Curiosity vs. Curiosity: Striking the Balance between Positive and Negative Outcomes in SETA Programs and Phishing Campaigns

Early stage paper

Philip Menard
The University of Texas at
San Antonio
philip.menard@utsa.edu

Hwee-Joo Kam
University of Tampa
hkam@ut.edu

Dustin K. Ormond
Creighton University
dustinormond@creighton.edu

Robert E. Crossler
Washington State University
rob.crossler@wsu.edu

ABSTRACT

Despite the best efforts of information security professionals, phishing remains one of the most successful attacks deployed by threat actors against organizations. Recent cybersecurity incidents have demonstrated that employees' innate curiosity instigated computer misuse, despite research indicating that curiosity can be leveraged for positive security outcomes. Curiosity has not been comprehensively studied in information security research from this vantage. In this study, we examine the tension between the benefits and detriments of curiosity among employees. In our proposed methodology, we will comprehensively assess the impact of curiosity through an experiment in which respondents participate in a SETA program designed to bolster curiosity according to specific types (or combinations of types). After the SETA program, we will present respondents with a series of legitimate emails and phishing messages, with the messages featuring language that leverages a specific type of curiosity in the content of the message. Additionally, we will survey respondents on their innate curiosity tendencies, allowing us to control for individual differences in curiosity among our sample. Based on this repeated-measures experimental design, we will use multilevel modeling to assess cross-level effects of between-subjects (individual) factors on within-subjects (message-level) outcomes.

Keywords

curiosity; SETA programs, phishing, multilevel modeling.

INTRODUCTION

Given the number of cyberthreats that exist, the constant battle for information security professionals against threat actors can be very daunting. Despite attempts to lessen the impact of these threats, organizations continue to fall susceptible to attacks, especially phishing attacks. For example, Cybertalk (2022) reported that 83% of organizations experienced a phishing attack in 2021 and further indicated that 90% of all organizational breaches are a result of phishing attacks. Recent high-profile examples highlight the devastating impacts resulting from phishing. Sony Pictures, JPMorgan Chase, Facebook, Google, and the US Democratic National Committee have each experienced financial damages and public embarrassment due to data breaches instigated by phishing attacks. Perhaps most alarmingly, the US Cybersecurity & Infrastructure Security Agency (CISA) has reported increased activity focused on infiltrating power grid systems through spear phishing attacks. The 2021 Verizon Data Breach Incident Report (Verizon Enterprise Solutions, 2021) reveals that social engineering is the most common attack type, with phishing being the primary technique utilized. Many organizations have made great strides in improving the technical countermeasures employed within their systems, yet human insiders represent an obvious weak point due to phishing susceptibility.

Employees' susceptibility to phishing attacks may be explained by gaining a better understanding of the role of curiosity. Recent cybersecurity incidents have demonstrated that employees' innate curiosity instigated computer misuse. A 2016 survey led by Black Hat revealed that 34% of users clicked on a suspicious link due to curiosity (Benenson et al., 2017) in spite of their information security awareness (ISA). A hacking group named "FIN7" cyber gang launched a social engineering attack by using a Windows 11 logo to entice employees to download malware-infected Word documents (ComTech Computer Services, 2021). Some employees downloaded the document out of their curiosity toward the new Windows 11 operating systems.

This presents an interesting problem, as curiosity has long been studied as a positive attribute that organizations can leverage for beneficial outcomes. In fact, information security researchers have observed such positive impacts. Silic and Lowry (2020) found that curiosity is an important component of piquing and maintaining interest within a security education training and awareness (SETA) program, which subsequently leads to positive organizational security outcomes. While research has indicated that curiosity can positively impact an organization's security profile, researchers have yet to examine which type of curiosity is most effective. Additionally, security researchers have also not tested the effectiveness of curiosity in the face of a phishing campaign designed to leverage employees' vulnerabilities derived from curiosity.

Although real-life incidents suggest that human curiosity could threaten information assets protection, the negative consequences of curiosity have not been widely studied in information security research from this vantage. Moody et al. (2017) empirically established that innately curious individuals were prone to phishing attacks. Meanwhile, Frauenstein & Flowerday (2020) demonstrated that phishing emails targeting curiosity could successfully trick victims into engaging with the email. These findings suggest that curiosity could be a threat to information asset protection. However, because the authors only examined curiosity as a generic trait and not from the vantage of specific curiosity types, these studies did not fully test the boundary conditions under which curiosity's role is maximally detrimental. Researchers recognize that curiosity can result in both positive and negative outcomes. Yet, we do not currently possess a comprehensive understanding of how to strike the proper balance of maximizing the benefits of curiosity and minimizing its detriments. This leads to our research question:

> *RQ: How can curiosity be leveraged to maximize desirable psychological processes related to SETA programs and minimize detrimental psychological processes related to phishing susceptibility?*

In this study, we examine the tension between the benefits and detriments of curiosity among employees. According to foundational research, curiosity manifests as four major types: epistemic, perceptual, sensory, and interpersonal. In our proposed methodology, we will comprehensively assess the impact of curiosity through an experiment in which respondents participate in a SETA program leveraging a type of curiosity (or combination of types). After the SETA program, we will present respondents with a series of legitimate and phishing messages, with the messages leveraging specific types of curiosity in the content of the message. Additionally, we will survey respondents on their innate curiosity tendencies, allowing us to control for individual differences in curiosity among our sample.

In the remainder of the paper, we provide the background literature and hypothesis development of our research model and provide more details regarding our proposed methodology and empirical analysis.

LITERATURE REVIEW AND HYPOTHESIS DEVELOPMENT

SETA Programs

SETA programs consist of distinct education, training, and awareness initiatives that impart an organization's information security policy to its employees (Guttman & Roback, 1995). SETA programs can be operationalized in various ways and emphasize delivering broad information about the security environment along with the skills required to perform any necessary security protocols (Lee & Lee, 2002; Whitman et al., 2001). Education, training, and awareness programs are individual categories of SETA and satisfy specific organizational goals (Cram et al., 2019; Crossler & Bélanger, 2014; Hu et al., 2021). An awareness program focuses on disseminating information about threats facing the organization and the countermeasures available to employees to mitigate such threats. Awareness programs are intended to increase employees' recognition of the pertinent threats to the corporate environment and reinforce the organization's chosen security practices and procedures. Compared to awareness programs, training programs shift the focus from the "what" the critical threats and associated countermeasures are to "how" employees can use the organization's given countermeasures to minimize specific threats. Training typically involves hands-on demonstrations within sandboxed environments. Education programs provide opportunity for deeper reflection into foundational security principles but are outside the purview of organizational SETA. Most employees will only participate in awareness and training programs, as education programs are primarily reserved for employees whose positions necessitate extensive security knowledge (i.e., security certification programs or degrees). Because of its interactive and educational components, SETA may be an ideal avenue for organizations to leverage its employees' curiosity.

Curiosity

Curiosity is a complex phenomenon that researchers have conceptualized in several ways. In broad terms, curiosity is a person's craving of new information or stimuli that promotes exploration. Under Berlyne's (1954) conceptualization, curiosity broadly fell under only two categories: epistemic curiosity and perceptual curiosity. *Epistemic curiosity* is defined as a person's drive to know and is aroused by knowledge gaps (Berlyne, 1954). *Perceptual curiosity* leads to a person's increased perception of and attention toward a specific stimulus and is aroused by visual, auditory, or tactile stimulation (Berlyne, 1954). Further, curiosity can be distinguished based on the type of exploration undertaken due to curiosity: diversive and specific exploration (Berlyne, 1960). Diversive exploration derives from the innate need for stimulation, regardless of the source or content; specific exploration is driven by curiosity toward a particular object or concept. Within both epistemic and perceptual curiosity, diversive and specific exploration can occur (i.e., epistemic-diversive curiosity or epistemic-specific curiosity). Researchers have established a robust lineage of empirical works examining these types of curiosity. For example, studies have shown that both epistemic-diversive and epistemic-specific curiosity facilitated creativity for problem-solving (Hardy III et al., 2017) and idea generation (Hagtvedt et al., 2019). However, in the decades since the initial conception of curiosity, two other types have been theorized and studied: sensory curiosity and interpersonal curiosity.

Sensory curiosity is a type of sensation-seeking behavior that drives a person to pursue increased sensory arousal and motivates a person's search for "novel or unusual sensory experiences" (J. A. Litman et al., 2005, p. 1125). *Interpersonal (or empathic) curiosity* is the drive to seek information about people, such as knowledge about individuals' experiences, their public and private behaviors, and their thoughts and feelings (J. A. Litman & Pezzo, 2007). Additionally, curiosity may be conceptualized or measured as emotional states elicited by specific stimuli (Yi et al., 2015) or as relatively stable tendencies that describe individuals' overall curiosity patterns that persist across a variety of stimuli (Kashdan et al., 2018).

Positive Outcomes of Curiosity

Across the various business disciplines (including IS), researchers have viewed curiosity as a personality type among employees that can be leveraged for positive outcomes. Curiosity has garnered considerable attention from the various business disciplines, with studies examining its effect on outcomes such as job performance (Mussel, 2013; Reio & Callahan, 2004), adaptation to new work environments (Harrison et al., 2011), knowledge collaboration (Faraj et al., 2011; Jeppesen & Frederiksen, 2006), voluntary contribution (Kokkodis et al., 2020), work-based creativity (Harrison & Dossinger, 2017), and entrepreneurial drive (Jeraj & Antoncic, 2013). Specific to IS research, Agarwal and Karahanna (2000) suggest that curiosity decreases the mental burden related to interacting with technology, thereby raising the probability of a person engaging. Relatedly, Lowry et al. (2013) showed that curiosity is an important factor in driving behavioral intention to use a system from a hedonic perspective. Additionally, people who are naturally more curious tend to pursue new opportunities online (McElroy et al., 2007; Tuten & Bosnjak, 2001), including a greater likelihood of engaging with advertisement emails (Chen et al., 2011). Schneider et al. (2013) proposed a research model with curiosity positioned as the key motivator of online lurking behavior. Yi et al. (2015) found that online product presentations could arouse consumers' curiosity and lead to increased purchase intentions. Overall, curiosity appears to be a fertile stream for ongoing IS research, including the security context.

Within the information security context, curiosity has been shown to have a positive effect on the effectiveness of SETA programs (Silic & Lowry, 2020). With the ongoing shortage of cybersecurity employees, researchers have found that leveraging employees' interest in cybersecurity plays an important role in re-training existing employees toward cybersecurity functions (Kam et al., 2022). Curiosity is closely linked to interest (Loewenstein, 1994) and likely serves as a critical trigger for instigating an employee's desire to pursue (or at least entertain) further training in cybersecurity. These studies have established that curiosity has a positive impact on an organization's overall security profile. However, much remains to be explored, including how specific forms of curiosity can be leveraged within SETA to maximize the program's impact.

In a prominent branch of curiosity research, Loewenstein (1994) posits that information gaps are critical drivers of curiosity. Attaining knowledge that fills an information gap directly satisfies an individual's epistemic curiosity. A SETA program on phishing mitigation that appeals to a participant's drive to fill an information gap will elevate the participant's epistemic curiosity, decreasing the likelihood of the participant's susceptibility to a phishing attack.

> *H1a: A SETA program that leverages epistemic curiosity will lead to decreased phishing susceptibility.*

Researchers have found that atmospheric cues, such as engaging audio/visual design, affect interaction with a given stimulus based on how much a person's perceptual curiosity is aroused by the cues (Koo & Ju, 2010). Therefore, as perceptual curiosity increases, a person is more likely to engage with a given stimulus. A SETA program on phishing mitigation that is crafted to capture a participant's attention through audio/visual design will pique the participant's perceptual curiosity, decreasing the likelihood of the participant's susceptibility to a phishing attack.

> *H1b: A SETA program that leverages perceptual curiosity will lead to decreased phishing susceptibility.*

Sensory curiosity is directly linked to a person's tendency toward seeking new sensations (J. A. Litman et al., 2005). When a person's sensory curiosity is piqued, the person is more likely to seek novel activities. Capturing a person's attention is critical within a SETA program (Kam et al., 2022), and sensory curiosity may be a key motivator in driving a person to pursue training on a particular security topic. A SETA program on phishing mitigation crafted to appeal to a participant's sensation-seeking desires will lead to elevated perceptions of sensory curiosity, thereby decreasing the chances of the participant being tricked into interacting with a phishing message.

> *H1c: A SETA program that leverages sensory curiosity will lead to decreased phishing susceptibility.*

Interpersonal curiosity is related to a person's desire to seek out "people-information" (J. A. Litman & Pezzo, 2007). Relatedly, researchers and practitioners have called for organizations to pursue a more people-centric model of information security (Blum, 2020), where employee considerations are integrated in organizational security designs. Tapping into a person's interpersonal curiosity may be an important lever in fostering a personal connection to the importance of a specific security topic, like phishing. A SETA program on phishing mitigation crafted to appeal to the humanity of the participant will result in elevated perceptions of interpersonal curiosity, decreasing the likelihood that the participant will fall prey to a phishing attack.

> *H1d: A SETA program that leverages interpersonal curiosity will lead to decreased phishing susceptibility.*

Negative Outcomes of Curiosity

Despite its potential benefits, curiosity may also drive employees to be more susceptible to phishing attacks (Moody et al., 2017). In fact, for some of the same reasons that curiosity can be leveraged for organizational benefits, social engineers can leverage curiosity to entice unwitting victims to interact with phishing attacks. Building on prior research into the effects of general dispositional curiosity on phishing susceptibility, we posit that phishing messages crafted to leverage specific forms of curiosity will elicit momentary perceptions of curiosity and ultimately increase the likelihood of phishing susceptibility. Conversely, if a phishing message does not elicit sufficient curiosity, the employee is more likely to pay attention to the external cues that signal the possibility of a phishing message or ignore the email altogether.

Research indicates that curiosity may derive from perceptions of information deprivation (J. Litman, 2005; J. A. Litman & Jimerson, 2004; Loewenstein, 1994) and lead to a desire to know more (Berridge, 1999; Berridge & Robinson, 1998). Curiosity derived from deprivation elicits stronger emotions than curiosity as derived from interest in a subject matter area (J. A. Litman & Jimerson, 2004). Because curiosity elicits information seeking (J. A. Litman & Jimerson, 2004; Loewenstein, 1994), epistemic curiosity, if leveraged within the content of a phishing message, has the potential to negate training on how to avoid phishing.

> *H2a: A phishing campaign that leverages a victim's epistemic curiosity will lead to increased phishing susceptibility.*

Moody et al. (2017) included perceptual curiosity in their study as a sub-construct of dispositional curiosity. In this manner, perceptual curiosity contributed to a person's phishing susceptibility, lending evidence to the hypothetical effect of perceptual curiosity. However, its exact effect within the phishing context remains unclear, as the authors only report on the effect of trait-based curiosity overall and did not treat perceptual curiosity as a pliable emotional state. Research has shown that stimuli can arouse perceptual curiosity, in turn capturing a person's attention as indicated by eye movement (Risko et al., 2012). Perceptual curiosity likely drives engagement with a phishing message in a similar fashion to interacting with a SETA program. As perceptual curiosity increases, a person is more likely to engage with a given stimulus (Koo & Ju, 2010). We believe that a phishing message that is crafted to capture a victim's attention through audio/visual design will pique the victim's perceptual curiosity, increasing the likelihood of the victim's susceptibility to the attack.

> *H2b: A phishing campaign that leverages a victim's perceptual curiosity will lead to increased phishing susceptibility.*

Researchers have linked perceptions of sensory curiosity to a person's risk-taking propensity, such as the desire to pursue entrepreneurial endeavors (Jeraj & Antoncic, 2013). If a person's sensory curiosity is triggered, the person will be less risk-averse and more willing to pursue an activity perceived as novel or thrilling. A phishing message crafted to appeal to a victim's sensation-seeking desires will lead to elevated perceptions of sensory curiosity, thereby increasing the chances of the victim being tricked into interacting with the phishing message.

> *H2c: A phishing campaign that leverages a victim's sensory curiosity will lead to increased phishing susceptibility.*

Although leveraging curiosity from a people-centric, empathic perspective results in positive outcomes for organizations, interpersonal curiosity potentially introduces problems as well. Researchers have found that interpersonal curiosity is a key antecedent of workplace gossip, which subsequently leads to multiple negative organizational outcomes (Sun et al., 2022). A phishing message crafted to appeal to victim's tendency toward snooping or spying behavior will result in elevated perceptions of interpersonal curiosity, increasing the likelihood of the receiver to fall prey to the phishing attack.

> *H2d: A phishing campaign that leverages a victim's interpersonal curiosity will lead to increased phishing susceptibility.*

Figure 1 illustrates the hypothesized relationships described above.

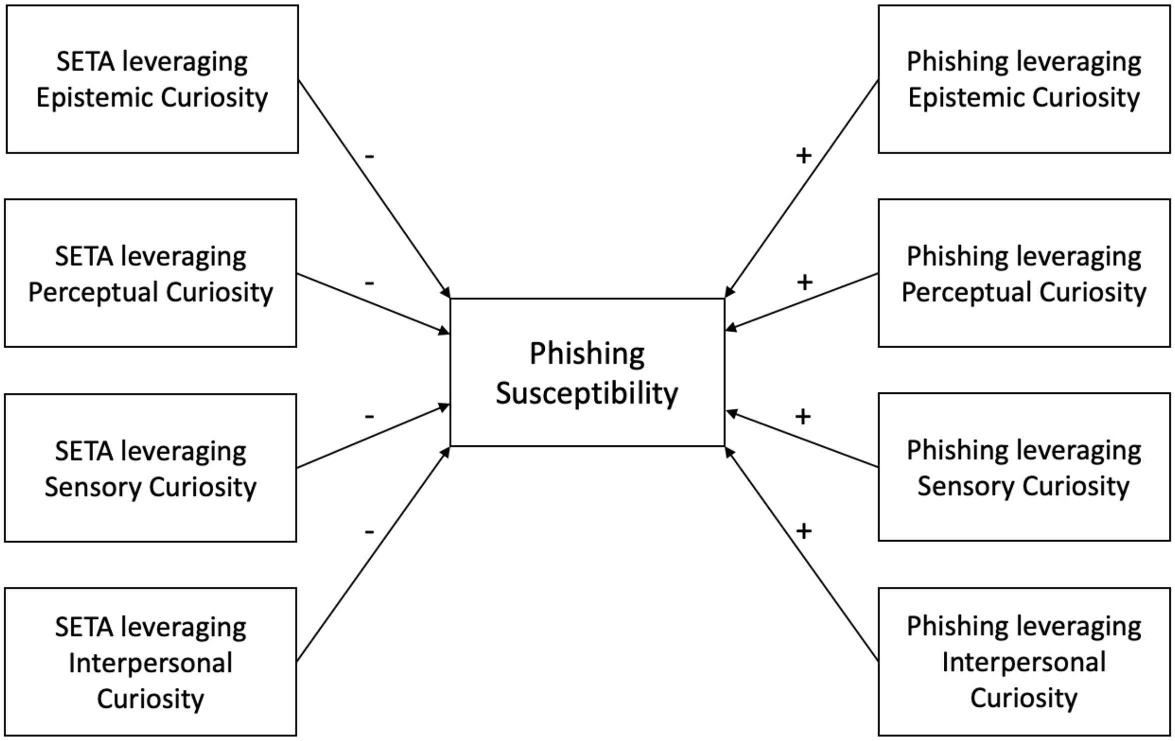
SETA leveraging Epistemic Curiosity
SETA leveraging Perceptual Curiosity
SETA leveraging Sensory Curiosity
SETA leveraging Interpersonal Curiosity
-
-
-
-
Phishing Susceptibility
+
+
+
+
Phishing leveraging Epistemic Curiosity
Phishing leveraging Perceptual Curiosity
Phishing leveraging Sensory Curiosity
Phishing leveraging Interpersonal Curiosity

Figure 1: Research Model

METHODS

To thoroughly examine how curiosity can produce positive and negative security outcomes in the context of phishing, we are planning on utilizing an experimental approach, described in the following sections. Because we have not collected data for this project, we welcome and appreciate any feedback that may improve our design.

Experimental Design

Our research design will feature an experiment where respondents will participate in a SETA program built to emphasize a type (or combination of types) of curiosity and will assess a series of email messages, indicating whether they believe the message is legitimate or phishing. This 2x2x2x2 full factorial design will result in 16 treatment groups representing the various combinations of curiosity-based SETA manipulations. The factorial manipulation matrix is shown in Table 1.

Table 1: Treatment Groups for Curiosity-based SETA Manipulations

	Curiosity Manipulations			
Treatment Group	**Epistemic**	**Perceptual**	**Sensory**	**Interpersonal**
1	N	N	N	N
2	N	N	N	Y
3	N	N	Y	N
4	N	N	Y	Y
5	N	Y	N	N
6	N	Y	N	Y
7	N	Y	Y	N
8	N	Y	Y	Y
9	Y	N	N	N
10	Y	N	N	Y
11	Y	N	Y	N
12	Y	N	Y	Y
13	Y	Y	N	N
14	Y	Y	N	Y
15	Y	Y	Y	N
16	Y	Y	Y	Y

N = curiosity type not leveraged; Y = curiosity type leveraged

The emails shown to the respondents will also be manipulated such that the message will emphasize one of the four types of curiosity. One message type will not feature curiosity-leveraged content, serving as a control. This results in 5 major message types. For each major message type, we will craft an email that is intended to be recognized as legitimate and one that is intended to be recognized as phishing, resulting in 10 total message types. We will display the messages to the respondents in random order and conduct post-hoc tests for order effect. For our experimental design that evaluates curiosity as it relates to SETA and phishing messages, we will conduct a pretest to ensure that the intended curiosity types are adequately perceived by the respondents.

Respondents' inherent curiosity traits may moderate the proposed effects of curiosity states. Researchers have identified a five-dimension structure to curiosity traits, resulting in four major curiosity dispositions: fascinated, problem solvers, empathizers, and avoiders (Kashdan et al., 2018). To control for respondents' innate curiosity traits, we will pre-screen our respondents with a survey measuring their curiosity types based on Kashdan et al.'s (2018) five-dimension conceptualization of curiosity (see Survey Instrument section below for further details on measurement scales used in this survey). We will use the results of the pre-screening instrument to ensure an even distribution of curiosity types within our 16 treatment groups.

Although calculating statistical power for multilevel models is more complex than single-level statistical models, researchers can utilize Monte Carlo simulations to estimate observed statistical power under varying conditions based on Level 1 and Level 2 sample sizes, estimated intraclass correlation coefficients, and effect sizes at each level (Arend & Schäfer, 2019). To achieve statistical power necessary to confidently interpret our two-level model (assuming medium-sized Level 1 and 2 direct effects and medium-sized random slopes for cross-level effects), our sample would need at least 175 respondents, with each respondent exposed to at least 12 experimental email messages (Arend & Schäfer, 2019). For practical purposes, we will sample 192 participants to ensure even distribution of respondents across treatment groups (12 per group) and an even distribution based on the four curiosity dispositions (3 respondents of a given type per group). To ensure an even distribution of email message types, we will show each respondent 20 messages (2 messages per message type).

Survey Instrument

During our pretest phase, we will conduct manipulation checks to ensure that each SETA program and phishing message used in the study will adequately elevate respondents' perceptions of the curiosity type(s) being manipulated. To measure curiosity perceptions, we will directly adapt previously validated scales for epistemic curiosity (J. A. Litman & Spielberger, 2003), perceptual curiosity (Collins et al., 2004), sensory curiosity (J. A. Litman et al., 2005), and interpersonal curiosity (J. A. Litman & Pezzo, 2007). To measure a respondent's general tendency toward a specific curiosity trait, we will use the five-dimension curiosity inventory (Kashdan et al., 2018). We list full inventory of measurement items in Appendix A.

DATA ANALYSIS AND RESULTS

Because we will be presenting our respondents with multiple messages to test their susceptibility to phishing, we will use multilevel modeling to assess both within-group and between-group effects. We will use Mplus as our statistical software (Muthén & Muthén, 2017).

CONCLUSION

Often, the easiest route to gaining access to organizational systems is by tricking employees through phishing campaigns or social engineering. Attackers are becoming more advanced in their deception techniques, and researchers must gain a better understanding of the psychological factors that contribute to a person's susceptibility to phishing, as well as training approaches that can impart the techniques employees can use to minimize the likelihood of being phished. In our proposed work, we hope to learn more about the psychological processes related to curiosity so that researchers can gain insight into how curiosity operates in this context. We also hope to equip security managers with tangible training techniques that can be incorporated into existing organizational SETA programs.

REFERENCES

Agarwal, R., & Karahanna, E. (2000). Time Flies When You're Having Fun: Cognitive Absorption and Beliefs about Information Technology Usage. *MIS Quarterly*, *24*(4), 665–694.

Arend, M. G., & Schäfer, T. (2019). Statistical power in two-level models: A tutorial based on Monte Carlo simulation. *Psychological Methods*, *24*(1), 1–19.

Benenson, Z., Gassmann, F., & Landwirth, R. (2017). Exploiting Curiosity and Context: How to Make People Click on a Dangerous Link despite their Security Awareness. *Black Hat 2016*. http://paper.seebug.org/papers/Security%20Conf/Blackhat/2016/us-16-Benenson-Exploiting-Curiosity-And-Context-How-To-Make-People-Click-On-A-Dangerous-Link-Despite-Their-Security-Awareness-wp.pdf

Berlyne, D. E. (1954). A theory of human curiosity. *British Journal of Psychology*, *45*(3), 180–191.

Berlyne, D. E. (1960). *Conflict, arousal, and curiosity*. McGraw-Hill.

Berridge, K. C. (1999). Pleasure, Pain, Desire, and Dread: Hidden Core Processes of Emotion. In *Well-being: The foundations of hedonic psychology* (pp. 525–557). Russell Sage Foundation.

Berridge, K. C., & Robinson, T. E. (1998). What is the role of dopamine in reward: Hedonic impact, reward learning, or incentive salience. *Brain Research Reviews*, *28*(3), 309–369.

Blum, D. (2020). *Rational Cybersecurity for Business: The Security Leaders' Guide to Business Alignment*. Springer Nature.

Chen, R., Wang, J., Herath, T., & Rao, H. R. (2011). An investigation of email processing from a risky decision making perspective. *Decision Support Systems*, *52*(1), 73–81.

Collins, R. P., Litman, J. A., & Spielberger, C. D. (2004). The measurement of perceptual curiosity. *Personality and Individual Differences*, *36*(5), 1127–1141.

ComTech Computer Services. (2021, September 21). Hackers Are Using Windows 11 Curiosity To Load Malware. *ComTech Computer Services, Inc.* https://www.comtech-networking.com/blog/item/hackers-are-using-windows-11-curiosity-to-load-malware/

Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2019). Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance. *MIS Quarterly*, *43*(2), 525–554. https://doi.org/10.25300/MISQ/2019/15117

Crossler, R., & Bélanger, F. (2014). An Extended Perspective on Individual Security Behaviors: Protection Motivation Theory and a Unified Security Practices (USP) Instrument. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *45*(4), 51–71. https://doi.org/10.1145/2691517.2691521

Faraj, S., Jarvenpaa, S. L., & Majchrzak, A. (2011). Knowledge Collaboration in Online Communities. *Organization Science*, *22*(5), 1224–1239. https://doi.org/10.1287/orsc.1100.0614

Frauenstein, E. D., & Flowerday, S. (2020). Susceptibility to phishing on social network sites: A personality information processing model. *Computers & Security*, *94*, 101862. https://doi.org/10.1016/j.cose.2020.101862

Guttman, B., & Roback, E. A. (1995). *An Introduction to Computer Security: The NIST Handbook* (Issue 800). U.S. Department of Commerce.

Hagtvedt, L. P., Dossinger, K., Harrison, S. H., & Huang, L. (2019). Curiosity made the cat more creative: Specific curiosity as a driver of creativity. *Organizational Behavior and Human Decision Processes*, *150*, 1–13.

Hardy III, J. H., Ness, A. M., & Mecca, J. (2017). Outside the box: Epistemic curiosity as a predictor of creative problem solving and creative performance. *Personality and Individual Differences*, *104*, 230–237.

Harrison, S. H., & Dossinger, K. (2017). Pliable Guidance: A Multilevel Model of Curiosity, Feedback Seeking, and Feedback Giving in Creative Work. *Academy of Management Journal*, *60*(6), 2051–2072. https://doi.org/10.5465/amj.2015.0247

Harrison, S. H., Sluss, D. M., & Ashforth, B. E. (2011). Curiosity adapted the cat: The role of trait curiosity in newcomer adaptation. *Journal of Applied Psychology*, *96*(1), 211–220. https://doi.org/10.1037/a0021647

Hu, S., Hsu, C., & Zhou, Z. (2021). Security Education, Training, and Awareness Programs: Literature Review. *Journal of Computer Information Systems*, *0*(0), 1–13. https://doi.org/10.1080/08874417.2021.1913671

Jeppesen, L. B., & Frederiksen, L. (2006). Why Do Users Contribute to Firm-Hosted User Communities? The Case of Computer-Controlled Music Instruments. *Organization Science*, *17*(1), 45–63. https://doi.org/10.1287/orsc.1050.0156

Jeraj, M., & Antoncic, B. (2013). A conceptualization of entrepreneurial curiosity and construct development: A multi-country empirical validation. *Creativity Research Journal*, *25*(4), 426–435.

Kam, H.-J., Ormond, D. K., Menard, P., & Crossler, R. E. (2022). That's interesting: An examination of interest theory and self-determination in organisational cybersecurity training. *Information Systems Journal*, *32*(4), 888–926.

Kashdan, T. B., Stiksma, M. C., Disabato, D. J., McKnight, P. E., Bekier, J., Kaji, J., & Lazarus, R. (2018). The five-dimensional curiosity scale: Capturing the bandwidth of curiosity and identifying four unique subgroups of curious people. *Journal of Research in Personality*, *73*, 130–149.

Kokkodis, M., Lappas, T., & Ransbotham, S. (2020). From Lurkers to Workers: Predicting Voluntary Contribution and Community Welfare. *Information Systems Research*, *31*(2), 607–626. https://doi.org/10.1287/isre.2019.0905

Koo, D.-M., & Ju, S.-H. (2010). The interactional effects of atmospherics and perceptual curiosity on emotions and online shopping intention. *Computers in Human Behavior*, *26*(3), 377–388.

Lee, J., & Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information Management & Computer Security*, *10*(2), 57–63. https://doi.org/10.1108/09685220210424104

Litman, J. (2005). Curiosity and the pleasures of learning: Wanting and liking new information. *Cognition & Emotion*, *19*(6), 793–814. https://doi.org/10.1080/02699930541000101

Litman, J. A., Collins, R. P., & Spielberger, C. D. (2005). The nature and measurement of sensory curiosity. *Personality and Individual Differences*, *39*(6), 1123–1133.

Litman, J. A., & Jimerson, T. L. (2004). The Measurement of Curiosity As a Feeling of Deprivation. *Journal of Personality Assessment*, *82*(2), 147–157. https://doi.org/10.1207/s15327752jpa8202_3

Litman, J. A., & Pezzo, M. V. (2007). Dimensionality of interpersonal curiosity. *Personality and Individual Differences*, *43*(6), 1448–1459.

Litman, J. A., & Spielberger, C. D. (2003). Measuring Epistemic Curiosity and Its Diversive and Specific Components. *Journal of Personality Assessment*, *80*(1), 75–86. https://doi.org/10.1207/S15327752JPA8001_16

Loewenstein, G. (1994). The Psychology of Curiosity: A Review and Reinterpretation. *Psychological Bulletin*, *116*(1), 75–98.

Lowry, P. B., Gaskin, J. E., Twyman, N. W., Hammer, B., & Roberts, T. L. (2013). Taking "Fun and Games" Seriously: Proposing the Hedonic-Motivation System Adoption Model. *Journal of the Association for Information Systems*, *14*(11), 617–671.

McElroy, J. C., Hendrickson, A. R., Townsend, A. M., & DeMarie, S. M. (2007). Dispositional factors in internet use: Personality versus cognitive style. *MIS Quarterly*, 809–820.

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. https://doi.org/10.1057/s41303-017-0058-x

Mussel, P. (2013). Introducing the construct curiosity for predicting job performance. *Journal of Organizational Behavior*, *34*(4), 453–472.

Muthén, L. K., & Muthén, B. O. (2017). *Mplus User's Guide* (Eighth Edition). Muthén & Muthén.

Reio, T. G., & Callahan, J. L. (2004). Affect, curiosity, and socialization-related learning: A path analysis of antecedents to job performance. *Journal of Business and Psychology*, *19*(1), 3–22.

Risko, E. F., Anderson, N. C., Lanthier, S., & Kingstone, A. (2012). Curious eyes: Individual differences in personality predict eye movement behavior in scene-viewing. *Cognition*, *122*(1), 86–90.

Schneider, A., Von Krogh, G., & Jäger, P. (2013). "What's coming next?" Epistemic curiosity and lurking behavior in online communities. *Computers in Human Behavior*, *29*(1), 293–303.

Silic, M., & Lowry, P. B. (2020). Using design-science based gamification to improve organizational security training and compliance. *Journal of Management Information Systems*, *37*(1), 129–161.

Sun, T., Schilpzand, P., & Liu, Y. (2022). Workplace Gossip: An Integrative Review of its Antecedents, Functions, and Consequences. *Journal of Organizational Behavior*, *fourthcoming*.

Tuten, T. L., & Bosnjak, M. (2001). Understanding differences in web usage: The role of need for cognition and the five factor model of personality. *Social Behavior and Personality: An International Journal*, *29*(4), 391–398.

Verizon Enterprise Solutions. (2021). *2021 Data Breach Investigations Report*.

Whitman, M. E., Townsend, A. M., & Alberts, R. J. (2001). Information systems security and the need for policy. In M. Khosrowpour (Ed.), *Information Security Management: Global Challenges in the New Millenium* (pp. 9–18). Idea Group Publishing.

Yi, C., Jiang, Z. (Jack), & Benbasat, I. (2015). Enticing and Engaging Consumers via Online Product Presentations: The Effects of Restricted Interaction Design. *Journal of Management Information Systems*, *31*(4), 213–242. https://doi.org/10.1080/07421222.2014.1001270

APPENDIX A

Measurement Scales

Perceptual Curiosity – Diversive (PC/D)

- Discover new places to go
- Travel to places/never been to
- Listen to new/unusual kinds of music
- Exploring my surroundings
- Trying different foods
- Visiting art galleries/museums

Perceptual Curiosity – Specific (PC/S)

- Smell something new/find out what
- Hear strange sound/find out what caused it
- See new fabric/touch and feel it
- Hear something/see what it is
- Hear musical instrument/like to see it
- See vocal group/different voice types

Epistemic Curiosity – Diversive (EC/D)

- Enjoy learning about subjects which are unfamiliar
- Fascinating to learn new information
- Enjoy exploring new ideas
- Learn something new/like to find out more
- Enjoy discussing abstract concepts

Epistemic Curiosity – Specific (EC/S)

- See a complicated piece of machinery/ask someone how it works
- New kind of arithmetic problem/enjoy imagining solutions
- Incomplete puzzle/try and imagine the final solution
- Interested in discovering how things work
- Riddle/interested in trying to solve it

Sensory Curiosity

- Hiking through a remote rain forest
- Going on a dog sledding trip
- Sailing around the world
- Riding a horse on a deserted beach
- Taking a voyage through a desert
- Camping in a remote wilderness
- Climbing a mountain I have never climbed
- Scuba diving
- Flying an airplane
- Traveling on a train like the Orient Express

Interpersonal/Empathic Curiosity – Curious about Emotions (IC/CE)

- Attend to non-verbal messages people send
- Observe facial expressions to figure out feelings
- Try to understand people's feelings
- Figure out what others are feeling by looking
- People open up to me about how they feel

Interpersonal/Empathic Curiosity – Spying and Prying (IC/SP)

- Think about interviewing others as a career
- Feel comfortable asking about private life
- Would make a good private detective
- Wish I could turn invisible to spy on people
- Think about being an investigative reporter

Interpersonal/Empathic Curiosity – Snooping (IC/Sn)

- Look at things in people's rooms
- Going into houses to see how people live
- Wonder what people's interests are
- Shuffle through things because intrigued
- Like to know what other people do

Five-Dimension Curiosity Scale (5DC)

Joyous exploration

- I view challenging situations as an opportunity to grow and learn.
- I am always looking for experiences that challenge how I think about myself and the world.
- I seek out situations where it is likely that I will have to think in depth about something.
- I enjoy learning about subjects that are unfamiliar to me.
- I find it fascinating to learn new information.

Deprivation sensitivity

- Thinking about solutions to difficult conceptual problems can keep me awake at night.
- I can spend hours on a single problem because I just can't rest without knowing the answer.
- I feel frustrated if I can't figure out the solution to a problem, so I work even harder to solve it.
- I work relentlessly at problems that I feel must be solved.
- It frustrates me not having all the information I need.

Stress Tolerance

- The smallest doubt can stop me from seeking out new experiences.
- I cannot handle the stress that comes from entering uncertain situations.
- I find it hard to explore new places when I lack confidence in my abilities.
- I cannot function well if I am unsure whether a new experience is safe.
- It is difficult to concentrate when there is a possibility that I will be taken by surprise.

Social curiosity

- I like to learn about the habits of others.
- I like finding out why people behave the way they do.
- When other people are having a conversation, I like to find out what it's about.
- When around other people, I like listening to their conversations.
- When people quarrel, I like to know what's going on.

Thrill seeking

- The anxiety of doing something new makes me feel excited and alive.
- Risk-taking is exciting to me.
- When I have free time, I want to do things that are a little scary.
- Creating an adventure as I go is much more appealing than a planned adventure.
- I prefer friends who are excitingly unpredictable.