Risks of Harm through Social Media Use: Scams and How Users Respond

Val Hooper
School of Marketing and International Business, Victoria University of Wellington, New Zealand

val.hooper@vuw.ac.nz

Abstract: Media reports abound of harm that can occur to the individual when using social media, from financial, emotional to psychological. To date, research around online harm and mitigation has tended to focus on specific risks such as phishing scams and identity theft. Some studies have explored the influence of factors such as age, cognitive ability, education, personality and risk propensity; while others have examined the effects of the type of attack, e.g. investment scam, on scam compliance. However, few studies, if any, have explored the individual's approach to the holistic notion of potential risk and harm that might occur through social media use, particularly scams, given that one seldom knows what sort of, when and where such an attack may occur. This study aims to address this gap in the research.

Informed by, amongst others, Protection Motivation Theory (Rogers, 1975), Reactance Theory (Brehm, 1966) and Self-Determination Theory (Deci & Ryan, 1985), exploratory interviews were conducted with a purposive sample of 25 individuals to ascertain (1) their knowledge and/or experience of scams and consequent harm in social media use and (2) their mitigation responses. Findings indicate a range of scam knowledge and experience. Financial damage occurred most frequently, and often significant emotional harm. A variety of tactics was embraced by the interviewees in order to mitigate the potential harm of social media use. These ranged from becoming expert in certain types of attacks, to adopting a head-in-the-sand approach. Various demographic, personality and contextual factors seemed to contribute to vulnerability and favoured mitigating tactics.

Suggestions are provided as to how to provide holistic guidance to users and the role of banks, social media and regulatory/advisory bodies. Areas of future research are also indicated.

Keywords: Online Scams, Scam Vulnerability, Scam Mitigation Behaviour, Personality, Context, Age

1. Introduction

In 2024, Australian scams accounted for AUS$ 292,542,032.41 in losses (Scamwatch, 2024), and online scams cost New Zealanders an estimated $2.3 billion in 2024 (Netsafe, 2024). While it's difficult to get an accurate picture of global costs of online scamming, because of differences in reporting and recording, and frequent non-reporting of incidences, these costs can be regarded as healthy indications of the damage that scams can cause.

Research into social media harm and mitigation has tended to focus on specific risks such as phishing scams and identity theft. Aspects such as the characteristics and profiles of the victims as well as the scammers have been studied in detail. The influence of factors such as age, cognitive ability, education, personality and risk propensity have been highlighted. However, when an individual encounters a scam, one seldom knows what sort of, when and where such an attack may occur. Few studies, if any, have explored the individual's approach to the holistic notion of potential risk and harm that might occur through social media use, particularly scams, so it's hard to know what the general preparedness of users is for these types of onslaughts. This study aims to address this gap in the research by asking two research questions: what are people's knowledge and/or experience of scams and consequent harm in social media use and (2) what are their mitigation responses.

The research reported in the following sections, records an initial exploration into the research questions by way of a literature review which informed qualitative interviews with 25 interviewees. The findings and their analysis are reported together with a discussion of directions for future research and guidance for practitioners.

2. Literature Review

A scam can be defined as "a fraudulent or deceptive act or operation" (Merriman-Webster, 2024). For many, their first experience of a scam was via email in the 1980s when the "Nigerian letter" became widespread. These scams were easily detectable through poor construction of the letter, inappropriate use of language, and also the unlikelihood of being approached by an unknown potentate (Tambe Ebot at al., 2024).

Since then scams have become more refined so that many are now difficult to detect and hoodwink many unsuspecting Internet users. Previously perpetrated via email, social media and mobile applications have enhanced the availability of pools of potential victims (Tambe Ebot et al., 2024).

Financial and romance scams are the general categories of the most prominent scams. Among the financial scams, investment scams, charity scams (Tambe Ebot et al., 2024), income tax refund scams, cryptocurrency investment feature largely (Shete at el., 2024). Romance scams encompass online dating scams, and sextortion scams. Phishing scams are very prevalent, as are vishing scams. In addition, delivery scams, lottery and prize scams are frequently reported (Shete at el., 2024). Cyberbullying is not so frequently reported but anecdotally, such scams are prevalent.

The scams that appear to be the most "successful"/effective, or most pervasive are the social engineering attacks. These include phishing (Sarno & Black, 2024), and advance fee fraud (AFF). AFF requires advance payment for reasons that range from investment, romance, pets, employment opportunities, lottery, drugs to transportation of goods.

Aspects of the messages also enhance response. These include elements of urgency – the need to respond speedily to the request or offer. In addition, the likelihood of the event occurring renders the recipient of the scam more amenable to responding, for instance, the expectation of money being deposited in one's bank account, the expectation or the probability of a parcel being delivered, the possibility of a prize, the desire to avoid some form of punishment (such as for outstanding tax), a likely good cause requesting a donation (Shete at el., 2024).

2.1 Responses to Scams

There are two categories of responses to scams: if one suspects the message is a scam; or if one does not suspect.

For those who suspect that a message is a scam, the following are the main courses of action: the message is ignored; attachments are not opened; the message might be deleted; and the possible scam reported to friends and family and, in rare instances, to a third party such as Netsafe. However, if the potential danger does not seem so large, chances are that the recipient will be more susceptible, especially if the reward might be immediate and is appealingly described (Langenderfer & Shimp, 2001). Alternatively, if a substantial potential danger can be identified, then the severity and the recipient's potential vulnerability to the danger are weighed up against one another, or appraised, before coping mechanisms such as response efficacy, self-efficacy and response costs are considered. Depending on the outcome, so the scam is responded to or not (Jansen & Van Schaik, 2018). This is in line with Rogers' (1975) protection motivation theory.

On the other hand, if no scam is suspected, then influences such as knowledge and experience, personality factors, age and contextual factors (see below) play much more of a role in determining response.

2.2 Mitigation Behaviour

Awareness and knowledge of potential threats is necessary before any mitigating or protective behaviour can ensue (Mohsin & Palvia, 2024). Individuals acquire knowledge by learning about specific scams or, more often, through (often bitter) experience. Indications are that the average recipient tends to learn more about the scams of which they've had direct or close experience, rather than about scams in general. Attitudes towards the various threats can develop (Hong et al., 2024) and the following responses illustrate both attitudes as well as personality.

Certain mitigating responses demonstrate sometimes rash, but often rational, behaviours. For instance, psychological reactance theory (Brehm, 1966) states that the reactance that people experience when something threatens their freedom of behaviour, motivates them to restore that freedom. They do this by a fight or flight response. Risk takers tend to fight, i.e. respond to the scam; risk avoiders choose flight and don't respond (Clayton et al., 2019). Such behaviour can be linked to self-determination theory (Deci & Ryan, 1985) which recognises the basic needs of autonomy, relatedness and competence. The need for autonomy is especially relevant so depending on how much they want guidance from others, the recipient will or will not respond.

Another way of dealing with potential danger or fear, is by threat devaluation (Thompson et al., 2024). Borrowing from the threat severity and threat vulnerability identified by Rogers (1975), such an approach is problem-focused as well as emotion-focused and seeks to minimise the threat by reducing the perceived severity of it, or one's vulnerability to it.

A further approach is by means of adaptive emotional regulation. According to Lazarus and Folkman's (1984) transactional theory of stress and coping, when stressful information is received, it is appraised cognitively in

order to deal with the stressor, as well as manage the negative emotions (Biggs et al., 2017). Such avoidance strategies can be regarded as burying one's head in the sand (Waldinger & Schulz, 2010).

2.3 Influences

The literature has identified many factors that can influence responses to scams. The following categories are the most relevant ones.

2.3.1 Knowledge and Experience

While an important mitigating action is to gain knowledge about scams and how to deal with them, in gathering information individuals include what they may learn about from others or from organisational actions (Li and Siponen, 2022), and what they may learn about through their own experience (De Kimpe et al., 2018).

With the rapid growth of the different types of scams, such as phishing, in particular (De Kimpe et al., 2018), individuals focus on what they're most interested in because of personal relevance or experience. They thus acquire information about one or two types of scams but remain ignorant of many of the rest.

2.3.2 Personality

Goldberg's (1992) Big 5 personality traits (extraversion, agreeableness, openness, conscientiousness, neuroticism) are one of the most popular personality trait theories and while the traits could apply in the responses to scams, other traits loom prominently. These include greed (Langenderfer & Shimp, 2001) which influences how much the recipient wishes to benefit from what is offered, and curiosity which refers to the desire to seek and learn new information (Litman, 2010). Curiosity has two main types: information seeking/cognitive curiosity and sensory curiosity, both of which stimulate exploratory behaviour (Litman & Spielberger, 2003), such as opening scam messages. In such behaviour, there is also an element of risk propensity and impulsivity, which have been identified as being influential in phishing responses (De Kimpe et al., 2018). Gullibility and susceptibility have been shown to influence online response behaviour (Langenderfer & Shimp, 2001) as has propensity to trust (Williams et al., 2017). On the other hand, scepticism also plays a role in influencing responses (Langenderfer & Shimp, 2001). Interestingly, Koning at el. (2024) did not find any clear personality profile that was more at risk of fraud, except those having low self-control.

2.3.3 Age

It has been argued that people over 64 and the young are more vulnerable because of reduced cognitive ability (Yu et al., 2023) and social isolation (Langenderfer & Shimp, 2001). However, Sarno and Black (2024) found that age did not predict susceptibility but, on the other hand, Olivier et al. (2015) found that psychosocial background, emotional vulnerability, the need for meaningful activity and opportunities for engagement were predisposing age-related factors. Gender and education are often regarded as exercising an influence together with age (Whitty, 2020).

2.3.4 Contextual Factors

Certain contextual factors, such as culture and organisations have been identified as exerting an interactional influence on response behaviour (Williams et al., 2017). The extent of elaboration needed in decision making, as with the elaboration likelihood model (Langenderfer & Shimp, 2001) has also featured as an influence.

Recipients of fraudulent messages may also be suffering from information security fatigue (Mohsin & Palvia, 2024) information security burnout (Pham et al., 2019) or reactance (Clayton et al., 2019). Information security fatigue occurs when an employee feels overwhelmed by the demands of adhering to security policies. Such fatigue may lead to risky online security behaviours (Furnell & Thomson, 2009). Burnout describes a state of mental weariness which includes two dimensions: exhaustion and cynicism. Consequent behaviour often evidences carelessness (Schaufeli &Bakker, 2004).

Extent of online purchasing behaviour and risky online self-disclosure, as well as experience of the Internet are further influential contextual factors (De Kimpe et al., 2018). Lastly, general life satisfaction has been noted as being an important influence (Hong et al., 2024).

3. Research Method

As the research was exploratory, an interpretive paradigm was adopted. Data were gathered by means of semi-structured individual interviews with 25 purposively selected participants. The participants were composed of both men and women and their ages ranged from 25 to over 65. Each interview lasted at most 40 minutes. They were recorded and subsequently transcribed for analysis. The broad categories explored with interviewees were according to the two main research questions: what is (1) their knowledge and/or experience of scams and consequent harm in social media use and (2) their mitigation responses, with opportunities to explore aspects that warranted further elaboration. Each participant was assured of the confidentiality.

The data were analysed according to the research questions. Thematic analysis was adopted in order to gain a holistic overview of response patterns. The responses were compared to the literature and unexpected and "new" insights were examined for pertinence and importance.

4. Findings

Interviewees were very forthcoming about their knowledge and/or experience of scams and consequent harm through social media use. The types of scams mentioned included the Nigerian letter, dating scams, parcel delivery, financial scams ("My husband said he just saw our money actually disappearing out of our account."), cryptocurrency scams, investment opportunity scams ("Friends of ours were wiped out. It was tragic. All his retirement money went into the scheme), encore scams, banks/telephone companies/computer companies "checking" users' details, adoption scams, and burglary scams ("Posting details of your trips and other "users" prompting you for details just validates when you'll be away")

In summary, the majority of interviewees had experienced online scams. A number had fallen prey to the scammers or had family members or friends who had had such experiences. The range of experiences seems to have been reflective of the different types of scams with those related to money being the stand-out scams by far. Another popular area of scamming noted was with regard to IT and connectivity. In other words, this would be another route to accessing data with financial details. Emotional scams, such as the adoption scam, featured strongly.

Considerable information was acquired via the media but organisations like banks and third party security agencies, such as Netsafe, that promoted online safety, played a prominent role in informing the public. However, knowledge was sketchy – possibly more extensive with regard to one or two scam types, but generally superficial.

4.1 Responses to Scams

The majority of interviewees usually exercised some form of precaution. If they were wary that a message was a scam, then they simply didn't respond, nor did they click on links or open attachments. Aspects that alerted them to potential scams were features such as repeats of similar messages, for example parcels requiring payment for delivery. Also, if invitations sounded too good to be true, then a catch was suspected. A few checked url's and compared them to the banks from whence they were claiming to be sent. Others actually contacted the organisation that was purportedly seeking their personal/financial details. Such actions are in accordance with advice provided by organisations such as Kiwibank (2024). The majority checked with family or friends, often showing them the message before proceeding. Interestingly, they checked for reassurance that they were doing the right thing; they checked for superior knowledge; and they checked for similarity of experience and the outcomes of subsequent actions – if there had been no negative consequences, they would follow respond to the message.

However, many interviewees had responded unwittingly to scam messages/instructions/invitations in the past as an automatic reaction. They hadn't stopped to think – and they hadn't suspected anything untoward. Similarly, a few interviewees had opened attachments to messages for the same reason, thereby providing opportunities for bugs to be inserted into their systems. A few had responded because the source seemed genuine, particularly in the case of messages from banks.

"It looked just like the usual messages from my bank with the same logo's, colours and layout."

In addition, one interviewee admitted that they couldn't resist opening attachments because they had been curious - as Litmen and Spielberg (2003) had found - or felt they might miss out on something interesting. Another had responded to an invitation because the prize had seemed so good – as had been found by

Langenderfer and Shimp (2001). A number of interviewees admitted that they had responded to scam invitations or had opened phishing links after they had had "a few drinks" and had thrown caution to the wind. Yet others had responded because they had been in a hurry and "hadn't had time to check through all the small detail".

4.2 Mitigation Behaviour

The approach of a number of interviewees was to be informed and try to protect themselves as intelligently as possible. This meant taking control of the situation (Li & Siponen, 2022). However, many interviewees adopted the approach of one who indicated: "I can't keep up so one never knows what's going to hit you. I suppose we've just got to be very careful". Others tried to become experts in certain areas for various reasons, such as: "Because I've lost money on a cryptocurrency scam, I suppose I've read up more about those and am extra vigilant". One interviewee was practical and reported: "The safest is to spread your assets so if you're scammed, then your loss will be only a portion of your assets." A couple of interviewees had considered decreasing/ceasing their social media use, as suggested by Thompson et al. (2024) but were reluctant to lose the benefits.

However, the vast majority relied on some other people or institutions to advise them (Li & Siponen, 2022), for instance the "more knowledgeable members of the family", or "I just leave all that sort of computer stuff to my husband." Institutionally, the workplace was a prominent source of protection: "At work, they're pretty good at distributing regular warnings about scams doing the rounds and what they've done to protect us." Others relied on the government, organisations such as Netsafe, or social media, seeing it as their responsibility to protect the users.

A good portion of the interviewees adopted a rather passive approach which ranged from fatalistic resignation - "I'll probably get zapped at some time -it seems to happen to so many people" - to a head-in-the-sand approach as suggested by Waldinger and Schulz (2010) whereby they downplayed the frequency and severity of scams – "Oh, it's just the media. They over-exaggerate everything!" (Thompson et al., 2024).

There were also elements of reactance (Rosenberg & Siegel, 2018) where a couple of interviewees indicated that they were fed up with continual messages from their IT departments telling them what and what not to do, and they'd just thrown caution to the wind and responded if the invitation seemed appealing.

Yet others rationalised that they were not important /wealthy enough to be the target of scammers. "I just console myself with the thought that I'm just small fry and the scammers are probably more interested in far wealthier folk than me."

4.3 Influential Factors

In their responses to potential scams, the interviewees indicated a number of factors that influenced their response decision.

Firstly, general IT knowledge and comfort of working in that sort of technological environment, played an important role. Knowledge seemed to boost people's confidence and power to control such risky situations. Interviewees felt empowered to make appropriate decisions. This applied whether the knowledge was just general or scam-specific.

Secondly, personality emerged as a very influential factor. A number of interviewees indicated considerable curiosity about "tempting" messages and a few succumbed and responded to the scam or opened a link or attachment. This accords with Litman's (2010) findings as well as those of Williams et al. (2017) who identified the trusting nature of people as making them more gullible.

Thirdly, the context of dealing with a scam is also important. A few interviewees noted that when they were hurried, distracted or frazzled, they acted in a less cautious, possibly quicker manner without thinking. These sorts of responses seem to indicate security fatigue (Mohsin & Palvia, 2024) or burnout (Schaufeli & Bakker, 2004) – too many security requirements when other activities seemed to require more attention. In addition, if retired, in many instances, the relative isolation implied less contact with, and advice from, others (Langenderfer & Shimp, 2021).

Fourthly, and linked to the above, as Yu et al. (2023) and Olivier et al. (2015) had found, age appears to exert an influence but more because certain conditions go hand-in-hand with advanced age. If retired, more time seemed available to spend on investigating "tempting" messages. Also not such regular exposure to cybersecurity training as in the workplace might reduce knowledge and make one more vulnerable. Furthermore, there is possibly more money in their accounts or to be invested.

Fifthly, exposure to notices from IT departments at work and training provided in that environment alerted interviewees to the existence and the danger of the different scams, as well as how to deal with them. The frequent messaging from the IT department, kept them constantly aware of potential harm (Hong et al., 2024; Mohsin & Palvia, 2024).

Sixthly, friends and particularly family members, were highly trusted and their advice was followed almost blindly. In many instances, such adherence to stereotypes of men, and the younger generation knowing more about IT matters could have been regarded as irrational.

Lastly, two aspects about social media participation and frequency of online activity stood out. In the first instance, some interviewees' views were that the more one exposed oneself to a risky environment, the more vulnerable one was. In the second instance, statements such as: "Oh, I buy lots of things online and nothing has ever happened to me" seemed to suggest an element of complacency. This is in line with De Kimpe et al. (2018) who found that extent of online activity led to (over)confidence.

5. Discussion

Findings indicate a variety of threat/harm awareness and experience. Financial damage occurred frequently, and often significant psychological harm. Various demographic and personality factors seemed to contribute to the vulnerability and also the favoured mitigation tactics.

Many influences worked in concert. For instance, age probably means eventual retirement – hence reduction in updates from IT departments, as well as reduction of exposure to colleague's anecdotes. There would also be the assumption that, despite trying one's best to stay abreast of developments, one would miss out on some. Thus, seeking information/guidance, reassurance from friends and family members was common. In addition, once retired and/or elderly, social interaction is usually reduced, and the resultant relative isolation decreases the opportunity for exposure for up to date information.

Then there is the almost blind trust in family members. Many interviewees, irrespective of how adept they might be with IT, relied on their husbands or male members of the family for guidance. The reversion to gender stereotypes of males being more competent with technical matters is surprising. An alternative was to rely on younger members of the family, the assumption being that they would know of latest developments. Overall, though, there seems to be a very strong trust in family members – whether because they're viewed through rose-coloured spectacles, or because it's assumed they would not provide harmful guidance. It places considerable responsibility on the trustees.

The views on abstinence from social media use would work, to a certain extent but it might be rather like robbing Peter to pay Paul, with an unbalanced loss in other beneficial aspects of socialisation.

Another important influence is the context in which one responds to scam messages. As noted, often alcohol consumption results in a less cautious attitude so one might be less careful in checking all the necessary details. Similarly, distraction or being in a rush might reduce caution - with lamentable results. A similar argument might be proffered with regard to online purchasing behaviour – reduction might result in reduced bargain/good buy opportunities.

It was quite clear that possessing a comprehensive knowledge of all possible scams that might assail one, is impractical, if not impossible. A sound approach might well be to equip oneself with general protective measures, rather than trying to address every type of scam. Such measures should also accommodate modern life and the personality, age and contextual factors that exert an influence on that life.

6. Conclusion

This research contributed meaningful insights into how both the theoretical approach as well as the practical approach to the risk of harm through scams might be enhanced. While support was lent to a number of theories such as the psychological reactance theory (Brehm, 1966) and Lazarus and Folkman's (1984) transactional theory of stress and coping, the main insights were with regard to the protection motivation theory (Rogers, 1995). Not only did the research strongly support the appraisal aspect of the protection motivation theory (Rogers, 1975) whereby the threat was assessed both in terms of the severity and the recipient's perceived vulnerability, but the coping mechanisms were seen as consisting of self-efficacy and response efficacy. While self-efficacy (or not) featured prominently, the response efficacy did not focus so much on the efficacy of the applications being used, but rather on the efficacy of external units, and subjective norms. Thus, proxy control was exercised by reliance

on units such as government bodies, authoritative organisations such as Netsafe, work places and social media, which the users hoped would introduce measures to protect them (Gong et al. 2020). The influence of subjective norms, whereby an individual perceives that significant others believe they should perform a certain action or not (Fishbein & Ajzen, 1975) was exercised by reference to knowledgeable family members. In addition, the moderating effects of personality, age, and context need to be considered in order to provide a more holistic understanding of users' responses to scams.

From a more practical perspective, because financial scams account for the majority of harm incurred, indications are that banks need to be proactive in providing anti-scam warnings and mitigations if response to a scam is realised. In additions, governments, third party agencies such as Netsafe, and social media can all play a significant role in contributing to such efforts. Social marketing campaigns targeted at vulnerable groups such as the elderly would go a long way to creating awareness of the dangers of scams and protective responses.

A typology of users and their scam propensity might come in handy in devising such campaigns. However, further confirmatory research would be needed in order to categorise users. Further research is also necessary into the emotional repercussions of scam victims. That would enhance such a typology.

Overall, this research has highlighted a number of areas that need further examination. Being exploratory in nature, the next steps would be to develop quantitative measures to confirm hypotheses which might develop from this research.

References

Biggs, A., Brough, P. and Drummond, S. (2017) *The handbook of stress and health: A guide to research and practice*, John Wiley & Sons, New York.

Brehm, J.W. (1966) *A theory of psychological reactance,* Academic Press, Oxford.

Clayton, R.B., Land, A., Leshner, G. and Quick, B.L. (2019) "Who fights, who flees? In integration of the LC4MP and psychological reactance theory" *Media Psychology*, Vol 22, No. 4, pp 545-571.

De Kimpe, L., Walrave, M., Hardyns, W., Pauwels, L. and Ponnet, K. (2018) "You've got mail! Explaining individual differences in becoming a phishing target" *Telematics and Informatics*, No. 25, pp 1277-1287.

Deci, E.L. and Ryan, R.M. (1985) *Intrinsic Motivation and Self-Determination in Human Behavior,* Plenum, New York.

Fishbein, M. & Ajzen, I. (1975) Predicting and understanding consumer behavior: Attitude-behavior and correspondence. In Ajzen, I. and Fishbein, M. (eds.). *Understanding Attitudes and Predicting Social Behavior* (pp. 148-172), Prentice-Hall. Englewood Cliffs, NJ.

Furnell, S. and Thomson, K-L. (2009) Recognising and addressing 'security fatigue' Computer Fraud & Security, Iss. 11, pp 7-11.

Goldberg, L.R. (1992). *Goldberg's Big Five Questionnaire* [Database record]. APA PsycTests.

Gong, X., Chen, K.Z.K., Cheung, C.M.K. and Lee, K.K.O. (2020) "What drives self-disclosure in mobile payment systems? The effect of privacy assurance approaches, network externality, and technology complementarity" Information Technology & People, Vol 33, No. 3, pp. 1174-1213.

Hong, Y., Wang, D., Shafiee, M.M. and Warkentin, M. (2024) Formation of cybersecurity awareness: A positive psychological perspective. AMCIS 2024 Proceedings, 17.

Jansen, J. and Van Schaik, P. (2018) "Persuading end users to act cautiously online: A fear appeals study of phishing" *Information Computer Security*, Vol 26, No. 3, pp 264-276.

Kiwibank. Fraud and scam protection. Accessed on 12 December 2024 at: https://www.kiwibank.co.nz/contact-us/security/types-of-scams

Koning, L., Junger, M. and Veldkamp, B. (2024) "Risk factors for fraud victimization: The role of socio-demographics, personality, mental, general, and cognitive health, activities, and fraud knowledge" *International Review of Victimology*, Vol 30, No. 3, pp 443-479.

Langenderfer, J. and Shimp, T.A. (2001) Consumer vulnerability to scams, swindles, and fraud: A new theory of visceral influences on persuasion Psychology & Marketing, Vol 18, No. 7, pp 763-783.

Lazarus, R.S. and Folkman, S. (1984) *Stress, appraisal and coping,* Springer, New York.

Li, Y. and Siponen, M. (2022) "Citizens' cybersecurity behavior: Some major challenges" *IEEE Security & Privacy*, Vol 20, No. 1, pp 54-61.

Litman, J.A. (2010) "Relationships between measures of I- and D-type curiosity, ambiguity tolerance, and need for closure: An initial test of the wanting-liking model of information seeking" *Personality and Individual Differences*, Vol 48, No. 4, pp 397-402.

Litman, J.A. and Spielberger, C.D. (2003) "Measuring epistemic curiosity and its diversive and specific components" *Journal of Personality Assessment*, No. 80, pp 75-86.

The Merriman-Webster Dictionary. Accessed 12 December 2024 online at: https://www.merriam-webster.com/dictionary/scam

Mohsin, M. and Palvia, P. (2024) "Unravelling the role of fatigue in cybersecurity behavior" *ICIS 2024 Proceedings*, Bangkok, Thailand, No. 14, 3037.

Netsafe (2024) Accessed 12 December 2024 at: https://www.netsafe.org.nz
Olivier, S., Burls, T., Fenge, L. and Brown, K. (2015) "Winning and losing": Vulnerability to mass marketing fraud" *The Journal of Adult Protection*, Vol 17, No. 6, pp 360-370.
Pham, H.C., Brennan, L. and Furnell, S. (2019) "Information security burnout: Identification of sources and mitigating factors from security demands and resources" *Journal of Information Security and Applications*, No. 46, pp 96-107.
Rogers, R.W. (1975) "A protection motivation theory of fear appeals and attitude change" *Journal of Psychology*, Vol 91, No. 1, pp 93-114.
Sarno, D.M. and Black, J. (2024) "Who gets caught in the Web of lies? Understanding susceptibility to phishing emails, fake news headlines, and scam text messages" *Human Factors*, Vol 66, No. 6, pp 1742-1753.
Scamwatch (2024) *Scam statistics*. Accessed 12 December 2024 at: https://www.scamwatch.gov.au/research-and-resources/scam-statistics
Schaufeli, W.B. and Bakker, A.B. (2004) "Job demands, job resources, and their relationship with burnout and engagement: a multi-sample study" *Journal of Organisational Behavior*, No. 25, pp 293-315.
Shete, N.L., Maddel, M and Shaikh, Z. (2024) "A comparative analysis of cybersecurity scams: Unveiling the evolution from past to present" *9th International Conference for Convergence in Technology*, Pune, India, 5-7 April.
Tambe Ebot, A.C., Siponen, M. and Topalli, V. (2023) "Towards a cybercontextual transmission model for online scamming" *European Journal of Information Systems*, Vol 33, No. 4, pp 571-596.
Thompson, N., McGill, T. and Narula, N. (2024) "No point worrying" – The role of threat devaluation in information security behavior" *Computers & Security*, Vol. 143, No. 103897, pp 1-12.
Waldinger, R.J. and Schulz, M.S. (2010) " Facing the music or burying our heads in the sand? Adaptive emotion regulation in mid-life and late life" *Research in Human Development*, Vol 7, No. 4, pp 292-306.
Whitty, M.T. (2020) "Is there a scam for everyone? Psychologically profiling cyberscam victims" *European Journal on Criminal Policy and Research,* No. 26, pp 399-409.
Williams, E.J., Beardmore, A. and Joinson, A.N. (2017) "Individual differences in susceptibility to online influence: A theoretical review" *Computers in Human Behavior*, No. 72, pp 412-421.
Yu, L. et al. (2023) "Vulnerability of older adults to government impersonation scams" *JAMA Network Open*, Vol 6, No. 9, pp 1-10.