Contextual Factors as Moderators of Demographic Effects on Phishing Victimization

Lina Zhou[1]
Belk College of Business, UNC Charlotte, Charlotte, NC, USA

Zhe Fu
College of Computing and Informatics, UNC Charlotte, Charlotte, NC, USA

Dongsong Zhang
Belk College of Business, UNC Charlotte, Charlotte, NC, USA

ABSTRACT

Phishing is a type of serious cybersecurity threat. Increasing effort has been made for understanding the determinants of phishing susceptibility, yet existing findings remain inconsistent when it comes to the effects of demographic factors. Moreover, phishing victimization is a related but distinct concept from phishing susceptibility. Studies have identified contextual factors in responding to phishing attacks. However, these contextual factors are *ad hoc* and do not address the development of theories. There is a scarcity of empirical research examining how contextual factors influence the determinants of phishing victimization. The study addresses these gaps by investigating the moderating effect of three contextual factors on the demographic determinants of phishing victimization. We develop hypotheses by drawing on theories from multiple disciplines and test them with real-world phishing data collected over an 18-month period. Our results not only support most of the hypotheses but also help explain the inconsistencies found in existing literature. The findings contribute to advancing phishing prevention and detection measures.

Keywords: phishing victimization, email phishing, context, cognitive stress, fear appeal, social engineering, moderating effect.

[1] Corresponding author. lzhou8@charlotte.edu +1 704 687 1976

INTRODUCTION

Phishing attacks pose a severe threat due to their ability to exploit human vulnerabilities through social engineering tactics. These attacks can lead to significant financial losses, data breaches, and exposure of confidential or private information. Despite the rising awareness of and investment in cybersecurity, phishing remains a leading cause of cyber incidents, with reports indicating that over 70% of security breaches begin with phishing emails (Lumpur 2020; Security 2024; Wright et al. 2023). The financial impact of phishing emails is staggering, with U.S. businesses alone losing over $2.9 billion in 2023 due to phishing-related business email compromises (IC3, 2023). The rise of ransomware further amplifies the danger of phishing, making it a persistent and escalating risk for organizations globally.

There has been increasing research on the development of countermeasures for email phishing. Existing research categorizes factors that influence phishing victimization into three primary categories, including demographic, psychosocial (Tornblad et al. 2021), and contextual factors (Greitzer et al. 2021). Demographic factors include age, gender, education level, and technical experience, etc., which can affect an individual's ability to recognize and respond to phishing attempts. Psychosocial factors, including personality traits and interpersonal behaviors, may increase an individual's vulnerability to phishing attempts. Context factors encompass technology self-efficacy, level of attention, and the alignment between the user’s context and the content of the phishing attack. Existing research has explored a variety of contextual variables, such as task context (Greene et al. 2018), social interactions (Moody et al. 2011), and cognitive stress (Wright et al. 2023).

However, there remain notable gaps in exploring the interactions between demographic factors and the context of phishing attacks. In addition, previous studies reveal inconsistent

relationship between demographic factors and phishing susceptibility (e.g., Liu et al., 2020; Li et al., 2020). We expect that incorporating contextual factors into phishing victimization analysis could offer valuable insights into this relationship. Furthermore, existing studies have primarily focused on phishing susceptibility (i.e., an individual's likelihood to fall for phishing attempts) (e.g., Sheng et al., 2010; Li et al., 2020) rather than phishing victimization (i.e., someone actually falling for a phishing scheme).

This research aims to investigate the influence of contextual factors on demographic determinants of phishing victimization. Specifically, we examine two contextual factors related to phishing attacks and another associated with the phishing target. We propose hypotheses on the moderating effects of those contextual factors and test them using real-world data collected from an organizational setting over a period of 18 months.

RELATED WORK

In this section, we review two streams of related work: demographic determinants of phishing susceptibility and contextual factors in phishing attacks. Our literature review focuses on phishing susceptibility due to the limited amount of empirical research on phishing victimization. Moreover, the contributing factors to phishing susceptibility and phishing victimization can overlap. For instance, someone highly susceptible may be more likely to become a victim.

Demographic Determinants of Phishing Susceptibility

Existing research has explored how different demographic factors correlate to susceptibility to phishing attacks. For example, Sheng et al. (2010) conducted a roleplay survey to study the relationship between demographics and phishing susceptibility. Their experimental results indicated that gender and age were two key demographics that could predict phishing susceptibility. Liu et al. (2020) investigated the influence of demographic characteristics of

employees on phishing victimization in the workplace, highlighting the significant effects of gender and technical experience of the phishing targets. However, they did not find a significant relationship between age and phishing victimization. Li et al. (2020) explored several potential predictors of phishing susceptibility, with a focus on demographic factors (e.g., age, gender, and job position/employment). Their results revealed a significant association between age or job position and phishing susceptibility, while gender was not found to be a determinant of phishing susceptibility. Those research efforts focus on exploring the effect of demographic characteristics of phishing targets on phishing susceptibility without considering the role of contextual factors, despite the latter may influence the target's susceptibility to phishing attacks. Moreover, findings on the effects of demographic factors are inconsistent across studies, further emphasizing the need to account for contextual influences in understanding phishing susceptibility.

Contextual Factors in Phishing Attacks

Phishing attacks occur within a multifaceted context that encompasses psychological, situational, social, and technological elements. We focus on the psychological and situational aspects of context in this study. Phishing targets' psychological states, such as stress, fatigue, and distraction, can make those individuals more susceptible to phishing. Phishing attempts often exploit human emotions, such as fear, curiosity, and urgency, to increase the likelihood of success. Moody et al. (2011) showed that social and psychological factors, including personality traits (e.g., trust, curiosity, and risk propensity) and Internet experience (e.g., Internet community identification and Internet anxiety), significantly influenced an individual's likelihood of being victimized by phishing attacks.

Wright et al. (2023) conducted a study where employees in the finance division of a large university were exposed to simulated email phishing attempts during their regular work activities.

Their study collected survey data on three individual-level psychological factors that reflect employees' familiarity with IT knowledge and work-task network (i.e., reliance on IT support, task centrality, and IT advice centrality), and two workgroup-level psychological factors related to the cognitive demands of employees' workgroup responsibilities (i.e., workgroup time pressure and workgroup resilience). Their findings suggest that individuals' susceptibility to phishing attacks is influenced by both their IT knowledge and the workgroup context in which employees process information. Greene et al. (2018) focused on how an employee's task context could influence phishing susceptibility. They found that phishing susceptibility increased when the message aligned with an employee's work context, making phishing messages seem more legitimate and reducing deeper scrutiny from employees.

Previous studies exploring the psychological and situational factors influencing phishing susceptibility have three main limitations. First, they often fail to examine how contextual factors may impact the effects of other variables on phishing susceptibility. Second, existing empirical studies have overlooked the role of cognitive stress of the phishing target in phishing victimization. Third, these studies typically categorize phishing content based on topic domains rather than the tactics that attackers employ to manipulate recipients' psychological state and increase their impulsivity in responding to phishing messages. Phishing tactics refer to specific psychological or strategic methods employed to deceive recipients, such as leveraging urgency and fear appeal, which exploit emotional states to cloud judgment and drive impulsive decisions. Lastly, existing work focuses on phishing susceptibility instead of phishing victimization.

HYPOTHESIS DEVELOPMENT

To address the above-mentioned limitations and shed light on the inconsistent findings of previous studies regarding the relationship between demographic factors and phishing

susceptibility, we aim to understand the role of contextual factors in phishing victimization in this study. While there are overlaps among the factors contributing to phishing susceptibility and victimization, victimization may depend on both individual susceptibility and other additional factors, such as attackers' tactics and the situational context of a phishing target. In this section, we propose hypotheses by drawing on the related theories.

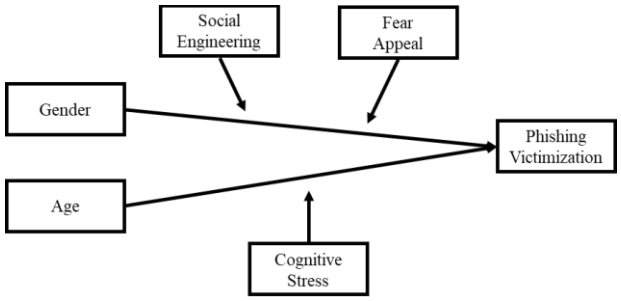

Figure 1. The Research Model

Bronfenbrenner's ecological theory (Bronfenbrenner 1977) and person-process-context model (Bronfenbrenner 1979) emphasize the significance of different layers of contextual factors, ranging from immediate (e.g., individual) to larger and broader contexts (e.g., cultural and societal), in shaping individuals' thoughts, feelings, and behaviors. This approach highlights the dynamic interplay between individuals and their contexts, recognizing that individuals' behavior cannot be fully understood in isolation from social and environmental factors that surround it (Bronfenbrenner 1977). Security research has highlighted the role of context or contextualism. Karyda et al. (2005) proposed a theoretical framework based on the theory of contextualism. The contextual factors for the application of information security policies include user participation, user goals, organizational culture, and so on. Cuppens and Cuppens-Boulahia (2008) proposed a context taxonomy, consisting of user-declared context (e.g., user purpose), provisional context (e.g., previous behavior), prerequisite context (e.g., depending on characteristics that join the different roles or entities in an event), temporal context (e.g., the time when an event occurs),

spatial context (e.g., a physical location or system architecture), and so on. We extend these theories and theoretical models to the context of phishing victimization by proposing that contextual factors may influence phishing victimization. Our research model is shown in Figure 1.

These contextual factors may influence both the strategies employed by attackers and the responses of potential victims. Routine Activity Theory (RAT) (Cohen and Felson 1979) highlights the relation of criminal events with space and time and its ecological nature. It posits that the occurrence of criminal events is influenced by the daily routines and activities of individuals. According to RAT, for a crime to take place, three essential elements must converge, including a motivated offender (e.g., a person who has the intention to launch a phishing attack), a suitable target (e.g., a person or asset perceived as vulnerable or valuable), and the lack of a capable guardian (e.g., security measures). They serve as contextual factors that prompt phishing attacks. Furthermore, understanding the circumstances that trigger criminal events enables changing those conditions and reducing the likelihood of their occurrence (Clarke 2008). Social engineering is a tactic frequently used in phishing attacks, where attackers exploit personal information, relationships, or behavior gathered about the phishing target (real or fabricated) to mislead individuals into revealing sensitive information, such as passwords, account numbers, or other personal identification details (Abraham and Chengalur-Smith, 2010). By making phishing messages more convincing and persuasive, social engineering is expected to influence the effect of demographic factors. Therefore, we propose the following hypotheses.

H1. Social engineering moderates the effect of age on phishing victimization.

H2. Social engineering moderates the effect of gender on phishing victimization.

Stress can impair individuals' attention, memory, and judgment, making them more vulnerable to deceptive communication and less able to critically evaluate phishing attempts

(Canfield and Fischhoff 2018). High stress levels can negatively affect individuals' cognitive functioning, leading them to rush into decisions. The diminished capability of cognitive processing can increase the likelihood of falling for phishing attacks. In addition, stressed individuals may be more likely to be victims of phishing tactics such as urgency and fear appeal, as their psychological state can impair their judgment and increase impulsivity. Further, stress can affect attention span and focus, making it harder for phishing targets to critically evaluate suspicious emails. Individuals under stress may have altered risk perceptions, leading them to underestimate threat. As a result, the effects of demographic factors are expected to vary with individuals' level of cognitive stress.

H3. Cognitive stress moderates the effect of age on phishing victimization.

H4. Cognitive stress moderates the effect of gender on phishing victimization.

Fear appeal is designed to evoke fear by highlighting the severity of a threat and the target's vulnerability to that threat. Such threats often use fear of consequences, such as the threat of rejection of tax return and warning of policy violation, to mislead victims into compliance, making targets worry about the repercussions in their workplace, personal finance, and other valuable assets. It creates a powerful emotion that makes the target to feel compelled to respond or act without thinking (Yeoh et al. 2022). As a result, the fear appeal may impair individuals' ability to critically evaluate the content. Thus, we propose the last set of hypotheses as follows.

H5. Fear appeal moderates the effect of age on phishing victimization.

H6. Fear appeal moderates the effect of gender on phishing victimization.

METHOD

Dataset

We used data collected from a phishing simulation and education project conducted by a university IT department on the east coast of the U.S. As part of the project, the university had a

crafted phishing email sent to the official email accounts of its employees once a month. The emails varied in their content. The responses of university employees to those phishing emails were monitored and logged, including whether someone clicked a hyperlink within a phishing email that redirected him/her to another webpage. If an employee clicked the link or downloaded or opened an attachment that he was not supposed to, he would receive an alert informing him that he had fallen victim to a phishing attempt. Along with this notification, he would also be provided with educational material on how to identify phishing attacks. In this study, these individuals were treated as victims of phishing attacks. We used de-identified data collected over 18 months.

Variables

The dependent variable is phishing victimization, which is a binary variable (Yes or No) defined as whether or not an employee clicks on a hyperlink embedded in a phishing email. The independent variables consist of two demographic factors, including gender (male or female) and age, while age is divided into three groups: young (20–34), middle (35–59), and old age (60 and above). Additionally, we consider three contextual factors, including social engineering, cognitive stress, and fear appeal. Cognitive stress was operationalized as whether a phishing attack was received during regular Spring and Fall semesters (high) or during breaks (low). We categorize coded social engineering and fear appeal using a multi-method approach based on the entire phishing emails. Two coders first manually annotated the data separately and then discussed the conflicting coding results to reach a consensus. One of the coders had two decades of research experience in phishing, and the other was very familiar with the phishing literature. In addition, we also leveraged GPT-4 to generate categorization suggestions for the phishing emails and used them as additional input for determining the labels. Cognitive stress is expected to be high during the regular semesters for several reasons: 1) faculty typically teach with fixed class time and other

obligations, which can lead to a hectic routine; 2) faculty often have service commitments at both department and university levels, leading to packed schedules and constant demands. In contrast, their stress levels tend to be lower during the summer and winter breaks when faculty often have reduced or no teaching responsibilities, allowing for self-reflection and thoughtful adjustment.

RESULTS

Moderating Effects of Social Engineering

Table 1 presents the descriptive statistics of phishing victimization, with and without social engineering, across different gender and age groups. We performed repeated measures ANOVA to test the possible moderating effect of social engineering on the effects of the two demographic variables. The omnibus analysis results show that age has a significant effect on phishing victimization ($F(1.222, 19.549)=6.127$, $p<.05$). However, none of the other main effects and interaction effects was significant ($p>.1$). The post hoc contrast analysis of age reveals a significant difference between young and old age groups ($p<.05$), and between middle and old age groups ($p<.01$). We further conducted pairwise comparisons of age groups with and without social engineering separately. The results show that when social engineering was employed, there is a significant difference between the young and old age groups ($p<.05$), and between the middle and old age groups ($p<.05$). However, when social engineering was not used, no significant difference was observed between young and old age groups ($p>.1$), while the difference between the middle and old age groups was marginally significant ($p<.1$). Similarly, we analyzed the effect of gender for both conditions, but the results did not yield a significant effect for either ($p>.01$).

In addition to conducting analyses at the level of phishing emails, we also tested the hypotheses at the user level. Given the presence of multiple phishing emails that both employed (i.e., confirm payment) and did not (e.g., fax received) social engineering, we devised a strategy

to select a matching sample for a rigorous examination of moderating effects. For instance, we first randomly selected one phishing email that did not incorporate social engineering and fear appeal, and did not involve cognitive stress, and another phishing email solely utilized social engineering. We then compared them using ordinal regression analysis. The results revealed a marginally significant difference between middle and old age groups ($p<.1$) when phishing emails employed social engineering tactics. However, no significant differences were detected among age groups ($p>.1$) when social engineering was absent. Additionally, no significant effect was detected for gender ($p<.1$) either. Thus, hypothesis H1 was supported, yet hypothesis H2 was not supported.

Table 1. Descriptive Statistics (mean (std)) of Phishing Victimization w/ and w/o Social Engineering

Gender	Age	w/o social engineering	w/ social engineering
Male	Young	0.0434 (0.0367)	0.0984 (0.0763)
	Middle	0.0433 (0.038)	0.1081 (0.1084)
	Old	0.0705 (0.119)	0.0705 (0.0639)
Female	Young	0.0537 (0.0573)	0.1052 (0.0864)
	Middle	0.0496 (0.0479)	0.1045 (0.0919)
	Old	0.0650 (0.0624)	0.1284 (0.1178)

Table 2. Pairwise Comparison Results of Age for without and with Social Engineering

Age group		Mean difference (I-J) (STE)	
I	J	w/o social engineering	w/ social engineering
Young	Middle	.002 (.008)	-.005 (.006)
Middle	Old	-.021 (.01)†	-.023 (.008)*
Old	Young	.019 (.016)	.028 (.013)*

Notes: *: $p<.05$; †: $p<.1$

Moderating Effects of Cognitive Stress

We present the descriptive statistics of phishing victimization for all gender and age group combinations for phishing attacks under low and high cognitive stress conditions in Table 3. We performed repeated measures ANOVA to test whether cognitive stress moderates the effects of the demographic variables. The omnibus analysis results show that age has a significant effect on phishing victimization ($F(1.218, 19.487)=6.001$, $p<.05$). However, none of the other main effects

and interaction effects was significant (p>.1). The post hoc contrast analysis of age reveals a significant difference between young and old age groups (p<.05), and between middle and old age groups (p<.01). We further conducted pairwise comparisons of age groups for both low stress and high stress conditions separately. The results indicate a significant difference between young and old age groups (p<.05), and between middle and old age groups (p<.01) when cognitive stress is high. However, no significant difference was found among the age groups when the cognitive stress was low (p>.1). Similarly, we analyzed the effect of gender under both low and high stress conditions, but the results did not yield a significant effect for either condition (p>.01).

To test the hypotheses at the user level, we chose one phishing email when the cognitive stress level was high (i.e., distributed in September), and compared it with another email characterized as low cognitive stress, which did not employ fear appeal or social engineering. The results indicate a marginally significant difference between middle and old age groups (p<.001), as well as between young and old age groups (p<.001) when the cognitive stress was high. However, no significant difference was observed between any pair of age groups (p>.1) when cognitive stress was low. Additionally, the effect of gender was marginally significant (p<.1) under high cognitive stress conditions. Therefore, hypothesis H3 was supported, while hypothesis H4 was partially supported.

Table 3. Descriptive Statistics (mean (std)) of Phishing Victimization with Different Levels of Cognitive Stress

Gender	Age	Low stress	High stress
Male	Young	0.0705 (0.0792)	0.0812 (0.0641)
	Middle	0.0745 (0.110)	0.0881 (0.0843)
	Old	0.0965 (0.119)	0.115 (0.0924)
Female	Young	0.0643 (0.0762)	0.0984 (0.0812)
	Middle	0.0656 (0.0817)	0.0943 (0.0822)
	Old	0.0783 (0.0827)	0.1199 (0.0114)

Table 4. Pairwise Comparison Results of Age for Different Levels of Cognitive Stress

Age group		Mean difference (I-J) (STE)	
I	J	Low	High
Young	Middle	-.003 (.008)	-.001 (.006)
Middle	Old	-.017 (.010)	-.026 (.008) **
Old	Young	.02 (.016)	.027 (.013)*

Notes: **: p<.01; *: p<.05

Moderating Effects of Fear Appeal

We present the descriptive statistics of phishing victimization for all gender and age group combinations for phishing attacks with and without fear appeal separately in Table 5.

The omnibus analysis results show that fear appeal has a significant effect on phishing victimization ($F(1.219, 19.503)=5.666$, $p<.05$). In addition, there is a significant interaction effect between gender and fear appeal ($p<.05$). However, none of the other main effects and interaction effects is significant ($p>.1$). The post hoc contrast analysis of age reveals a significant difference between the young and old age groups ($p<.05$) and between the middle and old age groups ($p<.01$). We then performed pairwise comparisons of age for both conditions. The results reveal a marginally significant difference between the young and old age groups ($p<.1$) and a strongly significant difference between the middle and old age groups ($p<.01$) when the fear appeal was absent. However, no significant difference was found among the age groups when fear appeal was employed ($p>.1$). Similarly, we analyzed the effect of gender in both contexts separately. The results reveal a marginally significant difference between male and female recipients ($p<.1$) when fear appeal was employed. However, there were no significant differences when phishing emails did not include a fear appeal.

At the user level, we also tested the hypotheses by selecting a phishing email that employed fear appeal (e.g., warning of critical security vulnerabilities such as malware risks) but no social engineering or cognitive stress, and compared it with another email that did not involve fear appeal,

social engineering, or cognitive stress. The results indicated a marginally significant difference between middle and old age groups ($p<.1$) and between young and old age groups ($p<.1$) only when the phishing email employed fear appeal. In addition, there was a strong significant effect of gender ($p<.001$) when fear appeal was present. Thus, both hypotheses H5 and H6 were supported.

Table 5. Descriptive Statistics (mean (std)) of Phishing Victimization w/ and w/o Fear Appeal

Gender	Age	w/o fear appeal	w/ fear appeal
Male	Young	0.0806 (0.0618)	0.0698 (0.0857)
	Middle	0.0867 (0.0805)	0.0752 (0.1203)
	Old	0.1130 (0.0881)	0.0968 (0.1303)
Female	Young	0.0991 (0.0785)	0.0573 (0.0786)
	Middle	0.0953 (0.0779)	0.0589 (0.0883)
	Old	0.1179 (0.1091)	0.0753 (0.0906)

Table 6. Pairwise Comparison Results of Age for without and with Fear Appeal

Age group		Mean difference (I-J) (STE)	
I	J	w/o fear appeal	w/ fear appeal
Young	Middle	-.001 (.006)	-.004 (.009)
Middle	Old	-.024 (.008)**	-.019 (.011)
Old	Young	.026 (.012)†	.022 (.017)

Notes: **: $p<.01$; †: $p<.1$

DISCUSSION

Major Findings

Our analysis results at both phishing email and user levels show that social engineering, fear appeal, and cognitive stress all moderate the effect of age on phishing victimization. Age has an effect only when a phishing attack employs social engineering and fear appeal, and when the cognitive stress is high. Specifically, old-age groups are more vulnerable to phishing victimization compared to young- and middle-aged groups. In addition, the effects of fear appeal become more complex when examining demographic determinants at both phishing email and individual levels.

The analysis results also show that fear appeal moderates, and cognitive stress partly moderates, the effect of gender on phishing victimization. Gender has an effect only when the

phishing attack vector employs fear appeal and when the cognitive stress is high. Specifically, females are more vulnerable to phishing victimization compared to males when the cognitive stress is high, while males are more vulnerable when fear appeal is present.

Research Contributions

This study makes multifold contributions to research on phishing. First, unlike most existing studies focusing on phishing susceptibility, we investigated a riskier behavior - phishing victimization. Second, we explored the impact of cognitive stress on the relationship between demographic factors and phishing victimization for the first time. Third, while fear appeal and social engineering are common phishing tactics, their moderating effects on the determinants of phishing victimization have not been empirically investigated before. This study addresses this gap. Our findings provide explanations for some of the inconsistent findings in the literature. Last but not least, we developed a multi-level approach to rigorously test the moderating effects of contextual factors. Exploring these aspects enhances our understanding of phishing victimization and its underlying mechanism, thereby facilitating the development of intervention measures.

Limitations and Future Work

First, the data were collected from the employees of a higher education institution, which may not generalize to other types of organizational context. Second, while our data is longitudinal, it does not support time series analysis due to data anonymization. Third, there are additional contextual factors that influence phishing victimization that are not addressed in this study, such as the time of phishing message distribution and the fit or relevance of phishing email content to employees' job responsibilities. These factors are interesting topics for future research.

REFERENCES

Abraham, S., & Chengalur-Smith, I. (2010). “An overview of social engineering malware: Trends, tactics, and implications.” *Technology in Society*, 32(3), 183-196. https://doi.org/https://doi.org/10.1016/j.techsoc.2010.07.001

Bandura, A. 1986. "The Explanatory and Predictive Scope of Self-Efficacy Theory," *Journal of Social and Clinical Psychology* (4:3), pp. 359-373.

Bronfenbrenner, U. 1977. "Toward an Experimental Ecology of Human Development," *American Psychologist* (32:7), pp. 513-531.

Bronfenbrenner, U. 1979. The Ecology of Human Development Experiments by Nature and Design. *Harvard University Press*.

Canfield, C. I., and Fischhoff, B. 2018. "Setting Priorities in Behavioral Interventions: An Application to Reducing Phishing Risk," *Risk Analysis* (38:4), pp. 826-838.

IC3 (Internet Crime Complaint Center). "2023 Internet Crime Report," Federal Bureau of Investigation, https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf.

Clarke, R. V. 2008. "Situational Crime Prevention," in *Environmental Criminology and Crime Analysis*, R. Wortley and L. Mazerolle (eds.). London: Willan.

Cohen, L. E., and Felson, M. 1979. "Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociologial Review*, 44 (4), 588-608."

Cuppens, F., and Cuppens-Boulahia, N. 2008. "Modeling Contextual Security Policies," *International Journal of Information Security* (7:4), pp. 285-305.

Greene, K., Steves, M., Theofanos, M., and Kostick, J. 2018. "User Context: An Explanatory Variable in Phishing Susceptibility," *Workshop on Usable Security (USEC) 2018*, San Diego, CA, USA.

Greitzer, F. L., Li, W., Laskey, K. B., Lee, J., and Purl, J. 2021. "Experimental Investigation of Technical and Human Factors Related to Phishing Susceptibility," *ACM Transactions on Social Computing* (4:2), pp. 1 - 48.

Karyda, M., Kiountouzis, E., and Kokolakis, S. 2005. "Information Systems Security Policies: A Contextual Perspective," *Computers & Security* (24:3), pp. 246-260.

Li, W., Lee, J., Purl, J., Greitzer, F., Yousefi, B., and Laskey, K. 2020. "Experimental Investigation of Demographic Factors Related to Phishing Susceptibility," In *Proceedings of the 53rd Hawaii International Conference on System Sciences (HICSS '20)*, pp. 2240-2249.

Lin, T., Capecci, D. E., Ellis, D. M., Rocha, H. A., Dommaraju, S., Oliveira, D. S., and Ebner, N. C. 2019. "Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content," *ACM Trans. Comput.-Hum. Interact*. (26:5), p. Article 32.

Liu, Z., Zhou, L., and Zhang, D. 2020. "Effects of Demographic Factors on Phishing Victimization in the Workplace," In *Proceedings of the PACIS*.

Lumpur, K. 2020. "91% of All Cyber Attacks Begin with a Phishing Email to an Unexpected Victim: 8 Simple Practices Towards Cyber-Resilience".

McCaul, K. D., Sandgren, A. K., O'Neill, H. K., and Hinsz, V. B. 1993. "The Value of the Theory of Planned Behavior, Perceived Control, and Self-Efficacy Expectations for Predicting Health-Protective Behaviors," *Basic and Applied Social Psychology* (14:2), pp. 231-252.

Moody, G., Galletta, D., Walker, J., and Dunn, B. 2011. "Which Phish Get Caught? An Exploratory Study of Individual Susceptibility to Phishing," *European Journal of Information Systems* (26:6), pp. 564-584.

Rogers, R. W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change1," *The Journal of Psychology* (91:1), pp. 93-114.

Security, T. 2024. "130 Cyber Security Statistics: 2024 Trends and Data." Fortra.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., and Downs, J. 2010. "Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Atlanta, Georgia, USA: Association for Computing Machinery, pp. 373–382.

Tornblad, M. K., Jones, K. S., Namin, A. S., and Choi, J. 2021. "Characteristics That Predict Phishing Susceptibility: A Review," In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, pp. 938-942.

Wright, R., Johnson, S., and Kitchens, B. 2023. "Phishing Susceptibility in Context: A Multilevel Information Processing Perspective on Deception Detection," *MIS Quarterly* (47:2).

Yeoh, W., Huang, H., Lee, W.-S., Al Jafari, F., and Mansson, R. 2022. "Simulated Phishing Attack and Embedded Training Campaign," *Journal of Computer Information Systems* (62:4), pp. 802-821.