Characteristics that Predict Phishing Susceptibility: A Review

McKenna K. Tornblad[1], Keith S. Jones[1], Akbar Siami Namin[2], and Jinwoo Choi[1]
[1]Dept. of Psychological Sciences, [2]Dept. of Computer Science, Texas Tech University, Lubbock, TX

Phishing attack countermeasures have previously relied on technical solutions or user training. As phishing attacks continue to impact users resulting in adverse consequences, mitigation efforts may be strengthened through an understanding of how user characteristics predict phishing susceptibility. Several studies have identified factors of interest that may contribute to susceptibility. Others have begun to build predictive models to better understand the relationships among factors in addition to their prediction power, although these studies have only used a handful of predictors. As a step toward creating a holistic model to predict phishing susceptibility, it was first necessary to catalog all known predictors that have been identified in the literature. We identified 32 predictors related to personality traits, demographics, educational background, cybersecurity experience and beliefs, platform experience, email behaviors, and work commitment style.

INTRODUCTION

Several countermeasures have been implemented to mitigate phishing attacks, i.e., attempts to gain personal information through malicious, mass-distributed electronic messages (Butavicius et al., 2015). These include 1) filtering phishing messages and blocking users from accessing fraudulent sites; 2) creating interfaces that warn users; and 3) training users how to identify and correctly behave in response to phishing attempts (Hong, 2012). Despite these efforts, phishing attacks continue to reach users who fall for them.

Therefore, alternative attempts to counteract phishing attacks have been proposed. Heartfield et al. (2016) suggest that understanding user characteristics that predict phishing susceptibility could be used to enhance phishing mitigation techniques. Systems that detect a user's susceptibility profile could deny access rights to protect information from a potentially susceptible user, and training programs could be customized based on a user's profile. Further, susceptibility profiles could be used to predict the effectiveness of users as phishing attack sensors and provide a gauge as to how accurate a phishing report may be based on users' characteristics.

Previous Work Toward Predicting Susceptibility

There is an extensive literature that identifies characteristics related to phishing susceptibility, including personality traits, online training and behavior, and demographics. That work provides an essential foundation by establishing characteristics of interest but does not currently allow for user susceptibility prediction with a high degree of certainty or determine whether it is possible to do so. No lone predictor highly correlates with susceptibility; therefore, it is necessary to investigate a combination of several factors to predict susceptibility.

To-date, only a handful of studies have predicted phishing susceptibility using multiple predictors, and those that did examined only a small number of select predictors. For example, Heartfield et al. (2016) investigated six predictors to create a predictive model of susceptibility. Studies such as this are useful, but do not provide a complete model predicting phishing susceptibility.

Current Work

Our long-term goal is to develop a comprehensive predictive model of phishing susceptibility, which can serve as the basis for user susceptibility profiles. As a first step toward this effort, we reviewed the literature to catalog all known factors predicting phishing susceptibility. Relevant papers were found through searches on Google Scholar, PsycINFO, ACM Digital Library, and IEEE using variations of the keywords individual, characteristic, predict, susceptibility, and phish. Reference lists were then used to find further studies for inclusion. Significant predictors from each paper were then synthesized into the following 32 predictors.

To our knowledge, ours is the only paper to-date to comprehensively review all the current literature related to predicting phishing susceptibility, which is a necessary step in creating a holistic phishing susceptibility model. This paper also provides a valuable resource for those working in this space who wish to better understand the current literature surrounding phishing susceptibility prediction.

PREDICTORS OF PHISHING SUSCEPTIBILITY

Personality Traits

Conscientiousness. Users who fall for phishing scams were higher in conscientiousness, or the tendency to be dependable and self-controlled, than those who do not fall for phishing scams (Halevi et al., 2015). Frauenstein and Flowerday (2020), however, found that high-conscientiousness users were less susceptible to phishing attacks on social networking sites due to lower reliance on quick, heuristic processing.

Agreeableness. Agreeableness, characterized by warmth and friendliness, was shown to be a significant predictor of phishing susceptibility such that those high in agreeableness were more susceptible (Alseadon, 2014).

Emotional Instability. Also known as neuroticism, one study found that the tendency to experience negative feelings (e.g., guilt) had a significant positive correlation with phishing susceptibility, but this relationship was only present for women (Halevi et al., 2013). Confirming this finding, Alseadon (2014) found that emotional *stability* was a significant predictor of phishing susceptibility such that those with low emotional stability were more susceptible, regardless of gender.

Openness to Experience. Openness to experience, or the willingness to try new things, was significantly positively correlated with phishing susceptibility (Alseadon, 2014). Additionally, users who are less open to new experience deleted legitimate emails more often than those who are more open, a behavior which may indicate less susceptibility to phishing (Hong et al., 2013). Contrary to these findings, Pattinson et al. (2012) found that high-openness users who were not informed that they were in a phishing study were better able to correctly manage phishing emails than low-openness users.

Extraversion. Extraversion, or level of outgoingness, was a significant predictor of phishing susceptibility such that more extraverted users were more susceptible (Alseadon, 2014; Lawson et al., 2020). Another study also demonstrated that less extraverted users delete legitimate emails more often than more extraverted users, which may affect risk of falling for a phishing attack (Hong et al., 2013). Pattinson et al. (2012), however, found that high-extraversion users who were not informed that they were in a phishing study were better able to correctly manage phishing emails than low-extraversion users. Welk et al. (2015) similarly found that low-extraversion users had better performance on a phishing detection task compared to high-extraversion users.

Impulsivity. Impulsivity, measured using the abbreviated impulsiveness scale (ABIS) from Coutlee et al. (2014), was a significant predictor of engagement in risky cybersecurity behaviors, such as downloading media from unlicensed sources and clicking on email links, which are related to falling for a phishing attack. Specifically, attentional and motor impulsivity were significant positive predictors for risky cybersecurity behavior. Non-planning, however, was a significant negative predictor (Hadlington, 2017). Additionally, impulse and emotion control were positively correlated with accurate phishing detection (Lawson et al., 2020; Welk et al., 2015).

Another study used the Cognitive Reflection Test (CRT; Frederick, 2005) to measure situational impulsivity in decision-making and found a significant correlation between impulsivity and judgments made about phishing email links such that those who were less impulsive were more likely to judge the link as unsafe (Butavicius et al., 2015). Jones et al. (2019) found CRT scores to significantly predict phishing susceptibility with higher CRT scores corresponding to lower susceptibility. Similarly, Parsons et al. (2013) found that those with higher CRT scores who did not know that they were participating in a phishing study were better able to appropriately respond to phishing emails.

Contrary to these findings, however, Kumaraguru et al. (2007) demonstrated that those with higher CRT scores were more likely to click on links in phishing emails even though they did not hold accounts with the apparent sender company, potentially due to curiosity or higher risk-taking tendencies. Similarly, Parsons et al. (2019) found that CRT score was a predictor of phishing susceptibility such that those with lower *situational* impulsivity were more susceptible. Interestingly, they also found that a measure of *dispositional* impulsivity (Hamilton et al., 2016) was a significant predictor such that those higher in dispositional impulsivity were less susceptible. These findings suggest that situational and dispositional impulsivity may differently predict susceptibility.

Sensation Seeking. The tendency to seek out new experiences and sensations, measured using a scale from Hoyle et al. (2002), significantly predicted phishing susceptibility such that those who were higher in sensation seeking were less able to discriminate between phishing and legitimate emails (Jones et al., 2019). Additionally, Whitty (2019) found that users with high sensation seeking and addictive tendencies were more likely to be cyber fraud victims.

Curiosity. The desire to acquire new knowledge and sensory experiences, or epistemic curiosity, measured using scales from Litman and Spielberger (2003), was shown to be a significant predictor of phishing susceptibility such that more curious users were more susceptible (Moody et al., 2017).

Risk Propensity. The tendency to take risks in different facets of life, measured using a scale from Nicholson et al. (2005), was shown to significantly predict phishing susceptibility such that those with higher risk propensity were more susceptible, but only when the phishing email came from a known source and the link it contained was text rather than numeric (Moody et al., 2017). Similarly, Sheng et al. (2010) found that financial risk aversion predicted phishing susceptibility such that users who were more risk averse were less susceptible.

Dispositional Trust and Distrust. Dispositional trust, or the tendency to believe in others' positive attributes, was shown to be a significant positive predictor of phishing susceptibility (scale developed by McKnight et al., 2004; Alseadon, 2014; Workman, 2008; Wright et al., 2009). Additionally, Hong et al. (2013) demonstrated that less trusting users were more likely to delete legitimate emails, a behavior that could potentially lower risk of falling for an attack. Although Moody et al. (2017) did not find significant main effects, they demonstrated that some subscales of dispositional trust, as well as distrust, measured using a scale from Moody et al. (2014), may be predictors of phishing susceptibility with stronger effects occurring when the user knows the apparent sender of the phishing email compared to when they do not. Wright and Marett (2010) did not find dispositional trust to predict phishing susceptibility; however, they did find that higher suspicion of humanity (i.e., distrust) was associated with lower susceptibility.

Submissiveness. Submissiveness, associated with obedience and compliance with an authority, was shown to be a significant positive predictor of phishing susceptibility in populations from two different countries (Alseadon, 2014; Alseadon et al., 2012). Additionally, Workman (2008) found obedience to authority to be a significant predictor of phishing susceptibility such that those who were more obedient were more susceptible.

Demographics

Age. Several studies have found that susceptibility is highest for users aged 18-25 and decreases with age (Jagatic et al., 2007, Kumaraguru et al., 2009; Parsons et al., 2019). However, other studies have failed to show a difference in phishing susceptibility by age (Gavett et al., 2017; Mohebzada et al., 2012; Moody et al., 2017; Zielinska et al., 2014), have shown gender, education, and Internet experience to be mediating factors (Lin et al., 2019; Sheng et al., 2010), or suggest that older adults may in fact be more susceptible than younger adults (Li et al., 2020; Lin et al., 2019; Whitty, 2019).

Sex. Several studies have shown that women tend to be more susceptible to phishing compared to men (Hong et al., 2013; Jagatic et al., 2007). In one study, 40% of women fell for a two-step phishing scheme compared to only 27% of men (Halevi et al., 2015). Another study found that 14% of men compared to

53% of women fell for a phishing attack (Halevi et al., 2013), indicating that sex differences in susceptibility may be large. This difference in susceptibility may, however, be mediated by technical knowledge (Sheng et al., 2010). Other studies did not find susceptibility differences between sexes (Gavett et al., 2017; Kumaraguru et al., 2009; Moody et al., 2017; Parsons et al., 2019; Zielinska et al., 2014), or suggest that men may in fact be more likely than women to click on phishing links and disclose personal information (Mohebzada et al., 2012).

Educational Background

Education Level. Education level significantly predicted suspiciousness toward phishing such that those with higher levels of education were more suspicious (Gavett et al., 2017), indicating that they are less likely to be phished. One study also found that those with a higher level of education were significantly better at correctly managing phishing emails, but only when they were not told that the study involved phishing (Parsons et al., 2013). Other studies, however, fail to show that education predicts susceptibility (Moody et al., 2017)

Academic Major. One study by Jagatic et al. (2007) demonstrated that those in science- and technology-related majors (e.g., computer science) were less susceptible to regular phishing than other majors. Interestingly, however, users in science majors were the most susceptible group to phishing when messages appeared to be from a friend.

Contrary to these findings, Parsons et al. (2013) found that when users were not told that they were in a phishing study, those who had completed a course in information systems or information technology were less able to correctly manage phishing emails. Additionally, employees in technical jobs were shown to equal non-technical employees in their ability to discriminate between phishing and legitimate emails, even after receiving anti-phishing training (Kumaraguru et al., 2008).

Cybersecurity-Related Experience and Beliefs

Computer Security Awareness. A user's self-reported level of technical knowledge and security awareness predict phishing susceptibility such that those with more knowledge and awareness are less susceptible (Heartfield et al., 2016; Sheng et al., 2010; Wright & Marett, 2010). Additionally, users who are more aware of cyber-risks and have a more pessimistic view of risk while using the Internet, measured using a scale from Campbell et al. (2007), were less susceptible to phishing. Specifically, those who believe they have a high likelihood of receiving spam emails, being misled, or being infected with a computer virus were less likely to be phished (Halevi et al., 2015). Downs et al. (2007), however, found that knowledge about general computer risks and concepts (e.g., cookies, viruses) did not predict phishing susceptibility.

Phishing Knowledge. Those who are familiar with the definition of phishing were significantly less likely to fall for email and website phishing scams (Downs et al., 2007). Wang et al. (2012) also showed that as scam knowledge increases, users are less likely to fall for phishing. In one study, older adults with prior knowledge of phishing and/or who had previously fallen victim to a phishing attack reported more suspiciousness toward phishing attempts than those without this prior knowledge (Gavett et al., 2017). However, one study that conducted a simulated phishing campaign on a university population showed that users who clicked on a link contained in a phishing email were more likely to click on another phishing link the week after (Li et al., 2020).

Type of Computer Security Training. Security training includes formal education, self-study, and work-based training. All three of these training methods have been shown to predict phishing susceptibility such that those with more training are less susceptible (Heartfield et al., 2016). Other studies also demonstrated that users who received anti-phishing training were significantly less likely to fall for subsequent phishing attacks, even up to a month later (Kumaraguru et al., 2009; Kumaraguru et al., 2008; Sheng et al., 2010).

Time Since Last Security Training. Regardless of type of security training, the time elapsed since the last training was shown to predict phishing susceptibility, although time since last self-study was the primary predictor. Users with more time since their last training were more susceptible, indicating the importance of staying up to date on new security-related topics (Heartfield et al., 2016).

Concern for Online Privacy. Online privacy concern, or apprehension surrounding disclosing personal information online, was shown to be a significant positive predictor of responding to a friend request from a fake profile on Facebook, but not of subsequently responding to a phishing message sent from this profile (Vishwanath, 2015).

Attitudes toward Cybersecurity. More negative attitudes and lower engagement with cybersecurity practices, measured using the attitudes towards cybersecurity and cybercrime in business scale (ATC-IB; Hadlington, 2017), were found to positively predict engagement in risky cybersecurity behaviors (Hadlington, 2017), which are often engaged in when a user falls for a phishing attack.

Platform Experience

Computer Literacy. A user's self-efficacy while using a computer was a highly important predictor of phishing susceptibility such that those with higher literacy were less susceptible (Heartfield et al., 2016; Wright & Marett, 2010).

Computer and Internet Usage. For users who were informed that they were in a phishing study, high familiarity with computers was associated with better phishing email management (Pattinson et al., 2012). Parsons et al. (2019) also found that percentage of time spent using a computer was a significant predictor of phishing susceptibility such that users who spent more time on a computer were more susceptible. Similarly, Moody et al. (2017) showed that a user's cumulative time spent on the Internet predicted phishing susceptibility with more time associated with higher susceptibility. Kumaraguru et al. (2007), however, did not find a relationship between hours spent on the Internet and susceptibility. Other studies have found the opposite relationship, where more web experience is in fact associated with lower susceptibility and increased ability to detect phishing (Wright et al., 2009; Wright & Marett, 2010).

Platform Familiarity. Knowing what is normal and abnormal for a platform may affect susceptibility to phishing attacks delivered via that platform. Familiarity with and comfort using email, measured with a scale from Carlson and Zmud (1999), were significant predictors of phishing susceptibility such that those with more experience were less susceptible (Alseadon et al., 2012). Downs et al. (2007) also found that users of PayPal and eBay were less likely to fall for email and web-based phishing attacks that spoofed these sites. However, Heartfield et al. (2016) did not find that familiarity with a platform type (e.g., email) or specific provider's platform (e.g., Gmail) predicted susceptibility.

Frequency of Use. How often a user accesses a particular platform predicted phishing susceptibility such that those who accessed a platform more often were less susceptible (Heartfield et al., 2016). Interacting with a particular platform may increase awareness of platform-specific phishing.

Duration of Use. Those who access a platform for longer amounts of time were less susceptible to phishing (Heartfield et al., 2016). Users who spend more time on a platform may have more opportunities to become familiar with what platform-specific attacks look like.

Habitual Use. Habitual platform use, or fixed, repeated patterns of behavior when interacting with a platform, causes inattention and lowered conscious involvement. Vishwanath et al. (2011) showed that habitual email use significantly contributed to phishing email susceptibility. Additionally, habitual Facebook use was the largest predictor of victimization in a social media-based attack (Vishwanath, 2015), indicating that susceptibility may be specifically related to habitual use on a particular platform type.

Internet Addiction. Internet addiction, measured using the online cognition scale from Davis et al. (2002), was a significant positive predictor of risky cybersecurity behaviors related to falling for a phishing attack (Hadlington, 2017).

Email Behaviors

Email Load. Vishwanath et al. (2011) demonstrated that those who received many emails were more likely to respond to phishing emails. Musuva et al. (2019), however, found that those who received many emails were less susceptible to phishing. Instead, those who were the most responsive to the emails they did receive were the most susceptible.

Tendency to Completely Read Emails. Users who completely read emails were significantly better at detecting phishing emails than those who glanced at or did not completely read the email contents (Welk et al., 2015).

Perceived Email Richness. Perceived email richness, or the ability to recognize that an email contains rich communication information (Carlson & Zmud, 1999), was a significant predictor of phishing susceptibility such that those who were better able to recognize the richness of email were less susceptible (Alseadon, 2014). In another study, however, perceived email richness was not shown to significantly predict susceptibility (Alseadon et al., 2012).

Work Commitment Style

Work commitment style consists of three subscales related to the reasons why people are committed to their job: 1) *normative* commitment based on obligation; 2) *continuance* commitment based on perceived benefits of employment and costs of leaving; and 3) *affective* commitment based on organizational identification and emotional attachment (Meyer & Allen, 1991). Workman (2008) found that work commitment style predicted phishing susceptibility depending on the content of the attack. Those high in normative commitment were susceptible to attacks involving reciprocation; those high in continuance commitment were susceptible to attacks involving escalating requests; and those high in affective commitment were susceptible to attacks involving social desirability. Vishwanath (2015) also found normative and continuance commitment to be significant positive predictors of responding to a friend request from a fake profile on Facebook, but not of subsequently responding to a phishing message sent from this profile. Affective commitment did not contribute to phishing susceptibility.

CONCLUSIONS AND FUTURE DIRECTIONS

The current review provides a summary of previous work identifying 32 known predictors of interest related to phishing susceptibility. These predictors can be categorized as personality traits, demographics, educational background, cybersecurity experience and beliefs, platform experience, email behaviors, and work commitment style.

To holistically evaluate all of these predictors and their relationships to each other and phishing susceptibility, we will conduct a large-scale human subjects experiment. This experiment will first have participants complete a measure of each known phishing susceptibility predictor. Then, participants will complete a phishing susceptibility test in which they will view a randomized set of emails, half of which will be phishing emails. Their judgements of whether each email is a phishing attack will provide a measure of phishing susceptibility. We will then use regression-based statistical analyses and machine learning approaches to determine the relationships among factors and determine which set of factors best predicts a user's phishing susceptibility.

ACKNOWLEDGEMENTS

This research was supported by the U.S. National Science Foundation (Award #: 1723765) and the U.S. Office of Naval Research (Award #: N00014-21-1-2007). Opinions, findings, and conclusions are those of the authors and do not necessarily reflect the views of the NSF or ONR.

REFERENCES

Alseadon, I. M., Chan, T., Foo, E., & Gonzalez Nieto, J. (2012). Who is more susceptible to phishing emails? A Saudi Arabian study. *ACIS 2012 Proceedings.* 1-11.

Alseadoon, I. M. (2014). The impact of users' characteristics on their ability to detect phishing emails [Doctoral dissertation, Queensland University of Technology].

Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2015). Breaching the human firewall: Social engineering in phishing and spear-phishing emails, *arXiv:1606.00887*, 1–10.

Campbell, J., Greenauer, N., Macaluso, K., & End, C. (2007). Unrealistic optimism in internet events. *Computers in Human Behavior*, *23*, 1273-1284.

Carlson, J. R., & Zmud, R. W. (1999). Channel expansion theory and the experiential nature of media richness perceptions. *Academy of management journal, 42*(2), 153-170.

Coutlee, C. G., Politzer, C. S., Hoyle, R. H., Huettel, S. (2014). An abbreviated impulsiveness scale constructed through confirmatory factor analysis of the Barratt Impulsiveness Scale Version 11. *Archives of Scientific Psychology, 2*(1), 1-12, https://doi.org/10.1037/arc0000005

Davis, R. A., Flett, Gl. L., & Besser, A. (2002). Validation of a new scale for measuring problematic Internet use: Implications for pre-employment screening. *CyberPsychology & Behavior*, *5*(4), 331-345.

Downs, J. S., Holbrook, M., & Cranor, L. F. (2007). Behavioral response to phishing risk. *Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit*. 37-44.

Frauenstein, D. E., & Flowerday, S. V. (2020). Susceptibility to phishing on social network sites: A personality information processing model. *Computers & Security*, *94*, 1-18.

Frederick, S. (2005). Cognitive reflection and decision making. *Journal of Economic Perspectives*, *19*(4), 25-42.

Gavett, B. E., Zhao, R., John, S. E., Bussell, C. A., Roberts, J. R., & Yue, C. (2017). Phishing suspiciousness in older and younger adults: The role of executive functioning. *PLOS ONE, 12*(2).

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7).

Halevi, T., Lewis, J., & Memon, N. (2013). A Pilot Study of Cyber Security and Privacy Related Behavior and Personality Traits. *WWW '13 Companion: Proceedings of the 22nd International Conference on World Wide Web*. 737-744.

Halevi, T., Memon, N., & Nov, O. (2015). Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. *SSRN Electronic Journal*.

Hamilton, K., Shih, S.-I., & Mohammed, S. (2016). The development and validation of the rational and intuitive decision styles scale. *Journal of Personality Assessment*, *98*(5), 523-535.

Heartfield, R., Loukas, G., & Gan, D. (2016). You are probably not the weakest link: Towards practical prediction of susceptibility to semantic social engineering attacks. IEEE Access, 4, 6910–6928.

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, *55*(1), 74-81.

Hong, K. W., Kelley, C. M., Tembe, R., Murphy-Hill, E., & Mayhorn, C. B. (2013). Keeping up with the Joneses: Assessing phishing susceptibility in an email task. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 57*(1), 1012–1016.

Hoyle, R. H., Stephenson, M. T., Palmgreen, P., Pugzles Lorch, E., & Lewis Donohew, R. (2002). Reliability and validity of a brief measure of sensation seeking. *Personality and Individual Differences*, *32*, 401-414.

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

Jones, H. S., Towse, J. N., Race, N., & Harrison, T. (2019). Email fraud: The search for psychological predictors of susceptibility. *PLOS ONE, 14*(1).

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 on Usable Privacy and Security - SOUPS '09*.

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F., & Hong, J. (2007). Getting users to pay attention to anti-phishing education. *Proceedings of the Anti-Phishing Working Groups 2nd Annual ECrime Researchers Summit*, 70–81.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2008). Lessons from a real world evaluation of anti-phishing training. *2008 ECrime Researchers Summit*.

Lawson, P., Pearson, C. J., Crowson, A., & Mayhorn, C. B. (2020). Email phishing and signal detection: How persuasion principles and personality influence response patterns and accuracy. *Applied Ergonomics, 86*, 103084.

Li, W., Lee, J., Purl, J., Greitzer, F., Yousefi, B., & Laskey, K. (2020). Experimental Investigation of Demographic Factors Related to Phishing Susceptibility. *Proceedings of the 53rd Hawaii International Conference on System Sciences.*

Lin, T., Capecci, D. E., Ellis, D. M., Rocha, H. A., Dommaraju, S., Oliveira, D. S., & Ebner, N. C. (2019). Susceptibility to spear-phishing emails. *ACM Transactions on Computer-Human Interaction, 26*(5), 1–28.

Litman, J. A., & Spielberger, C. D. (2003). Measuring epistemic curiosity and its diversive and specific components. *Journal of Personality Assessment*, *80*(1), 75-86.

McKnight, D. H., Kacmar, C. J., & Choudhury, V. (2004). Dispositional trust and distrust distinctions in predicting high-and low-risk Internet expert advice site perceptions. *E-Service, 3*(2), 35-58.

Meyer, J. P. & Allen, N. J. (1991). A three-component conceptualization of organizational commitment. *Human Resource Management Review*, *1*(1), 61-89.

Mohebzada, J. G., Zarka, A. E., Bhojani, A. H., & Darwish, A. (2012). Phishing in a university community: Two large scale phishing experiments. *2012 International Conference on Innovations in Information Technology (IIT)*.

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

Moody, G. D., Galletta, D. F., & Lowry, P. B. (2014). When trust and distrust collide online: The engenderment and role of consumer ambivalence in online consumer behavior. *Electronic Commerce Research and Applications*, *12*, 266-282.

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

Nicholson, N., Soane, E., Fenton-O'Creevy, M., & Willman, P. (2005). Personality and domain-specific risk taking. *Journal of Risk Research, 8*(2), 157-176.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2013). Phishing for the truth: A scenario-based experiment of users' behavioural response to emails. In L. J. Janczewski, H. B. Wolfe, & S. Shenoi (Eds.), *SEC 2013. IFIP Advances in Information and Communication Technology,* (pp. 366-378). Springer.

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.

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others? *Information Management & Computer Security, 20*(1), 18–28.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. *Proceedings of the 28th International Conference on Human Factors in Computing Systems.*

Vishwanath, A. (2015). Habitual Facebook use and its impact on getting deceived on social media. *Journal of Computer-Mediated Communication*, *20*(1), 83-98.

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems, 51*(3), 576–586.

Wang, J., Herath, T., Chen, R., Vishwanath, A., & Rao, H. R. (2012). Phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *IEEE Transactions on Professional Communication*, *55*(4), 345-362.

Welk, A. K., Hong, K. W., Zielinska, O. A., Tembe, R., Murphy-Hill, E., & Mayhorn, C. B. (2015). Will the "phisher-men" reel you in? *International Journal of Cyber Behavior, Psychology and Learning, 5*(4), 1–17.

Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime, 26*(1), 277–292.

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology, 59*(4), 662–674.

Wright, R. T., & Marett, K. (2010). The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. *Journal of Management Information Systems, 27*(1).

Wright, R., Chakraborty, S., Basoglu, A., & Marett, K. (2009). Where did they go right? Understanding the deception in phishing communications. *Group Decision and Negotiation, 19*(4), 391–416.

Zielinska, O. A., Tembe, R., Hong, K. W., Ge, X., Murphy-Hill, E., & Mayhorn, C. B. (2014). One phish, two phish, how to avoid the Internet phish: Analysis of training strategies to detect phishing emails. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 58*(1), 1466–1470.