which would equip them to move beyond the heuristic mode and better engage in systematic processes. Awareness may lead knowledgeable users to more deliberate judgements, decisions and protective reactions. Additionally, it appears that such programs should also pay more attention to educating users about the risks caused by security threats.

Hypothesis 3 posited that users' prior security (i.e., phishing) experience or having been a victim of cybercrime play a significant role in users' phishing susceptibility. Based on our findings, users who had prior experience with security threats would engage more in safe practices and reactions. Prior experience may likely increase users' sufficiency threshold that they would shift from heuristic processing to more deliberate mode before any reaction.

Regarding other individual differences, based on our findings, younger students (e.g., between 18 to 20 years old) presented riskier reactions than older students (above 35 years old). Users with expert skills (e.g., the use of programming languages to develop applications) and advanced technical skills (e.g., the ability to manage and configure applications) demonstrated a safer phishing reaction than users with basic or intermediate technical skills. In addition, our findings show undergraduate students were more likely to click on a malicious link and submit their data than postgraduate students.

The results of the present study also show that students' vulnerabilities and practices differ according to gender, 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 (Flores et al., 2015; Sheng et al., 2010). Therefore, this variation may be bridged by providing customized training in order to improve security awareness and protective reactions among female users. 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), the findings of this study suggest that there is a large discrepancy between students' perceived protective practices and their actual reactions to contextualized phishing messages. Researchers have previously reported a conflict between users' beliefs about information security and their information security reactions. For example, users believe that they can protect their computers from hackers, despite their unfamiliarity with different types of security threats such as phishing, and countermeasures (e.g., installing a firewall) (Stanciu & Tinca, 2016). In addition, our findings

revealed that students were less susceptible to the phishing message geared toward free goods (an iPad mini) than for course-related messages. This implies 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 protective practices which conflicted with their phishing reactions in the course-related context. Therefore, relying on technical skills and high self-confidence in detecting phishing messages would increase users' vulnerability to phishing attacks. Drawing on HSM, users' self-confidence along with the deception of course-related messages from reliable sources would lower their sufficiency threshold that lead them to make quick uncertain judgments in the heuristic mode.

8 Theoretical and Practical Contributions

This study provides important theoretical contributions to the information security domain. It has been recommended to develop and test security models with a principal focus on the heuristic, automatic cognition worldview compared to the deliberate thoughtful process of security decision making and behaviours, to fill the gap in the current understanding of information security (Dennis & Minas, 2018). Accordingly, the present study investigated users' security reactions from the heuristic processing view to capture their unconscious phishing reactions. It establishes that contextual factors modify the effectiveness of phishing attempts. Heuristics would likely reduce rational logic processes and increase vulnerability to fraudulent messages. Most previous studies applied theories that may explain the cognition and behaviours of individuals but cannot fully predict and interpret users' automatic cognition based on their reactive and immediate emotions. Therefore, theories that focus on users' automatic, heuristic cognitions such as HSM are needed to understand their immediate reactions against phishing attacks.

The findings of this study offer support to the HSM. A contextualized phishing message from a reliable source may likely prompt individuals to act quickly without carefully considering the possible consequences of the action. Contextualized 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-contextualized messages. Although initial suspicion causes recipients to process a message more systematically, the contextualized message from a strong, trustworthy source would likely convince them that the message is legitimate. Our 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 lowered the user's sufficiency threshold, thus influencing their appraisal of or their response to the legitimacy of the message. This study suggests that HSM is a potentially worthwhile theoretical foundation for studying phishing and related cybercrime reactions.

The implications for practice call for thoughtful changes. In order to improve security compliance behaviour, users' experience-based heuristics can be changed. To reduce their vulnerability to phishing, the appetitive response approach should be replaced with heuristics that generate an avoidance response to the phishing messages, which can be referred to as aversion training. For example, organizations can send a series of phishing emails with links that trigger an alarm when they are clicked. After being tricked, most users would develop a strong avoidance heuristic to not click the links without deliberate evaluation. This will

improve users' heuristics and trigger the more systematically deliberate thinking mode for clicking on email links.

Based on the 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 contextualized 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 contextualized strategies, individuals' demographic characteristics should be taken into account to counteract user vulnerabilities4. Training counteracts users' phishing susceptibility through raising their sufficiency threshold effects to stop or limit heuristic processing, and thus it may increase the chance of systematic processing of messages.

We suggest it is highly important that higher education institutions not only develop security training programs, but students' enrolment in such training, their security awareness as well as their actual security practices (e.g., through utilizing 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 recognize security threats such as phishing, how to respond to and report these threats, and what is the magnitude and the 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 organizations for which they work.

9 Limitations, Future Research and Conclusion

The present study was conducted in a single higher education institution in New Zealand, so replicating it in wider community settings will help further validate its findings. This is especially because individuals with different cultures from different countries may behave differently regarding phishing messages (Eroglu & Croxton, 2010). 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 contextualized messages on 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 that receive different phishing emails should be used. We applied only two frames for the phishing emails. However, comparisons between these two scenarios provide interesting insights into the influence of framing and contextualization. Building mistakes into the phishing email suggests that these findings are only valid if phishers make mistakes, but phishing attacks are becoming increasingly sophisticated with stolen credentials and flawless English. Therefore, future studies should incorporate flawless phishing messages.

HSM provides a theoretical framework for future studies in which both quantitative and qualitative data may be collected to investigate and measure the research models and hypotheses more systematically. Quantitative data collected through surveys (e.g., scenario-based) and phishing experiments, would allow researchers to assess the hypotheses in a positivist way. On the other hand, qualitative data collected through field observations and interviews would allow investigators to obtain more first-hand insights into the phishing attacks, how individuals respond to and think about them, and provide the chance to validate theoretical reasoning and refine it.

Future studies may consider incorporating the anchoring effect in phishing experiments. The anchoring effect refers to the disproportionate impact of initially presented values on individuals when they make decisions and judgments (Tversky & 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 & Boo, 2011). The impact of a strong anchor such as users' prior experience or a trustworthy source in phishing experiments needs to be explored to realize if individuals who are presented with a particular parameter or a trustworthy source would make insufficient adjustments when making their final decision.

We tested the proposition that successful phishing attacks take advantage of Internet users by reducing their sufficiency threshold and luring 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. It has been investigated through an experiment with emails framed based on the proposed hypotheses to evoke user reactions. We found that phishing awareness is associated with users' protective practices and reactions related to phishing. We also tested the assertion that there is a discrepancy between users' perceptions of their phishing practices and their actual phishing reactions. We found a large gap between users' perception and their actual reaction in contextualized phishing messages, while not much difference between perception and reaction exists in a non-contextualized general message. Our findings reveal that the different demographics are associated with susceptibility to phishing. Therefore, the study suggests the need for context-based and targeted education based on demographic features (e.g., gender).

Acknowledgement

We acknowledge InternetNZ for providing financial support for this paper.

References

Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security, 68*, 160-196.

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies, 82*, 69-82.

Anderson, B. B., Vance, A., Kirwan, C. B., Jenkins, J. L., & Eargle, D. (2016). From warning to wallpaper: Why the brain habituates to security warnings and what can be done about it. *Journal of Management Information Systems, 33*(3), 713-743.

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

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior, 38*, 304-312.

Arachchilage, N. A. G., Love, S., & Beznosov, K. (2016). Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior, 60*, 185-197.

Bailey, J. L., Mitchell, D., Robert, B., & Bradley, K. (2008). Analysis of student vulnerabilities to phishing. *AMCIS 2008 Proceedings*, 271.

Beycioglu, K. (2009). A cyberphilosophical issue in education: Unethical computer using behavior–The case of prospective teachers. *Computers & Education, 53*(2), 201-208.

Blythe, M., Petrie, H., & Clark, J. A. (2011). F for fake: four studies on how we fall for phish Symposium conducted at the meeting of the *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* https://dl.acm.org/doi/pdf/10.1145/1978942.1979459

CERTNZ. (2019). *Quarter Three Report 2019*. Retrieved 2019, https://www.cert.govt.nz/about/quarterly-report/quarter-three-report-2019/

Chaiken, S. (1982). The heuristic/systematic processing distinction in persuasion Symposium conducted at the meeting of the Symposium on Automatic Processing, Society for Experimental Social Psychology, Nashville, IN

Chaiken, S. (1987). The heuristic model of persuasion. *Hillsdale, NJ: Lawrence Erlbaum.* Symposium conducted at the meeting of the Social influence: the Ontario symposium. *5* (3-39).

Chen, S., & Chaiken, S. (1999). The heuristic-systematic model in its broader context. In S. Chaiken & Y. Trope (Eds.), *Dual-process Theories in Social and Cognitive Psychology* (pp. 73-96). New York (NY): Guilford.

Chen, X., Chen, L., & Wu, D. (2018). Factors that influence employees' security policy compliance: an awareness-motivation-capability perspective. *Journal of Computer Information Systems, 58*(4), 312-324.

Chen, Y., Ramamurthy, K., & Wen, K.-W. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems, 55*(3), 11-19.

Chou, H.-L., & 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*, 83-96.

Cohen, J. B., & Reed, A. (2006). A multiple pathway anchoring and adjustment (MPAA) model of attitude generation and recruitment. *Journal of Consumer Research, 33*(1), 1-15.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79-98.

Dennis, A. R., & Minas, R. K. (2018). Security on autopilot: Why current security theories hijack our thinking and lead us astray. *ACM SIGMIS DATABASE for Advances in Information Systems, 49*(SI), 15-38.

Dinev, T., & 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), 386-408.

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006). Decision strategies and susceptibility to phishing Symposium conducted at the meeting of the Proceedings of the second symposium on Usable privacy and security. https://dl.acm.org/doi/pdf/10.1145/1143120.1143131

Eagly, A. H., & Chaiken, S. (1993). *The psychology of attitudes*: Harcourt brace Jovanovich college publishers.

Epley, N., & Gilovich, T. (2006). The anchoring-and-adjustment heuristic: Why the adjustments are insufficient. *Psychological science, 17*(4), 311-318.

Eroglu, C., & Croxton, K. L. (2010). Biases in judgmental adjustments of statistical forecasts: The role of individual differences. *International Journal of Forecasting, 26*(1), 116-133.

Esch, F. R., Schmitt, B. H., Redler, J., & Langner, T. (2009). The brand anchoring effect: A judgment bias resulting from brand awareness and temporary accessibility. *Psychology & Marketing, 26*(4), 383-395.

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

Furnham, A., & Boo, H. C. (2011). A literature review of the anchoring effect. *Socio-Economics, 40*(1), 35-42.

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

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

Hajli, N., & 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), 111-123.

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

Halevi, T., Memon, N., & Nov, O. (2015). *Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks*. Available at SSRN: https://ssrn.com/abstract=2544742

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

Hassandoust, F., & Techatassanasoontorn, A. A. (2020). Understanding users' information security awareness and intentions: A full nomology of protection motivation theory. In *Cyber Influence and Cognitive Threats* (pp. 129-143): Elsevier.

Hilligoss, B., & Rieh, S. Y. (2008). Developing a unifying framework of credibility assessment: Construct, heuristics, and interaction in context. *Information Processing & Management, 44*(4), 1467-1484.

Hovav, A., & 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), 99-110.

Irwin, L. (2020). *The 5 most common types of phishing attack*. Retrieved from https://www.itgovernance.eu/blog/en/the-5-most-common-types-of-phishing-attack

Iuga, C., Nurse, J. R., & Erola, A. (2016). Baiting the hook: factors impacting susceptibility to phishing attacks. *Human-centric Computing and Information Sciences, 6*(1), 1-20.

Jacowitz, K. E., & Kahneman, D. (1995). Measures of anchoring in estimation tasks. *Personality and Social Psychology Bulletin, 21*(11), 1161-1166.

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

Jakobsson, M., & Ratkiewicz, J. (2006). Designing ethical phishing experiments: a study of (ROT13) rOnl query features Symposium conducted at the meeting of the Proceedings of the 15th international conference on World Wide Web. https://dl.acm.org/doi/pdf/10.1145/1135777.1135853

Jansen, J., & Van Schaik, P. (2018). Persuading end users to act cautiously online: A fear appeals study on phishing. *Information & Computer Security, 26*(3), 264-276.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS Quarterly, 34*(3), 549-566.

Kahneman, D. (2011). *Thinking, fast and slow*: Macmillan.

Kim, D., & Kim, J. H. (2013). Understanding persuasive elements in phishing e-mails. *Online Information Review*.

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F., & Hong, J. (2007). Getting users to pay attention to anti-phishing education: evaluation of retention and transfer Symposium conducted at the meeting of the Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit https://dl.acm.org/doi/pdf/10.1145/1299015.1299022

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology, 10*(2), 1-31.

Lim, J. S., Ahmad, A., Chang, S., & Maynard, S. B. (2010). Embedding Information Security Culture Emerging Concerns and Challenges Symposium conducted at the meeting of the Pacific Asia Conference on Information Systems https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1041&context=pacis2010

Loewenstein, G., O'Donoghue, T., & Bhatia, S. (2015). Modeling the interplay between affect and deliberation. *Decision, 2*(2), 55-81.

Luo, X. R., Zhang, W., Burd, S., & Seazzu, A. (2013). Investigating phishing victimization with the Heuristic–Systematic Model: A theoretical framework and an exploration. *Computers & Security, 38*, 28-38.

McElwee, S., Murphy, G., & Shelton, P. (2018). Influencing Outcomes and Behaviors in Simulated Phishing Exercises*IEEE. Symposium conducted at the meeting of the SoutheastCon 2018*. https://ieeexplore.ieee.org/document/8479109

McHugh, M. L. (2013). The chi-square test of independence. *Biochemia Medica, 23*(2), 143-149.

Mitnick, K. D., & Simon, W. L. (2003). *The art of deception: Controlling the human element of security*: John Wiley & Sons.

Moody, G. D., Galletta, D. F., & Dunn, B. K. (2017). Which phish get caught? An exploratory study of individuals' susceptibility to phishing. *European Journal of Information Systems, 26*(6), 564-584.

Musuva, P. M., Getao, K. W., & Chepken, C. K. (2019). A new approach to modelling the effects of cognitive processing and threat detection on phishing susceptibility. *Computers in Human Behavior, 94*, 154-175.

Nouh, M., Nurse, J. R., Webb, H., & Goldsmith, M. (2019). Cybercrime investigators are users too! Understanding the socio-technical challenges faced by law enforcement. *arXiv preprint arXiv:1902.06961*.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2015). The design of phishing studies: Challenges for researchers. *Computers & Security, 52*, 194-206.

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., & Calic, D. (2015). Factors that influence information security behavior: An Australian web-based study. *International Conference on Human Aspects of Information Security, Privacy, and Trust*. (pp. 231-241). Springer, Cham.

Petty, R. E., & Cacioppo, J. T. (1984). The effects of involvement on responses to argument quantity and quality: Central and peripheral routes to persuasion. *Journal of Personality and Social Psychology, 46*(1), 69.

Pienta, D., Thatcher, J. B., & Johnston, A. (2020). Protecting a whale in a sea of phish. *Journal of Information Technology*, 0268396220918594.

Resnik, D. B., & Finn, P. R. (2018). Ethics and phishing experiments. *Science and Engineering Ethics, 24*(4), 1241-1252.

Salah El-Din, R (2012) To Deceive or not to Deceive! Ethical Questions in Phishing Research. In *HCI Research in Sensitive Contexts: Ethical Considerations Workshop at HCI, Birmingham*, UK. http://eprints.leedsbeckett.ac.uk/4834/

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.* https://dl.acm.org/doi/pdf/10.1145/1753326.1753383

Simon, H. A. (1965). *Administrative Behavior. A Study of Decision-making Processes in Administrative Organization*: Macmillan.

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

Soghoian, C. (2008, October). Legal risks for phishing researchers. In *2008 eCrime Researchers Summit* (pp. 1-11). IEEE. https://ieeexplore.ieee.org/document/4696971

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

Straub, D., Boudreau, M. C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information systems, 13*(1), 380-427.

Turner, C. G., & Monk-Turner, E. (2007). Gender differences in occupational status in the South Korean labor market: 1988-1998. *International Journal of Social Economics*.

Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. *Science, 185*(4157), 1124-1131.

Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research, 45*(8), 1146-1166.

Wang, J., Li, Y., & Rao, H. R. (2016). Overconfidence in phishing email detection. *Journal of the Association for Information Systems, 17*(11), 759-783.

Wang, J., Li, Y., & Rao, H. R. (2017). Coping responses in phishing detection: an investigation of antecedents and consequences. *Information Systems Research, 28*(2), 378-396.

Wegener, D. T., Petty, R. E., Detweiler-Bedell, B. T., & 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), 62-69.

Whetten, D. A. (2009). An examination of the interface between context and theory applied to the study of Chinese organizations. *Management and Organization Review, 5*(1), 29-56.

White, G., Ekin, T., & Visinescu, L. (2017). Analysis of protective behavior and security incidents for home computers. *Journal of Computer Information Systems, 57*(4), 353-363.

White, G. L. (2015). Education and prevention relationships on security incidents for home computers. *Journal of Computer Information Systems, 55*(3), 29-37.

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

Wirth, W., Böcking, T., Karnowski, V., & Von Pape, T. (2007). Heuristic and systematic use of search engines. *Journal of Computer-Mediated Communication, 12*(3), 778-800.

Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., & Marett, K. (2014). Research note—influence techniques in phishing attacks: an examination of vulnerability and resistance. *Information Systems Research, 25*(2), 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), 252-271.

Wu, M., Miller, R. C., & Garfinkel, S. L. (2006). Do security toolbars actually prevent phishing attacks? *Proceedings of the SIGCHI conference on Human Factors in computing systems*. https://dl.acm.org/doi/pdf/10.1145/1124772.1124863

Appendix A. Summary of Related Literature on Phishing

Author(s)/Year	Research Approach	Elements Investigated	Behavioral Aspect	Theory	Relevant findings
Musuva, Getao, and Chepken (2019)	Observations of phishing susceptibility and self-reported questionnaires	Attack quality, motivation to process, ability to process and knowledge, threat detection and elaboration	Phishing susceptibility	Elaboration likelihood model	Threat detection was found to explain why people who expend cognitive effort processing phishing communication are less likely to fall for phishing threats.
Jansen and Van Schaik (2018)	Online survey with fear appeal conditions	Perceived vulnerability and severity, fear, response efficacy, self-efficacy and response cost	Protective motivation	Protection motivation theory	Self-efficacy and fear were the most significant determinants of protection motivation.
McElwee et al. (2018)	Simulated phishing exercise	Outcome-based controls and behavior-based controls	Susceptibility to phishing	Agency theory	Behavior-based controls (e.g., targeted training) were more successful in reducing susceptibility to phishing.
Resnik and Finn (2018)	Ethics and phishing experiments	Phishing experiments are ethical if there is an opt-out option for participants and they are debriefed afterwards	Ethical phishing experiments	-	Although phishing experiments consist of deception and breach informed consent requirements, the risks can be minimized if the confidentiality and the privacy of participants are protected.
Vishwanath, Harrison, and Ng (2018)	Two experimental studies	Cyber risk beliefs, deficient self-regulation, Heuristic and systematic processing, email habit	Suspicion, cognition, and automaticity model (SCAM)	Suspicion	Individuals are likely to fall victim to phishing emails when aspects of the email aroused suspicion about the request. When individuals believe their cyber actions are quite risky, they tend to systematically process emails.
Aleroud and Zhou (2017)	Online survey	A taxonomy including attacking techniques, countermeasures, targeted environments and communication media	Phishing detection and prevention	-	The taxonomy provides guidance for the design of effective techniques for phishing detection and prevention. The taxonomy also helps practitioners to evaluate and select methods, tools and features to handle phishing problems.

Author(s)/Year	Research Approach	Elements Investigated	Behavioral Aspect	Theory	Relevant findings
Goel et al. (2017)	Online survey	Situational factors and contextualization of phishing emails	Vulnerability to phishing	Heuristic-systematic processing model	Contextualized messages that appeal to recipients' psychological weaknesses increase their vulnerability to phishing.
Moody et al. (2017)	Phishing experiment and online survey	Situational and personality factors	Susceptibility to phishing	Delphi method	Emails sent from a known source significantly increase user susceptibility to phishing, as does a user's risk propensity, curiosity, Internet anxiety and general Internet usage.
Wang et al. (2017)	Online survey experiment	Perceived phishing threat and detection efficacy, phishing anxiety	Coping responses in the process of phishing email detection.	Extended parallel process model	Perceived detection efficacy increases coping adaptiveness. Coping adaptiveness positively impacts the two objective measures in the study, detection effort and detection accuracy.
Anderson et al. (2016)	Phishing experiment-NeuroIS techniques, functional magnetic resonance imaging (fMRI)	Polymorphic warnings and conventional warnings	Behavior towards security messages (e.g. warning against phishing) via NeuroIS techniques	Stimulus-model comparator theory and the dual-process theory	Polymorphic warnings reduced habituation compared to conventional warnings.
Arachchilage et al. (2016)	Mobile game prototype.	Perceived severity, susceptibility and threat, safeguard effectiveness and cost, self-efficacy and avoidance motivation	Avoiding phishing attacks	-	Participants' threat perception, self-efficacy, safeguard effectiveness, perceived threat severity and susceptibility elements positively influence threat avoidance behavior, whereas safeguard cost had a negative impact on it.

Author(s)/Year	Research Approach	Elements Investigated	Behavioral Aspect	Theory	Relevant findings
Iuga et al. (2016)	Web-based study	Demographic characteristics of individuals, time-related factors and users' ability to correctly detect a phishing attack	Phishing behavior	Anchoring effect	Psychological anchoring effect, gender and the years of computer usage have a significant positive impact on users' ability to detect phishing attacks. Popup-based phishing attacks have a higher success rate.
Alsharnouby, Alaca, and Chiasson (2015)	User eye tracking study to identify the phishing websites	Improved browser security indicators and increased awareness of phishing	Phishing detection practice	-	Individuals still fall for phishing and don't invest much time looking at security measures, although those that do are less susceptible to phishing.
Flores et al. (2015)	Scenario-based survey, phishing experiments, follow-up interviews	Added personal information about the target to an attack, individual's trust, computer experience at work, helpfulness and gender	Risky phishing behavior	-	The degree of target information in an attack increased the likelihood that an organizational employee falls victim to an actual phishing attack.
Parsons, McCormac, Pattinson, Butavicius, and Jerram (2015)	A role play scenario experiment	Category (e.g., industry or sender) of emails	Phishing detection practice	Signal detection theory	Informed participants were significantly better at discriminating between phishing and genuine emails than uninformed participants.
Arachchilage and Love (2014)	Online questionnaire	Conceptual knowledge or procedural knowledge on computer users' self-efficacy	Phishing threat avoidance behavior	Technology threat avoidance theory	Conceptual and procedural knowledge positively impact on computer users' self-efficacy, which enhance their phishing threat avoidance behavior.
Wright et al. (2014)	Field experiment	Influence techniques (liking, reciprocity, social proof, consistency, references to authority, and scarcity)	Susceptibility to phishing attacks	Persuasion and motivation theory	Influence techniques such as liking, reciprocity, social proof, consistency, authority, and scarcity were significant predictors, implying fictitious experiences decrease phishing effectiveness

Author(s)/Year	Research Approach	Elements Investigated	Behavioral Aspect	Theory	Relevant findings
Luo et al. (2013)	Qualitative explorative study	Psychological mechanisms such as argument quality, source credibility, genre conformity underlying the effectiveness of phishing attacks	Spear phishing victimization	Heuristic systematic model	High argument quality, strong source creditability and strong genre conformity appears to lead to successful victimization.
Salah El-Din (2012)	Controlled-lab studies	Need for deception, legal restrictions of conducting phishing studies	Phishing reaction	-	Proposed a roadmap to consider legal and ethical aspects prior conducting a phishing study.
Blythe et al. (2011)	Multi-method set of a few studies	Strategies used to identify phish	Phishing detection	Critical theory	Detection rates for phishing messages with logos were significantly lower than for those without. Warnings about how to avoid phishing look exclusively to the user.
Soghoian (2008)	Case studies	Legal risks	Social phishing reaction	-	The key risks are abuses of a provider's terms of use, intellectual property copyright and rights infringement.
Kumaraguru et al. (2007)	A user study	Simulated phishing emails in detection of the real phishing attacks	Phishing detection behavior	-	A methodology called PhishGuru has been developed that was proved to be effective in training individuals regarding phishing attacks.

Appendix B. Measurement Items of the Study

Variable	Measurement items	Source
Phishing awareness (familiarity)	On a scale from 1 to 9 (1 = not familiar at all; 9 = very familiar), please indicate your level of familiarity with the threat of phishing.	(Hanus & Wu, 2016)
Prior experience of security threats	Have you ever experienced the following situation (such as desktops, phones, tablets, laptops etc.)? (yes or no - you may select multiple answers) • A cyber-attack from opening a link or an attachment in a fraudulent email (called "phishing") • A cyber-attack from visiting a website • A cyber-attack from a new icon or program (e.g., pop-up offering a free computer security scan) appeared out of nowhere • You had important personal information stolen, such as your credit card number • Someone used or attempted to use your personal information without permission to obtain new credit cards or loans, run up debts, open other accounts, or commit other fraud. • Someone used or attempted to get your accounts' username and passwords such as bank account, or debit/check cards. The ratings for each respondent on each item sum were summed to provide an overall score.	Adapted from Wang et al. (2016) and modified for phishing context

Variable	Measurement items	Source
Perceived protective practices	On a scale from 1 to 5: • 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? • 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? • 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? • 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? • I click on email links or posts with touching winning messages such as winning an Apple iPad. The ratings for each respondent on each scenario were averaged to provide an overall score.	(Bailey et al., 2008)

Appendix C: Phishing Messages

Phishing message 1: Obtaining their course results

Sender: A personal email address, (***addmin@gmail.com)

Dear Student,
You are receiving this email in order to check the status of your attendence and assessments results.
Please click on the button below in order to check your **attendence** and **assignments** results.

If you have any pending "Disciplinary Hearings" it may also influence your results. See the Policy below.

Passing a Paper
Students must and submit all assessments for a paper

Final Examination
NOTE: the Final Examination is the final assessment a student takes for their paper and is normally worthe 60%.

Re-sit Examinations
NOTE: this is an opportunity for a student to take the final assessment at a later date in their program (and not imediately after their finishing their paper).

Failed Students
Students will be marked as having failed a paper if they have not achieved an overall paper mark of 50% after all opportunities have been given to the student.

Thank you,
Cathy
Exam Officer
[School name]
T: +649 XXXXXX | F: +649 XXXXXX | Adress: XXXXX
E: cathy@[school domain with a typo].com (it should be 'co.nz' instead)

Phishing message 2: Winning an iPad mini
From: NZ Apple Research Team
Subject: Get a free iPad mini for giving it a test drive
Dear Student:
You've won an iPad mini! Apple (NZ Premium Reseller) is distributing its new mini tablet to select university/institution students who are willing to help evaluate it. The tablet has the same capabilities as an iPad with a smaller screen. In return for the free tablet all we will request is for you to provide us feedback on the product every two weeks. You will be provided a template to fill out your experiences with the tablet. Apple is an equal opportunity company and you were randomly selected without any cultural or racial bias. Please register at the following link and make sure that you accept the terms and conditions at the end of the form.
http://applle.com/resarchnzipadmini/

Best Wishes,
Apple Research Team, NZ

Appendix D. Proportion of Respondents Who Opened the Phishing Email, Clicked on the Link and Submitted Data by Study Level

	% Did Not Open	% Opened	% Clicked	% Submitted Data	Total number of respondents
Postgraduate – Level 9	2.6%	6.7%	0.7%	4.5%	39 (14.5%)
Postgraduate – Level 8	2.6%	5.9%	3%	4.1%	42 (15.6%)
Undergraduate – Level 7	1.1%	3%	1.5%	6.7%	33 (12.3%)
Undergraduate – Level 6	0.7%	1.1%	1.9%	30%	92 (33.7%)
Undergraduate – Level 5	2.2%	2.6%	0.4%	18%	63 (23.2%)

doi: https://doi.org/10.3127/ajis.v24i0.2693