1-25-2024

Investigating Age-Related Factors in Phishing Susceptibility: A Focus on Decision-Making Processes in HCI Context

Babak Safaei
McMaster University, safaeb1@mcmaster.ca

Milena Head
McMaster University, headm@mcmaster.ca

Investigating Age-Related Factors in Phishing Susceptibility: A Focus on Decision-Making Processes in HCI Context

Babak Safaei
DeGroote School of Business
McMaster University
safaeb1@mcmaster.ca

Milena Head
DeGroote School of Business
McMaster University
headm@mcmaster.ca

ABSTRACT

The widespread adoption of digital interfaces, amplified by the worldwide drive for digital inclusion, presents unique challenges, especially for older adults navigating the online realm. This research investigates aging populations' pronounced susceptibility to phishing schemes—a sophisticated digital threat with significant financial and societal implications. This study seeks to explore human-computer interaction (HCI) security for older adults, examining the interplay of heuristic and deliberate decision-making processes while accounting for age-related cognitive changes, behavioural attributes, and experiential factors. A comprehensive 2x2x2 factorial experimental design is proposed, which integrates variances in message themes (health and finance), gain-loss framing, and age disparities. The research harnesses Neuro Information Systems (NeuroIS) techniques, including EEG and eye-tracking, combined with questionnaires, to capture users' dynamic perceptions during phishing encounters. The anticipated findings aspire to shape HCI guidelines tailored for aging populations while contributing to developing user-centric security awareness programs and digital interfaces, mitigating cyber threat repercussions.

Keywords

Phishing susceptibility, digital interfaces, older adults, dual process theories, cognitive aging, HCI security.

INTRODUCTION

Internet expansion and rapid technological developments over the past decade have made computers integral to people's everyday lives. Alongside their myriad benefits, these developments have also escalated intricate IT threats and misuse, often termed the "dark sides of IT" (Boroon et al., 2021). Phishing, a sophisticated social engineering tactic, mirrors legitimate messages to exploit human behaviour and cognitive biases, extract information, bypass security measures, and capitalize on inherent vulnerabilities in human-computer interaction (HCI) (Goel, 2017). Despite the older adult population's pronounced vulnerability to online threats, research focusing on their unique HCI challenges remains limited (Shang et al., 2022). The amplified exposure of older adults to digital services, especially post-pandemic, combined with an often-prevalent lack of security awareness, risks their well-being, optimal aging, and independence (Burton et al., 2022).

Research on decision-making changes related to aging presents mixed findings (Bruine de Bruin et al., 2012), which extends to the domains of phishing susceptibility and technology adeptness (Sarno et al., 2023). Natural aging accompanies cognitive and functional declines, affecting older adults' information processing and risk responses (Hassandoust et al., 2020). While fluid intelligence (e.g., reasoning) naturally wanes with age, the experiential knowledge (i.e., crystalized intelligence) and potential protective attributes gained over time may counterbalance this decline, reflected in decision-making within the digital realm (Shang et al., 2022). Although older adults exhibit adaptive cognitive and experiential capabilities, these mechanisms might not always translate seamlessly to ICT competencies. The current digital divide emphasizes this, showing older adults' general lag in IT engagement, which influences their IT norms recognition and online vulnerability (Choudrie, 2021; Lu et al., 2022).

While anti-phishing automated tools often falter against sophisticated threats, the burden shifts to user judgments, highlighting the importance of delving into human-centric factors influencing phishing interactions (Jaeger and Eckhardt, 2021). This study adopts a multifaceted lens to investigate decision-making determinants and antecedents in phishing susceptibility across various age groups. We propose a model investigating key individual-static, contextual-dynamic, and message characteristics that influence phishing susceptibility while considering age, experience, and HCI dynamics. This approach offers a holistic view of the "why" and "how" aspects, addressing the research questions noted below.

1. Why do older and younger adults succumb to online phishing schemes?
2. How do individual, contextual, and message attributes differentially influence decision-making processes and phishing susceptibility across older and younger adults?

Recognizing the importance of users' perceptions of a risky situation and interface experiences in responding to online

threats, this proposed study emphasizes the need for HCI-focused solutions tailored to the unique needs of older adults. Such an approach is essential for effective strategy formulation against online threats, aiming to bridge the digital divide in an increasingly digital world.

THEORETICAL DEVELOPMENT

This study adopts a multi-theoretical approach, blending cognitive, behavioural, and aging insights. We focus on phishing within the HCI and information security framework, emphasizing intuitive and bounded rational decision-making. Central to our study is the Heuristic-Systematic Model (HSM) (Dennis and Minas, 2018), which highlights an interplay between deliberate and heuristic processing, resonating with dual-process theories (Evans, 2008). These theories underscore how System 1's rapid, intuitive processing often predominates due to the principle of least effort in decision-making, while System 2 is activated in more deliberate thought processes. This framework is particularly relevant for examining how aging influences cognitive effort and susceptibility thresholds in phishing exposures. While System 1 often leads to susceptibility due to biases in quick reactions to deceptive cues, analytical processing may still be swayed by heuristic biases (Hassandoust et al., 2020). Aging factors shift reliance towards heuristic and affective processes, impacting phishing vulnerability due to the primary focus on superficial message elements (Morgan et al., 2019). This underscores the significance of tailoring HCI designs, particularly for older users, to accommodate the cognitive shifts and enhance security decision-making.

Integrating the Truth-Default Theory (TDT) (Levine, 2014), we examine how age amplifies truth-biased thinking, increasing phishing susceptibility. Combining TDT with dual-process theory reveals that humans initially view messages as truthful, increasing vulnerability to heuristic biases. Prospect Theory (PT) (Kahneman and Tversky 1979) is also incorporated to understand the role of loss and gain perceptions in decision-making. PT deviates from normative decision models to highlight subjective interpretations, including the framing effect: individuals lean towards risk aversion when confronted with potential gains and risk-seeking with potential losses, affecting heuristic thinking (Dennis and Minas, 2018). Age-related studies link PT to heightened susceptibility to cognitive biases and overestimating unlikely events in older adults (Hess, 2015). We also employ Selective Engagement Theory (Hess, 2006) to explain how older adults effectively allocate mental resources based on task relevance, compensating for the effects of cognitive decline.

RESEARCH MODEL AND HYPOTHESES

The research model, depicted in Figure 1, investigates phishing susceptibility by examining key individual, contextual, and behavioural attributes. The following sections outline the model and present our hypotheses.

Individual Static Characteristics

As a crucial factor in problem-solving, fluid intelligence influences phishing susceptibility. Age-related cognitive decline and amplified reliance on truth-biased heuristics might impair older individual's ability to detect phishing (Morgan et al., 2019). Thus, we propose:

- H1: Fluid cognitive ability is negatively related to phishing susceptibility
- H1b: The negative effect of fluid cognitive ability on phishing susceptibility would be stronger for older adults than younger adults

Security training and phishing victimization experience can influence phishing perception and response (Moody et al., 2017). Such experiences can shift truth bias and promote protective behaviour, mainly through System 2 processing (Hassandoust et al., 2020). This process might be moderated by age, especially considering age-related cognitive decline, challenges older adults face in applying learned rules, their reliance on past experiences in decision-making, and discrepancies in transferring crystallized intelligence to HCI (Shang et al., 2022). Although some studies suggest that experience could lead to overconfidence in phishing detection across ages (Wang et al., 2016), others indicate older adults' improved performance in confidence-related tasks (Bruine de Bruin et al., 2012). Thus, we hypothesize:

- H2: Prior cyber victimization experience is negatively related to phishing susceptibility
- H2b: The negative effect of prior cyber victimization experience on phishing susceptibility would be stronger for older adults than younger adults
- H3: Prior security training experience is negatively related to phishing susceptibility
- H3b: The negative effect of prior security training experience on phishing susceptibility would be stronger for younger adults than older adults

Contextual Dynamic Characteristics

Cognitive engagement, allocating mental resources to comprehend a situation, influences behaviour in phishing scenarios (Ayaburi and Baidoo, 2023). Higher cognitive engagement is associated with thorough analysis and context-aware behaviour (Vance et al., 2022). Such engagement can be amplified by fear appeals in persuasive phishing content, moving users from a truth bias to a more analytical mindset, drawing attention to suspicious cues, and reducing phishing susceptibility. Older adults might display different engagement levels due to their unique decision-making sensitivities and cognitive resource allocation (Liu et al., 2021). Hence, we propose:

- H4: Higher cognitive engagement is negatively related to phishing susceptibility
- H4b: The negative effect of higher cognitive engagement on phishing susceptibility would be stronger for older adults than younger adults

In phishing scenarios, users' initial trust evolves to caution, affecting their susceptibility to phishing (Abbasi et al., 2021). Perceived risk, a cognitive judgment distinct from emotional responses, is a key predictor of security behaviour (Vance et al., 2014). Although users' initial threat responses are automatic, increased risk perceptions trigger analytical thinking, enhancing cue detection and reducing phishing susceptibility. Characterized by cautious behaviour and crystallized intelligence, older adults may perceive and evaluate risks uniquely, sometimes overestimating unlikely events, affecting their decision-making (Hess et al., 2015). Nonetheless, their consistent risk evaluations could mitigate phishing risks (Bruine de Bruin et al., 2012). Thus, we hypothesize:

- H5: Perceived risk is negatively related to phishing susceptibility
- H5b: The negative effect of perceived risk on phishing susceptibility would be stronger for older adults than younger adults

Message Characteristics

Task context and relevance influence human behaviour, with message framing exploiting cognitive vulnerabilities to influence reasoning and phishing responses (Wright and Jensen, 2014). Personalized messages, particularly about group-related concerns, can manipulate users' motivations, leading to a reliance on heuristics. The associated emotional connection can often override deliberate processing, thus elevating phishing success rates. We aim to focus on health and finance-related messages, given their high stakes and growing phishing incidences in these areas, especially among aging individuals. Drawing from PT, aging and health and financial vulnerabilities might lead to riskier behaviour in the face of potential losses (Hess, 2015). As older adults increasingly engage with online banking and electronic health platforms, they might become more susceptible to phishing attacks on concerns like retirement and health. Also, older adults may engage in less intensive cognitive processing but exhibit a heightened sensitivity to personal relevance, possibly leading to more thorough evaluations and balancing out age-related information-processing constraints (Liu et al., 2021). Older adults' potential financial stability and proneness to health concerns make them prime targets for cyberattacks (Gavett et al., 2017). Thus, we hypothesize:

- H6: Messages in the financial and health contexts are positively related to phishing susceptibility compared to messages in a less critical context
- H6b: The positive effect of messages in financial and health contexts on phishing susceptibility is stronger for older adults than younger adults

Framing significantly influences individual behaviour, often to seemingly irrational extents (Dennis and Minas, 2018). Content that invokes motivational drives of acquisition (e.g., gains propelled by hope) and defense (e.g., avoiding loss spurred by fear) can distort judgment, intensify heuristics usage, raising phishing susceptibility, especially for loss frames that promote risk-seeking (Goel et al., 2017). This effect is accentuated among older adults due to their loss-aversion tendencies and cognitive status, affecting their ability to resist framing (Bruine de Bruin et al., 2012). Thus, we hypothesize:

- H7: Messages with loss frames are more likely to increase phishing susceptibility than messages with gain frames.
- H7b: The effect of message framing on phishing susceptibility is moderated by age, indicating differential susceptibility to gain and loss-framed messages across age groups

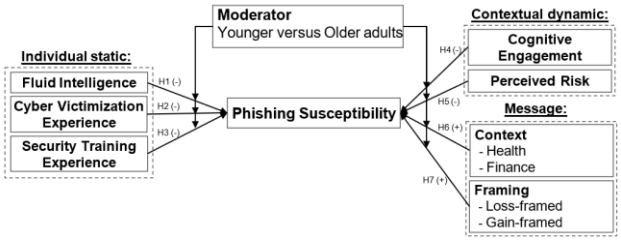

Figure 1. Overview of the proposed research model

METHODOLOGY

A lab experiment will be conducted to examine factors influencing email phishing susceptibility. The experiment will follow a 2x2x2 factorial design, where the initial factor manipulates message content tiers (health versus finance), the subsequent factor manipulates message framing (gain versus loss), and the last factor differentiates between age demographics (older versus younger adults, with 65 years as the age threshold). To ensure content validity, we will employ measurement scales primarily derived from existing literature and tailored to this study. Fluid cognitive ability will be gauged using the shortened Raven's Progressive Matrices, focusing on problem-solving and intellectual capacity (Raven et al., 2003). Perceived risk will be evaluated using threat severity and risk perception questionnaires (Johnston and Warkentin, 2010), while cognitive engagement will be determined via perceptional questionnaires on mental resource utilization (Guinea et al., 2014). Self-reports will assess experience factors.

Furthermore, a multi-method experimental approach will be adopted, employing Neuro Information Systems (NeuroIS) techniques with neurophysiological equipment to capture additional objective measures of users' dynamic states, discerning cognitive engagement, and perceived risks during phishing encounters. Experimental activities will occur at the McMaster Digital Transformation Research Centre (MDTRC), employing eye tracking and electroencephalography. EEG will be utilized in an Event-Related Potential (ERP) scenario, focusing on fixation-related ERPs, allowing for the measurement of brain responses to specific stimuli related to threat identification (Vance et al., 2014). Eye tracking with measurements of eye movements, fixation patterns, and blink rates will quantify cognitive engagement (Anderson et al., 2016; Ranti et al., 2020). By triangulating neurophysiological

measures with self-reports, the study will overcome potential weaknesses and biases associated with behavioural questionnaires and produce a more holistic understanding of subconscious reactions during phishing attempts (Dimoka et al., 2012). The MDTRC provides access to the Mobile User Experience Lab (MUXL), facilitating an inclusive sampling approach by reaching a wider demographic with diverse mobility levels.

A power analysis for this controlled experiment indicates a requirement of 128 participants for a medium effect size (f=0.25) and a power of 0.8. Accounting for potential data loss, we aim to recruit approximately 144 participants (i.e., 72 older and 72 younger adults, 18 per cell). Participants will initially complete consent forms outlining the study's procedure and instructions. They will then fill out surveys to assess individual static factors and demographics. They will be presented with phishing and legitimate emails on a computer interface and instructed to interact with the messages to identify phishing. The emails will include message framing and context variations, containing attachments, multimedia elements, URLs, and visible sender addresses to simulate a real-world scenario. Phishing susceptibility will be assessed with a dichotomous, action-oriented behavioural assessment monitoring users' activities such as opening attachments, interacting with multimedia, replying to emails, and any misidentifications made (Wang, 2016). Neurophysiological data will be collected during phishing exposures. Subsequently, participants will complete additional surveys to assess dynamic factors, including cognitive engagement. A subset of participants will be interviewed at the end of the session to obtain richer insights into user perceptions.

ANTICIPATED CONTRIBUTIONS

Rooted in a multi-method perspective, this research aims to make substantive contributions to the academic and practitioner audiences. Our investigation addresses gaps in information security, aging, and dark IT. Responding to the mandate for a deeper delve into decision-making processes in the IS realm, this study provides crucial insights into an under-researched population and topic, extending the notions of aging-related decision-making changes to the HCI security context and offering insights into these factors that influence phishing susceptibility. The anticipated theoretical contributions will assist academics across domains, including aging, IS, HCI, and psychology, thus paving the way for further research on older adults' technology interactions and vulnerability to online fraud.

Furthermore, this study will aid practitioner audiences, including policymakers, educators, and media, by informing the design of personalized security measures and educational programs tailored to the unique needs of older adults. By enhancing their understanding of security risks and promoting safer online behaviour, especially in high-risk contexts, this research aims to mitigate the financial, social, emotional, and health consequences of phishing, thus promoting optimal aging, social connectedness, and independence. The outcomes will assist in enhancing strategies in place and developing novel interventions that encourage older adults' safe technology use, thus helping to bridge the digital divide. Ultimately, this could improve the life quality of aging populations by enabling them to use technology in various domains with greater assurance.

REFERENCES

1. Abbasi, A., Dobolyi, D., Vance, A. and Zahedi, F.M. (2021). The phishing funnel model: a design artifact to predict user susceptibility to phishing websites. *Information Systems Research*, *32*(2), 410-436. https://doi.org/10.1287/isre.2020.0973
2. Anderson, B., Vance, A., Kirwan, C. B., Eargle, D., and Jenkins, J. L. (2016). How users perceive and respond to security messages: a NeuroIS research agenda and empirical study. *European Journal of Information Systems*, *25*(4), 364-390. https://doi.org/10.1057/ejis.2015.21
3. Ayaburi, E. W., and Andoh-Baidoo, F. K. (2023). How do technology use patterns influence phishing susceptibility? A two-wave study of the role of reformulated locus of control. *European Journal of Information Systems*, 1-21. https://doi.org/10.1080/0960085X.2023.2186275
4. Boroon, L., Abedin, B. and Erfani, E. (2021) The Dark Side of Using Online Social Networks: A Review of Individuals' Negative Experiences. *Journal of Global Information Management (JGIM)*, *29*(6), 1-21. https://doi.org/10.4018/JGIM.20211101.oa34
5. Bruine de Bruin, W., Parker, A. M., and Fischhoff, B. (2012). Explaining adult age differences in decision-making competence. *Journal of Behavioral Decision Making*, *25*(4), 352-360. https://doi.org/10.1002/bdm.712
6. Burton, A., Cooper, C., Dar, A., Mathews, L., and Tripathi, K. (2022). Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: A realist review. *Experimental Gerontology*, *159*, 111678. https://doi.org/10.1016/j.exger.2021.111678
7. Choudrie, J., Banerjee, S., Kotecha, K., Walambe, R., Karende, H., and Ameta, J. (2021). Machine learning techniques and older adults processing of online information and misinformation: A covid 19 study. *Computers in Human Behavior*, *119*, 106716. https://doi.org/10.1016/j.chb.2021.106716
8. Dennis, A. R., and Minas, R. K. (2018). Security on autopilot: Why current security theories hijack our thinking and lead us astray. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *49*(SI), 15-38. https://doi.org/10.1145/3210530.3210533
9. Dimoka, A., Banker, R. D., Benbasat, I., Davis, F. D., Dennis, A. R., and Gefen, D. l. (2012). On the use of neurophysiological tools in IS Research: Developing a

research agenda for neuroIS. *MIS Quarterly, 36*(3), 679–702. https://doi.org/10.2307/41703475
10. Evans, J. St. B. T. (2008). Dual-processing accounts of reasoning, judgment, and social cognition. *Annual Review of Psychology, 59*, 255-278.
11. Gavett, B. E., Zhao, R., John, S. E., Bussell, C. A., Roberts, J. R., and Yue, C. (2017). Phishing suspiciousness in older and younger adults: The role of executive functioning. *PLoS One, 12*(2), e0171620. https://doi.org/ 10.1371/journal.pone.0171620
12. Goel, S., Williams, K., and Dincelli, E. (2017). Got Phished? Internet Security and Human Vulnerability. *Journal of the Association for Information Systems*, *18*(1), 22–44. https://doi. org/10.17705/1jais.00447
13. Guinea, A., Titah, R., and Léger, P. (2014). Explicit and Implicit Antecedents of Users' Behavioral Beliefs in Information Systems: A Neuropsychological Investigation, *Journal of Management Information Systems*, *30*(4), 179-210, https://doi.org/10.2753/MIS0742-1222300407
14. Hassandoust, F., Singh, H., and Williams, J. (2020). The role of contextualization in individuals' vulnerability to phishing attempts. *Australasian Journal of Information Systems*, *24*. https://doi.org/10.3127/ajis.v24i0.2693
15. Hess, T. M. (2006). Adaptive aspects of social cognitive functioning in adulthood: Age-related goal and knowledge influences. *Social Cognition, 24*, 279–309. https://doi.org/10.1521/soco.2006.24.3.279
16. Hess, T. M. (2015). A prospect theory-based evaluation of dual-process influences on aging and decision making: Support for a contextual perspective. In *Aging and decision making: Empirical and Applied Perspectives* (pp. 189-212). Academic Press.
17. Jaeger, L. and Eckhardt, A. (2021) Eyes wide open: The role of situational information security awareness for security-related behaviour. *Information Systems Journal*, *31*(3), 429-472. https://doi.org/10.1111/isj.12317
18. Johnston, A. C., and Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly, 34*(3), 549-566. https://doi.org/10.2307/25750691
19. Kahneman, D., and Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica, 47*(2), 263–291. http://dx.doi.org/10.2307/1914185
20. Levine, T. R. (2014). Truth-default theory (TDT): A theory of human deception and deception detection. *Journal of Language and Social Psychology, 33*(4), 378-392. https://doi.org/10.1177/0261927X14535916
21. Liu, X., Ji, L., and Peng, H. (2021). The impacts of task relevance and cognitive load on adults' decision information search. *Aging, Neuropsychology, and Cognition*, *28*(1), 78-96. https://doi.org/10.1080/13825585.2020.1712320
22. Lu, X., Head, M., Yang, J., and Tariq, A. (2022). An Investigation of Misinformation Susceptibility of Older Adults: A Persuasive Perspective. *SIGHCI 2022 Proceedings. 27.*
23. Moody, G. D., Galletta, D. F., and 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.
24. Morgan, P. L., Williams, E. J., Zook, N. A., and Christopher, G. (2019). Exploring older adult susceptibility to fraudulent computer pop-up interruptions. In *Proceedings of International Conference on Human Factors in Cybersecurity*, 56-68. https://doi.org/10.1007/978-3-319-94782-2_6
25. Ranti, C., Jones, W., Klin, A., and Shultz, S. (2020). Blink rate patterns provide a reliable measure of individual engagement with scene content. *Scientific reports*, *10*(1), 8267.
26. Raven, J., Raven, J. C., and Court, J. H. (2003). Manual for Raven's Progressive Matrices and Vocabulary Scales. Pearson.
27. Sarno, D. M., and Black, J. (2023). Who Gets Caught in the Web of Lies?: Understanding Susceptibility to Phishing Emails, Fake News Headlines, and Scam Text Messages. *Human Factors*, https://doi.org/10.1177/00187208231173263
28. Shang, Y., Wu, Z., Du, X., Jiang, Y., Ma, B., and Chi, M. (2022). The psychology of the internet fraud victimization of older adults: A systematic review. *Frontiers in Psychology*, *13*, 912242. https://doi.org/10.3389/fpsyg.2022.912242
29. Tversky, A., and Kahneman, D. (1974). Judgment under Uncertainty: Heuristics and Biases: Biases in judgments reveal some heuristics of thinking under uncertainty. *Science*, *185*(4157), 1124-1131. https://doi.org/10.1126/science.185.4157.1124
30. Vance, A., Anderson, B. B., Kirwan, C. B., and Eargle, D. (2014). Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG). *Journal of the Association for Information Systems*, *15*(10), 679–722. https://doi.org/10.17705/1jais.00375
31. Vance, A., Eargle, D., Eggett, D., Straub, D., and Ouimet, K. (2022). Do security fear appeals work when they interrupt tasks? A multi-method examination of password strength. *MIS Quarterly*, *46*(3), 1721-1738. https://doi.org/10.25300/MISQ/2022/15511
32. Wagner, N., Hassanein, K., and Head, M. (2010). Computer use by older adults: A multidisciplinary review. *Computers in Human Behavior*, *26*(5), 870–882.https://doi.org/10.1080/0960085X.2019.1708218
33. Wang, J., Li, Y. and Rao, H. R. (2016). Overconfidence in phishing email detection. *Journal of the Association for Information Systems*, *17*(11), 1. https://doi.org/10.17705/1jais.00442
34. Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., and Marett, K. (2014). Influence Techniques in Phishing Attacks: An Examination of Vulnerability and Resistance. *Information Systems Research*, *25*(2), 385–400. https://doi.org/10.1287/isre.2014.0522