International Institute for Applied Knowledge Management

Refereed Paper Proceedings - KM Conference 2024 – Warsaw, Poland

A Publication of the International Institute for Applied Knowledge Management

Refereed Paper Proceedings

KM2024 Conference Sponsoring Schools and Organizations:

SGH Warsaw School of Economics

International Institute for Applied Knowledge Management

KM2024 Conference Partner Organizations:

ISACA®

SAMSUNG

ABR SESTA MARKET RESEARCH & CONSULTING

International Institute for Applied Knowledge Management

Refereed Paper Proceedings - KM Conference 2024 – Warsaw, Poland

A Publication of the International Institute for Applied Knowledge Management

Table of Contents

International Institute for Applied Knowledge Management

Refereed Paper Proceedings - KM Conference 2024 – Warsaw, Poland

A Publication of the International Institute for Applied Knowledge Management

Conference Chairs, Organizers, OJAKM Editorial Board Leadership, and Program Committee

KM2024 Conference Co-Chairs

Celina Sołek-Borowska
Warsaw School of Economics, Poland
csolek@sgh.waw.pl

Patryk Dziurski
Warsaw School of Economics, Poland
pdziur@sgh.waw.pl

KM2024 Conference Organizers and Coordinators

Yair Levy
Nova Southeastern University, FL, USA
levyy@nova.edu

Shonda Brown
IIAKM, USA
registration@iiakm.org

Michelle M. Ramim
Nova Southeastern University, USA
michelle.ramim@gmail.com

Vered Silber-Varod
Tel Aviv University, Israel
veredsv@tauex.tau.ac.il

KM2024 Conference Workshops Co-Chairs

Christiaan Maasdorp
Stellenbosch University, South Africa
chm2@sun.ac.za

Julita Haber
Fordham University, USA
jhaber7@fordham.edu

Online Journal of Applied Knowledge Management (OJAKM) – Editorial Board Leadership

KM2024 Program Committee Co-Chairs

KM2024 Program Committee Members

Ina Blau	The Open University of Israel, Israel
Alan Rafael Boesing	Universidade Federal do Rio Grande do Sul, Brazil
Marko Bohanec	Jožef Stefan Institute, Slovenia
Benny Bornfeld	Ruppin Academic Center, Israel
Steve Bronsburg	Nova Southeastern University, USA
Shonda Brown	IIAKM, USA
Brian Buckles	National Defense University, USA
Kom Campiranon	Thammasat University, Thailand
Melissa Carlton	Lindsey Wilson College, USA
Dimitar Christozov	American University of Bulgaria, Bulgaria
Molly Cooper	Ferris State University, USA
Carla Curado	ISEG - University of Lisbon, Portugal
Gabriel Cornejo	DoD, USA
John Del Vecchio	Nova Southeastern University, USA
Bostjan Delak	Faculty of information studies, Novo Mesto, Slovenia
Horatiu Dragomirescu	Bucharest University of Economic Studies, Romania
Patryk Dziurski	Wroclaw University of Economics, Poland
Darrell Eilts	Loyola University New Orleans, USA
Monika Eisenbardt	University of Economics in Katowice, Poland
Benjamin Fabian	Technical University of Applied Sciences Wildau, Germany
Steven Furnell	University of Nottingham, UK
Ruti Gafni	Tel-Aviv Yaffo Academic College, Israel
Nitza Geri	The Open University of Israel, Israel
Tiago Goncalves	Universidade de Lisboa - ISEG, Portugal
Julita Haber	Fordham University, USA
Wilnelia Hernandez	WH-Consulting, Puerto Rico
Andreas Häberlin	Nova Southeastern University and St. Thomas University, USA
Angel Hueca	Carnegie Mellon University/CERT, USA
Emmanuel Jigo	JiSec, USA
Oliver Jokisch	HSF University of Meissen, Germany
Dan Kohen Vacs	Holon Institute of Technology, Israel
Gila Kurtz	HIT - Holon Institute of Technology, Israel
Yair Levy	Nova Southeastern University, USA
Christiaan Maasdorp	Stellenbosch University, South Africa
Juan M. Madrid	Universidad Icesi, Colombia
Herbert Mattord	Kennesaw State University, USA
Saw Sandi Maung	University of Pannonia, Hungary

John McConnell	Johns Hopkins Health System, USA
Eliel Melon	University of Puerto Rico, Puerto Rico
Stephen Mujeye	Illinois State University, USA
Federico Niccolini	University of Pisa, Italy
Martina Neri	University of Pisa, Italy
Sergio Nunes	ISEG - University of Lisbon, Portugal
Rema Padman	Carnegie Mellon University, USA
Tal Pavel	The Academic College of Tel Aviv–Yaffo, Israel
Ilona Paweloszek	Czestochowa University of Technology, Poland
Michal Pietrzak	Warsaw University of Life Sciences - WULS, Poland
Margarida Piteira	SOCIUS - Research Centre in Economic and Organizational Sociology, Portugal
Przemyslaw Polak	Warsaw School of Economics, Poland
Tommy Pollock	Tidewater Comm. College and National Defense University, USA
Ashraf Qutaishat	University of Minho, Portugal
Daphne Raban	University of Haifa, Israel
Michelle Ramim	Nova Southeastern University, USA
Meir Russ	University of Wisconsin - Green Bay, USA
Vincent Ribiere	Bangkok University, Thailand
Nanette Saes	Stellenbosch University, South Africa
Joanna Santiago	ISEG - University of Lisbon, Portugal
Dara Schniederjans	University of Rhode Island, USA
Tamar Shamir-Inbal	The Open University of Israel, Israel
Sofia Sherman	The Academic College Tel Aviv Yaffo, Israel
Ingo Siegert	Otto von Guericke University, Germany
Vered Silber-Varod	Tel Aviv University, Israel
Anna Soltysik-Piorunkiewicz	University of Economics in Katowice, Poland
Celina Sołek-Borowska	Warsaw School of Economics, Poland
Mathupayas Thongmak	Thammasat Universit, Thailand
Michael Tu	Purdue University Northwest, USA
Rolf von Rössing	ISACA, Switzerland
Simon Vrhovec	University of Maribor, Slovenia
Bruce Watson	Stellenbosch University, South Africa
Tobi West	Coastline College, USA
Nathan White	Central Washington University, USA
Jędrzej Wieczorkowski	Warsaw School of Economics, Poland
Amir Winer	The Open University of Israel, Israel
Ewa Ziemba	University of Economics in Katowice, Poland

Rina Zviel-Girshin	Ruppin Academic Center, Israel

We would like to thank all the Program Committee (PC) members for their outstanding scholarly reviews and dedicated feedback to the authors!

International Institute for Applied Knowledge Management

Refereed Paper Proceedings - KM Conference 2024 – Warsaw, Poland

A Publication of the International Institute for Applied Knowledge Management

Towards assessing the role of persuasion principles and cybersecurity skills training on senior citizens' SMiShing susceptibility

[Research-in-Progress]

Brian Bisceglia, Nova Southeastern University, USA, bb1704@mynsu.nova.edu

Yair Levy, Nova Southeastern University, USA, levyy@nova.edu

Gregory Simco, Nova Southeastern University, USA, greg@nova.edu

Wei Li, Nova Southeastern University, USA, lwei@nova.edu

Carlene Blackwood-Brown, Seneca Polytechnic, Canada, carlene.blackwood-brown@senecapolytechnic.ca

Abstract

In recent years, senior citizens have fallen victim to phishing attacks and collectively lost many millions of dollars each year. One attack vector for committing phishing is SMiShing, where the attacker sends a Short Message Service (SMS) communication that often contains operationalized principles of persuasion to execute an attack. Prior research has shown persuasion principles can improve phishing attacks' success. However, it appears that limited research has been done regarding senior citizens' susceptibility to SMiShing and the use of persuasion principles. The main goal of this work-in-progress study is to empirically evaluate the influence of the five principles of persuasion on senior citizens' susceptibility to SMiShing attacks using simulated SMS messages that will be validated initially by Subject Matter Experts. Also, it will seek to empirically evaluate whether senior citizens' susceptibility to SMiShing is reduced after attending a novel hands-on Security, Education, Training, and Awareness (SETA) session. Data from the simulated SMiShing attack results and demographic information will then be compared. In conclusion, the novel SETA program may help reduce senior citizens' susceptibility to SMiShing and help secure senior citizens' accumulated wealth.

Keywords: Persuasion, SETA, seniors, decision-making, phishing, SMiShing.

Introduction

Social engineers manipulate people by exploiting their vulnerabilities and influencing them to take actions that may leave them vulnerable to the social engineer's malicious actions (Hadnagy, 2011). Social engineers have used different mediums to deliver their attacks, such as Short Message Service (SMS) messages, voice, and email (Alabdan, 2020). Phishing attacks are used to fraudulently acquire a person's credentials, steal personal information, deliver malware, and direct unsuspecting victims to phishing websites (Jain & Gupta, 2021; Stone-Gross et al., 2009). In 2022,

persons aged 60 years or more lost more than $14 million to cyber-attacks. Phishing attacks have been performed through different mediums, including SMS messages, which were originally limited to 160 characters but can be extended to much more (Dryburgh & Hewett, 2004). Phishing attacks performed via SMS messages are called SMiShing attacks (Alabdan, 2020). The ability to send and receive SMS messages is available to 97% of Americans and 92% of senior citizens aged 65 years or more (Dryburgh & Hewett, 2004; Pew Research Center, 2021).

The persuasive effect of phishing attacks has been increased with the inclusion of the different principles of persuasion identified by Cialdini (2007), Ferreira et al. (2015), Gragg (2003), as well as Stajano and Wilson (2011). Persons have also been shown to be more susceptible to phishing attacks when they use heuristics or System 1 to make decisions regarding phishing attacks (Butavicius et al., 2015; Kahneman, 2011; Parsons et al., 2019). Kahneman (2011) explained that System 1 is a system in a person's mind that often makes decisions with limited conscious effort and makes them quickly. Prior research has shown that the success rate of phishing attacks on mobile device or cellphone users, such as SMiShing attacks, has been enhanced by the exploitation of various mobile device or cellphone affordances (Felt & Wagner, 2011; Goel & Jain, 2018; Mishra & Soni, 2019). Security, Education, Training, and Awareness (SETA) programs have been shown effective at reducing people's susceptibility to phishing and SMiShing attacks (Alwanain, 2020; Blackwood-Brown et al., 2021; Kumaraguru et al., 2009). Specifically, prior research has shown that senior citizens who attended a SETA program improved their cybersecurity skills and fell victim less often to phishing attacks (Alwanain, 2020; Blackwood-Brown et al., 2021; Kumaraguru et al., 2009). The main Research Question (RQ) that this study will address is: Does attending a training program that includes principles of persuasion affect senior citizens' susceptibility to SMiShing? This study has one RQ and eight hypotheses. The RQ is: What are the specific Subject Matter Experts (SMEs) identified set of SMiShing messages and legitimate SMS messages that can be used to judge participants' susceptibility to SMiShing? The eight hypotheses will be the direct effect of each principle of persuasion on senior citizens' susceptibility to SMiShing, their intercorrelations, and comparisons based on demographic indicators.

Literature Review

Social Engineering

Previous studies have indicated that incorporating the principles of persuasion can enhance the efficacy of a social engineering attack (Abass, 2018; Algarni et al., 2017; Bullée et al., 2018; Cheung et al., 2015; Jain et al., 2016; Wang et al., 2021). For example, Algarni et al. (2017) investigated the *authority* and *reciprocation* principles on persons' susceptibility to social engineering attacks and mediated by the perceived worthiness of the social engineering attacker. They found that the *authority* principle of persuasion was found to be more influential during these attacks. Algarni et al. (2017) and Cheung et al. (2015) both showed that *liking* and *social proof* principles have increased the likelihood of disclosing personal information to attackers while they use social networking platforms. Moreover, Workman (2008) emphasized that a social engineer

may attempt to gain trust by getting the victim to like them by establishing a friendly rapport and appearing similar to the victim. Prior research has further shown that the effectiveness of social engineering attacks depends on how the would-be victim processes the attacker's information (Antonucci et al., 2022; Gragg, 2003; Jain et al., 2016). For example, Jain et al. (2016) highlighted that social engineering attacks that invoke the use of System 1 can help the attacker "bypass logical argument and counterargument" or the use of System 2 (p. 95). Antonucci et al. (2022) discovered that delaying access to a phishing email's link by three seconds and displaying a red warning message can engage System 2 and decrease the chances of the link being clicked or a malicious attachment being downloaded. In addition, the success rates of social engineering attacks have been decreased due to SETA programs (Gragg, 2003; Jain et al., 2016; Mensch & Wilkie, 2011; Salahdine & Kaabouch, 2019).

Cybersecurity Threats

Prior research has shown that the quality of senior citizens' decisions may diminish as they age (Gregory & Samanez-Larkin, 2013). For example, Gregory and Samanez-Larkin (2013) highlight that older persons make more mistakes when making financial decisions. In addition, research has further shown that older people's decision-making competence declines with age and when retention demands increase (Bruine de Bruin et al., 2012; Del Missier et al., 2010, 2012; Freitas et al., 2007; Rosi et al., 2019). Additionally, Rosi et al. (2019) found that the application of decision rules deteriorated with age, resulting in poorer performance among older adults. However, some studies have shown that applying decision rules and the speed in making decisions may not decline with age (Bruine de Bruin et al., 2012; Dror et al., 1998; Lizarraga et al., 2007). In addition, prior research has shown that older adults have a diminished sensitivity to deception and lying, along with an increased tendency to trust others, which has been shown to increase their vulnerability to fraud (Castle et al., 2012; Ruffman et al., 2012).

Principles of Persuasion

Cialdini (2007) identified six principles of persuasion, which are commonly known as "weapons of influence." These principles are *consistency*, *reciprocation*, *social proof*, *authority*, *liking*, and *scarcity*. *Reciprocation* is the feeling of obligation or indebtedness that one person may feel towards another. *Consistency* is the desire to be and appear consistent. *Social proof* or social validation refers to people looking to others to help them make decisions. The *authority* principle asserts influence or persuasion when the requestor is perceived as an authority figure. *Liking* is when a person is more likely to agree with someone they like. Finally, the *scarcity* principle relies on the time or supply of something being perceived as limited quantities. Each of the principles of persuasion can cause a System 1 response to a stimulus or at least reduce the involvement of System 2 (Cialdini, 2007). According to Gragg (2003), social engineers rely on several psychological principles during social engineering attacks. Moreover, Stajano and Wilson (2011) discovered several human weaknesses that scammers take advantage of during real-world scams. Ferreira et al. (2015) synthesized the doctrines of the weapons of influence, psychological principles, and real-world scam weaknesses identified by Cialdini (2007), Gragg (2003), as well

as Stajano and Wilson (2011), respectively. Ferreira et al. (2015) synthesized a list of principles of persuasion including *authority*; *social proof*; *liking, similarity, and deception*; *commitment, reciprocation, and consistency*; and *distraction*.

Security, Education, Training, and Awareness (SETA) Programs

Prior research has shown that SETA programs have increased people's cybersecurity skill levels and have reduced susceptibility to cyber-attacks (e.g., phishing) (Alwanain, 2020; Blackwood-Brown et al., 2021; Burns et al., 2019; Kumaraguru et al., 2008, 2009; Zwilling et al., 2022). Cybersecurity skills have been defined as "a combination of knowledge, experience, and ability that enables end-users to perform well" (Carlton & Levy, 2015, p. 2). Carlton and Levy (2017) found that individuals with cybersecurity skills play a crucial role in minimizing the losses caused by cyber-attacks. Zwilling et al. (2022) showed that Internet users with a greater security awareness incorporated more cyber-secure behaviors. Burns et al. (2019) showed that the benefits of SETA training in a corporate environment improved the phishing awareness of those who attended the SETA program and even those who did not participate in the training program. Alwanain (2020) and Kumaraguru et al. (2008) both found that attending a SETA program reduced the number of times their participants clicked on malicious links included in phishing and SMiShing attacks. While prior research has shown that SETA programs reduce people's susceptibility to cyber-attacks, their effectiveness can decrease over time (Bullée et al., 2016; Kumaraguru et al., 2008; Sikolia et al., 2023).

Mobile Device Affordances

Research has identified several cellphone affordances contributing to a user's susceptibility to phishing (Felt & Wagner, 2011; Goel & Jain, 2018; Mishra & Soni, 2019). One of the affordances identified by the research is the relatively small size of a cellphone's screen (Felt & Wagner, 2011; Goel & Jain, 2018; Kim & Sundar, 2014; Shahriar et al., 2015; Vishwanath, 2016; Wu et al., 2016). Felt and Wagner (2011) and Goel and Jain (2018) found that small cellphone screens can hide malicious Universal Resource Locators (URLs). Another consequence of a cellphone's small screen is the limited space for its keyboard, which can make it difficult to type and can lead to typos (Wu et al., 2016). This difficulty in typing may encourage the user to rely on links in SMS messages, which can expose them to malicious content, such as SMiShing messages (Wu et al., 2016). Moreover, cellphones contain large amounts of personal data that may be used to victimize the owner or increase susceptibility to phishing attacks (Burns et al., 2019; Goel & Jain, 2018). Hur and Shamsi (2017) showed that cellphones running the Android operating system were susceptible to attacks that could compromise the privacy and security of the user (due to its open-source nature). However, people still fall victim to SMiShing on iOS devices (Mylonas et al., 2011). In addition, prior research has shown that attackers can trick the cellphone user into believing they are on a legitimate website but are actually on a malicious website and can be tricked into entering login credentials due to the lack of details within the mobile login interface (Goel & Jain, 2018; Niu et al., 2008; Shahriar et al., 2015).

Kahneman's System 1 and System 2

Kahneman (2011) adopted the monikers System 1 and System 2 to represent the intuitive and reasoning paths of information processing, respectively. System 1 is vulnerable to persuasion primarily due to its reliance on heuristics and subsequent biased decisions derived from using heuristics (Kahneman, 2011; Tversky & Kahneman, 1974). Nonetheless, despite System 1 being vulnerable to persuasion, it can develop a resistance to persuasion via training or developing skills and proficiency from System 2 (Kahneman, 2011; Kahneman & Frederick, 2013). System 2 may also be vulnerable to persuasion due to confirmation bias or the need for consistency (Ajzen, 1996; Kassin et al., 2013). Tversky and Kahneman (1974) described three heuristics that are used to render intuitive judgment under uncertainty: (1) representativeness, (2) availability, as well as (3) anchoring and adjustment. Kahneman (2011) defined a heuristic as "a simple procedure that helps adequate, though often imperfect, answers to difficult questions" (p. 98). Heuristics can be used by System 1 to quickly assess often imperfect information where the assessment of this information occurs regardless of motives or incentives (Gilovich & Griffin, 2013; Kahneman & Frederick, 2013; Tversky & Kahneman, 1974). The affect heuristic is another mental shortcut based on feelings of goodness or badness towards an object or stimulus. It often involves automated choices based on liking or fondness (Slovic et al., 2013).

Proposed Methodology

Overview of Research Design

This study will use a quantitative research method that will utilize a true experimental design – a pretest-posttest Control group design – to determine the effectiveness of a treatment (Creswell, 2014; Sekaran & Bougie, 2016). This study will include three phases to evaluate this study's main goal. During phase one, an expert panel will be used to produce a validated set of SMiShing messages and a validated set of legitimate SMS messages. When experts' consensus is achieved on the content of the sets using the Delphi methodology, the results will address this study's one research question. During phase two, a pilot study will be utilized to help ensure the different strategies (i.e., pretest, posttest, and training) are understandable and achievable for the senior citizen participants (Kraemer & Blasey, 2016). Phase three will be the main study, where pretest data collection, training, posttest data collection, and pre-analysis data screening will occur. Also, during this phase, the final data analysis will be completed, thereby addressing all of this study's hypotheses. During phases two and three, the training content will be delivered via the Basic Skills Training (BST) methodology, which consists of four phases (i.e., instruction, modeling, rehearsal, and feedback). The training will be led by an instructor, and the session will last no longer than 30 minutes. This study’s participants will be drawn from South Florida (i.e., City of Fort Lauderdale Community Centers). To ensure ethical standards are met, we obtained an Institutional Review Board (IRB) review for this study (Kite & Whitley, 2018).

Newly SMiShing Hands-On SETA Program

This study will use the Behavioral Skills Training (BST) methodology to bring SETA training to the participants. The BST methodology includes four phases: (1) instruction, (2) modeling, (3) rehearsal, and (4) feedback. O'Connell (2016) found that the components of BST, especially modeling, worked best for training Facebook skills to senior citizens versus instruction alone. An instructor will be present during training and run in small groups of less than 20. During the first phase of the BST methodology, instruction will cover social engineering, phishing, SMiShing, and descriptions of the principles of persuasion. In the second phase, participants will be presented with simulated SMiShing messages that illustrate the principles of persuasion and help them recognize as well as respond to the persuasive tactics employed in the SMiShing messages. In the third and fourth phases, participants will be given two SMiShing examples for each operationalized principle of persuasion and asked to evaluate the likelihood (via the 7-point Likert Scale) that the example is a SMiShing message and identify which persuasion principle was used. After answering, the participant will be given feedback on their answers.

Instrument Development

Instrument development will be conducted in three phases. During phase 1, the goal will be to identify and validate a set of messages that SMEs identify as SMiShing and legitimate SMS messages. The Delphi methodology will be employed to select validated SMiShing and legitimate SMS messages for assessing senior citizens' susceptibility to SMiShing attacks. Delphi methodology is a method for achieving a reliable consensus among experts (Dalkey & Helmer, 1963). Arithmetic means of the quantitative assessments by the SMEs will be used to determine when there is an acceptable consensus amongst the experts (Gafni & Levy, 2023). Phase 2 includes a pilot study to help ensure the validity and reliability of the instrument's set of measures identified by the SMEs (Creswell, 2014; Straub, 1989). Creswell (2014) explained that a pilot study can help ensure an instrument's content validity and possibly improve its questions. Straub (1989) showed that an instrument's pretest can help establish its measures' reliability, construct validity, and content validity. Phase 3 will be the main data collection phase of this study. The data collected during this phase of this study will be used to determine if the threats to internal and external validity have been addressed. For example, this study will implement several mitigations for reducing the possible negative effects on internal and external validity, such as keeping the participants' ages as close as possible and ensuring a minimum number of participants.

Conclusions and Discussions

This study aims to reduce senior citizens' susceptibility to SMiShing attacks and help prevent the financial losses associated with falling victim to these attacks. This study will create a novel SETA program that intends to improve senior citizens' knowledge of SMiShing messages and the principles of persuasion operationalized in these messages, as well as investigate whether the knowledge and identification of these principles improve System 1's decisions about their response to SMiShing messages. All of this while potentially being distracted and using a cellphone that has

affordances that may work against making a correct decision. By providing senior citizens with the knowledge, awareness, and skills necessary to identify and potentially avoid SMiShing messages, this study could positively impact the lives of many senior citizens.

Future Research

Future research could investigate how the different principles of persuasion and this study's novel training program impact other age groups' susceptibility to SMiShing. In addition, future research could investigate whether SETA programs incorporating the principle of persuasion improve System 1's ability to make correct decisions while distracted and using a cellphone. Finally, it could be beneficial to investigate the effectiveness of messages operationalizing the principles of persuasion used in other phishing attack vectors or sent on the social media platform X (formally Twitter). The X platform enforces a 280-character limit per message (i.e., via a free account), which falls between an SMS message's original and the extended character limit (Dryburgh & Hewett, 2004; Twitter, 2024).

References

Abass, I. A. M. (2018). Social engineering threat and defense: A literature survey. *Journal of Information Security*, *09*(04), 257–264. https://doi.org/10.4236/jis.2018.94018

Ajzen, I. (1996). The social psychology of decision making. In E. T. Higgins & A. W. Kruglanski (Eds.), *Social psychology: Handbook of basic principles* (pp. 1–948). The Guilford Press.

Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. *Future Internet*, *12*(10), 1–39. https://doi.org/10.3390/fi12100168

Algarni, A., Xu, Y., & Chan, T. (2017). An empirical study on the susceptibility to social engineering in social networking sites: The case of Facebook. *European Journal of Information Systems*, *26*(6), 661–687. https://doi.org/10.1057/s41303-017-0057-y

Alwanain, M. I. (2020). Phishing awareness and elderly users in social media. *International Journal of Computer Science and Network Security*, *20*(9), 114–119. https://doi.org/10.22937/IJCSNS.2020.20.09.14

Antonucci, A. E., Levy, Y., Dringus, L. P., & Snyder, M. (2022). Experimental study to assess the impact of timers on user susceptibility to phishing attacks. *Research and Practice Journal of Cybersecurity Education, Research and Practice*, *2021*(2), 1–27. https://digitalcommons.kennesaw.edu/jcerp/vol2021/iss2/6/

Blackwood-Brown, C., Levy, Y., & D'Arcy, J. (2021). Cybersecurity awareness and skills of senior citizens: A motivation perspective. *Journal of Computer Information Systems*, *61*(3), 195–206. https://doi.org/10.1080/08874417.2019.1579076

Bruine de Bruin, W., Parker, A. M., & 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

Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. (2018). On the anatomy of social engineering attacks—A literature-based dissection of successful attacks. *Journal of Investigative Psychology and Offender Profiling*, *15*(1), 20–45. https://doi.org/10.1002/jip.1482

Bullée, J. W., Montoya, L., Junger, M., & Hartel, P. H. (2016). Telephone-based social engineering attacks: An experiment testing the success and time decay of an intervention. *Proceedings of the 2016 Singapore Cyber-Security Conference*, 107–114. https://doi.org/10.3233/978-1-61499-617-0-107

Burns, A. J., Johnson, M. E., & Caputo, D. D. (2019). Spear phishing in a barrel: Insights from a targeted phishing campaign. *Journal of Organizational Computing and Electronic Commerce*, *29*(1), 24–39. https://doi.org/10.1080/10919392.2019.1552745

Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2015). Breaching the human firewall: Social engineering in phishing and spear-phishing emails. *Proceedings of the 26th Australasian Conference on Information Systems*, 1–10.

Carlton, M., & Levy, Y. (2015). Expert assessment of the top platform independent cybersecurity skills for non-IT professionals. *Proceedings of the 2015 IEEE SoutheastCon*, 21–26. https://doi.org/10.1109/SECON.2015.7132932

Carlton, M., & Levy, Y. (2017). Cybersecurity skills: Foundational theory and the cornerstone of advanced persistent threats (APTs) mitigation. *Online Journal of Applied Knowledge Management*, *5*(2), 16–28. https://doi.org/10.36965/ojakm.2017.5(2)16-28

Castle, E., Eisenberger, N. I., Seeman, T. E., Moons, W. G., Boggero, I. A., Grinblatt, M. S., & Taylor, S. E. (2012). Neural and behavioral bases of age differences in perceptions of trust. *Proceedings of the 2012 National Academy of Sciences of the United States of America*, *109*(51), 20848–20852. https://doi.org/10.1073/pnas.1218518109

Cheung, C., Lee, Z. W. Y., & Chan, T. K. H. (2015). Self-disclosure in social networking sites the role of perceived cost, perceived benefits and social influence. *Internet Research*, *25*(2), 279–299. https://doi.org/10.1108/IntR-09-2013-0192

Cialdini, R. B. (2007). *Influence: The psychology of persuasion*. Harper Collins Publishers.

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). SAGE Publications, Inc.

Dalkey, N., & Helmer, O. (1963). An experimental application of the Delphi method to the use of experts. *Management Science*, *9*(3), 458–467. https://doi.org/10.1287/mnsc.9.3.458

Del Missier, F., Mäntylä, T., & de Bruin, W. B. (2010). Executive functions in decision making: An individual differences approach. *Thinking and Reasoning*, *16*(2), 69–97. https://doi.org/10.1080/13546781003630117

Del Missier, F., Mäntylä, T., & de Bruin, W. B. (2012). Decision-making competence, executive functioning, and general cognitive abilities. *Journal of Behavioral Decision Making*, *25*(4), 331–351. https://doi.org/10.1002/bdm.731

Dror, I., Katona, M., & Mungur, K. (1998). Age differences in decision making: To take a risk or not? *Gerontology*, *44*, 67–71.

Dryburgh, L., & Hewett, J. (2004). *Signaling system no. 7 (SS7/C7): Protocol, architecture, and services*. Cisco Press.

Felt, A. P., & Wagner, D. (2011). *Phishing on mobile devices*.

Ferreira, A., Coventry, L., & Lenzini, G. (2015). Principles of persuasion in social engineering and their use in phishing. *Proceedings of the International Conference on Human Aspects of Information Security*, *9190*, 36–47. https://doi.org/10.1007/978-3-319-20376-8_4

Freitas, M. I. d'Ávila, Ribeiro, A. F., Radanovic, M., & Mansur, L. L. (2007). Working memory: Differences between young adults and the aged in listening tasks. *Dementia & Neuropsychologia*, *1*(2), 147–153. https://doi.org/10.1590/s1980-57642008dn10200006

Gafni, R., & Levy, Y. (2023). Experts' feedback on the cybersecurity footprint elements: In pursuit of a quantifiable measure of SMBs' cybersecurity posture. *Information and Computer Security*, 1–23. https://doi.org/10.1108/ICS-05-2023-0083

Gilovich, T., & Griffin, D. (2013). Introduction - heuristics and biases: then and now. In T. Gilovich, D. W. Griffin, & D. Kahneman (Eds.), *Heuristics and Biases* (14th ed., pp. 1–857). Cambridge Press.

Goel, D., & Jain, A. (2018). Mobile phishing attacks and defense mechanisms: State of art and open research challenges. *Computers and Security*, *73*, 519–544. https://doi.org/10.1016/j.cose.2017.12.006

Gragg, D. (2003). *A multi-level defense against social engineering*. SANS Institute. https://www.sans.org/reading-room/whitepapers/engineering/multi-level-defense-social-engineering-920

Gregory, R., & Samanez-Larkin, G. (2013). Financial decision making and the aging brain. *Nature Neuroscience*, *16*(5), 648–653. https://doi.org/10.1038/nn.3364

Hadnagy, C. (2011). *Social engineering: The art of human hacking*. Wiley Publishing Inc.

Hur, J., & Shamsi, J. (2017). A survey on security issues, vulnerabilities, and attacks in Android based smartphones. *Proceedings of the 2017 International Conference on Information and Communications Technologies*, 40–46.

Jain, A. K., & Gupta, B. B. (2021). A survey of phishing attack techniques, defence mechanisms and open research challenges. *Enterprise Information Systems*, 1–39. https://doi.org/10.1080/17517575.2021.1896786

Jain, A., Tailang, H., Goswami, H., Dutta, S., Sankhla, M. S., & Kumar, R. (2016). Social engineering: Hacking a human being through technology. *IOSR Journal of Computer Engineering*, *18*(5), 94–100. https://doi.org/10.9790/0661-18050594100

Kahneman, D. (2011). *Thinking fast and slow*. Farrar, Straus, and Giroux.

Kahneman, D., & Frederick, S. (2013). Representativeness revisited: Attribute substitution in intuitive judgment. In T. Gilovich, D. W. Griffin, & D. Kahneman (Eds.), *Heuristics and Biases: The psychology of intuitive judgment* (14th ed., pp. 1–857). Cambridge Press.

Kassin, S. M., Dror, I. E., & Kukucka, J. (2013). The forensic confirmation bias: Problems, perspectives, and proposed solutions. *Journal of Applied Research in Memory and Cognition*, *2*(1), 42–52. https://doi.org/10.1016/j.jarmac.2013.01.001

Kim, K. J., & Sundar, S. S. (2014). Does screen size matter for smartphones? Utilitarian and hedonic effects of screen size on smartphone adoption. *Cyberpsychology, Behavior, and Social Networking*, *17*(7), 466–473. https://doi.org/10.1089/cyber.2013.0492

Kite, M., & Whitley, B. (2018). *Principles of research in behavioral science*. Routledge.

Kraemer, H., & Blasey, C. (2016). *How many subjects (2nd ed.)*. Sage.

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). School of phish: A real-world evaluation of anti-phishing training. *Proceedings of the 5th Symposium of Usable Privacy and Security*, 1–12. https://www.cmu.edu/iso

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2008). Lessons from real world evaluation of anti-phishing training. *Proceedings of the 5th Symposium on Usable Privacy and Security*, 1–12.

Lizarraga, M., Baquedano, M., & Cardelle-Elawar, M. (2007). Factors that affect decision making: gender and age differences. *International Journal of Psychology and Psychological Therapy*, *7*(3), 381–391. https://www.redalyc.org/articulo.oa?id=56070306

Mensch, S., & Wilkie, L. (2011). Information security activities of college students: An exploratory study. *Academy of Information and Management Sciences Journal*, *14*(2), 91–116.

Mishra, S., & Soni, D. (2019). SMS phishing and mitigation approaches. *Proceedings of the 12th International Conference on Contemporary Computing*, 1–5.

Mylonas, A., Dritsas, S., Tsoumas, B., & Gritzalis, D. (2011). Smartphone security evaluation: The malware attack case. *Proceedings of the 2011 International Conference on Security and Cryptography*, 25–36.

Niu, Y., Hsu, F., & Chen, H. (2008). iPhish: Phishing vulnerabilities on consumer electronics. *Proceedings of the 1st Conference on Usability*, 1–8. http://us.lge.com/products/model/detail/

Parsons, K., Butavicius, M., Delfabbro, P., & Lillie, M. (2019). Predicting susceptibility to social influence in phishing emails. *International Journal of Human Computer Studies*, *128*, 17–26. https://doi.org/10.1016/j.ijhcs.2019.02.007

Pew Research Center. (2021). *Mobile fact sheet*. https://www.pewresearch.org/internet/fact-sheet/mobile

Rosi, A., Bruine de Bruin, W., Del Missier, F., Cavallini, E., & Russo, R. (2019). Decision-making competence in younger and older adults: Which cognitive abilities contribute to the application of decision rules? *Aging, Neuropsychology, and Cognition*, *26*(2), 174–189. https://doi.org/10.1080/13825585.2017.1418283

Ruffman, T., Murray, J., Halberstadt, J., & Vater, T. (2012). Age-related differences in deception. *Psychology and Aging*, *27*(3), 543–549. https://doi.org/10.1037/a0023380

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, *11*(4), 1–17. https://doi.org/10.3390/FI11040089

Sekaran, U., & Bougie, R. (2016). *Research methods for business* (7th ed.). Wiley.

Shahriar, H., Klintic, T., & Clincy, V. (2015). Mobile phishing attacks and mitigation techniques. *Journal of Information Security*, *6*(3), 206–212. https://doi.org/10.4236/jis.2015.63021

Sikolia, D., Biros, D., & Zhang, T. (2023). How effective are SETA programs anyway: Learning and forgetting in security awareness training. *Research and Practice Journal of Cybersecurity Education, Research and Practice*, *2023*(1), 1–9.

Slovic, P., Finucane, M., Peters, E., & MacGregor, D. G. (2013). The affect heuristic. In T. Gilovich, D. W. Griffin, & D. Kahneman (Eds.), *Heuristics and biases: The psychology of intuitive judgment* (14th ed., pp. 1–857). Cambridge Press.

Stajano, F., & Wilson, P. (2011). Understanding scam victims: Seven principles for systems security. *Communications of the ACM*, *54*(3), 70–75. https://doi.org/10.1145/1897852.1897872

Stone-Gross, B., Cova, M., Cavallaro, L., Gilbert, B., Szydlowski, M., Kemmerer, R., Kruegel, C., & Vigna, G. (2009). Your botnet is my botnet: Analysis of a botnet takeover. *Proceedings of the 2009 ACM Conference on Computer and Communications Security*, 635–647. https://doi.org/10.1145/1653662.1653738

Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly: Management Information Systems*, *13*(2), 147–165. https://doi.org/10.2307/248922

Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. *Science*, *185*(4157), 1124–1131. https://doi.org/http://www.jstor.org/stable/1738360

Twitter. (2024, January 12). *Counting characters*. https://developer.twitter.com/en/docs/counting-characters

Vishwanath, A. (2016). Mobile device affordance: Explicating how smartphones influence the outcome of phishing attacks. *Computers in Human Behavior*, *63*, 198–207. https://doi.org/10.1016/j.chb.2016.05.035

Wang, Z., Zhu, H., & Sun, L. (2021). Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. *IEEE Access*, *9*, 11895–11910. https://doi.org/10.1109/ACCESS.2021.3051633

Workman, M. (2008). A test of interventions for security threats from social engineering. *Information Management and Computer Security*, *16*(5), 463–483. https://doi.org/10.1108/09685220810920549

Wu, L., Du, X., & Wu, J. (2016). Effective defense schemes for phishing attacks on mobile computing platforms. *IEEE Transactions on Vehicular Technology*, *65*(8), 6678–6691. https://doi.org/10.1109/TVT.2015.2472993

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269

Authors Biographies

Brian Bisceglia is a Ph.D. candidate in Cybersecurity Management at Nova Southeastern University (NSU)'s College of Computing and Engineering. He earned a Bachelor's degree in Electronic Engineering Technology and a Master's degree in Applied Computer Science, both from Wentworth Institute of Technology. Brian has over 25 years of experience in digital forensics and computing fields. He works as a full-time Detective Sergeant for a large city and is part of a federal task force aimed at combating human trafficking and child exploitation. He has testified in state and federal courts and participated in various state-level cyber working groups. Furthermore, he is credited as an inventor or co-inventor on three U.S. patents related to electronic circuit designs and electromagnetics.

Yair Levy, Ph.D. is a Professor of Information Systems and Cybersecurity at the College of Computing and Engineering at Nova Southeastern University, the Director of the Center for Information Protection, Education, and Research (CIPhER) (http://infosec.nova.edu/), and chair of the Cybersecurity Curriculum Committee at the college. He conducts innovative research from the 'human factor' in cybersecurity, including social engineering and supply chain cybersecurity. Levy authored numerous peer-reviewed journal articles, conference proceedings, book chapters, and other publications. His scholarly research has been cited over 8,000 times. Dr. Levy was trained in 2015 by the Federal Bureau of Investigation (FBI) on various topics and actively serves as a Board Member of the FBI-affiliated InfraGard South Florida chapter and serves as the Education Sector Chief. Additionally, he has been serving as the National Co-Lead for the National Security Agency (NSA)'s Community of Practice in Cyber Defense (CoP-CD) (https://www.caecommunity.org/community-of-practice/cyber-defense). He is an active member of the Florida Department of Law Enforcement South Florida Cybercrime Working Group (SFCWG) as part of the Florida Fusion Centers. He consults local, state, and federal government agencies on cybersecurity topics. He is also a frequently invited keynote speaker at national and international meetings, as well as regular media interviews as a Subject Matter Expert (SME) on cybersecurity topics. Read more about Dr. Levy at: https://sites.nova.edu/levyy/

Gregory E. Simco, Ph.D. is a Professor and Chair in the College of Computing and Engineering at Nova Southeastern University (NSU). He received his Bachelor of Science in Engineering (Computer and Information Science) from the University of Florida, and a Master of Science and Ph.D. in Computer Science from NSU. Prior to joining NSU, Dr. Simco was the Technical and Team leader for OS/2 and Workplace OS kernel and file systems for IBM and Senior Research and Development Engineer and Director of Systems Software for the Panda Project. Dr. Simco's research interests are in operating and distributed systems in the areas of security, dependability, and performance. Dr. Simco is the author of various conference presentations and journal articles primarily focusing on the architecture, design, performance, and evaluation of survivable/dependable distributed systems. He is involved in NSU's Florida Lambda Rail project and the Secure and Robust Distributed Systems initiative within the National Center of Academic Excellence in Cybersecurity Cyber Defense and Cyber Research at NSU. Dr. Simco teaches undergraduate and graduate courses in operating and distributed systems and is a Project/Co-Project Director for US Department of Education grants and Principle/Co-Principle Investigator of NSF grants totaling over 25 million dollars. The grants focus on computer science and cybersecurity research and student success efforts to broaden access to high-need STEM degrees and graduate/professional pathway preparedness.

Wei Li, Ph.D. is a professor in the College of Engineering and Computing at Nova Southeastern University. His research interests include network security, artificial intelligence, security engineering, and machine learning. He received his master's and Ph.D. degrees in Computer Science and Engineering from Mississippi State University. He was an active researcher and frequent reviewer in the field of computer networking and cybersecurity, with about 50 publications in refereed journals and conferences. He is a senior member of IEEE, a member of ACM, and a member of UPE.

Carlene Blackwood-Brown, Ph.D. is a faculty member in the School of IT Administration & Security at Seneca Polytechnic in Canada as well as the program coordinator for a two-year graduate certificate program and the faculty internationalization lead in the school. She is also the director and cybersecurity consultant at Technologically Speaking Inc., which focuses on creating and delivering cybersecurity-related consulting, training, and other technical solutions to organizations and individuals, delivering the requisite knowledge and skills to protect the integrity, security, and confidentiality of their digital assets (https://technologicallyspeaking.ca). She received her undergraduate and MS degrees in management information systems from the University of the West Indies, Jamaica, and her Ph.D. in information systems with a concentration in cybersecurity from Nova Southeastern University. Dr. Blackwood-Brown also holds a certificate from Harvard University in cybersecurity.