

# **Curiosity, Learning, and Information Security in Organizations**

**Early stage paper**

**Yaojie Li**

University of New Orleans  
yli27@uno.edu

**Yu Zhao**

Lamar University  
yzhao2@lamar.edu

**Yuan Li**

University of Tennessee  
yli213@utk.edu

## **ABSTRACT**

Curiosity is not merely a “forbidden fruit” that triggers security threats and risks. It can be a potent catalyst for fostering diverse forms of security learning among organizational employees, thus establishing an intelligent and vigilant human firewall. In this study, we developed a curiosity-driven security learning model rooted in flourished psychological curiosity studies and educational literature. Our research reveals that security curiosity, driven by an individual’s trait curiosity, facilitates conceptual security learning, while the relationship between security curiosity and analytical security learning is fully mediated by security cognitive engagement. Our study illuminates the dynamics of curiosity-driven security learning in the workplace, underscoring the critical role of security cognitive engagement. Finally, we discuss directions for developing this work-in-progress paper and its potential contributions to advancing organizational and behavioral security research.

## ***Keywords***

Trait curiosity, security curiosity, intrinsic motivation, cognitive engagement, security learning, curiosity-driven learning, information security.

## **INTRODUCTION**

Employees are crucial to a contemporary organization's comprehensive security system. They represent the weakest link of the security chain due to their potential oversights and errors (Bulgurcu et al., 2010; Safa et al., 2016; Guo et al., 2011), while they can also form an extended human defense network against security threats when effectively educated and empowered (Dhillon et al., 2020; Puhakainen & Siponen, 2010). According to Gartner's report (2023), the information security and risk management market will increase from \$188.1 billion to \$288.5 billion between 2023 and 2027, with a compound annual growth rate of 11.0%. Acknowledging the importance of organizational information security, astute executives invest not only in security technologies but also in employee security education, training, and awareness (SETA) programs. Another Forbes (2023) survey indicated that 64% of U.S. companies have invested in employee security training nearly as much as they have in purchasing security solutions, services, and applications (62%). This balanced approach underscores the increasingly important role of employee preparedness in enhancing organizational information security.

While many organizations have initiated SETA programs, it is crucial to move beyond one-off training sessions that are often insufficient. These sessions, typically featuring generic and unengaging content, fail to address the diverse demands of employees in different security roles, responsibilities, and knowledge levels. Therefore, it is imperative to categorize security training and education based on specific learning needs while integrating active learning strategies into these programs.

In organizational and behavioral security literature, security policy compliance has been a dominant theme, which primarily focuses on various mechanisms designed to ensure the effectiveness of security policies and procedures. One prime example is SETA programs.

However, these programs often emphasize formal and mandatory training, education, and assessment, overlooking employees' potential to act as active players in learning and applying security countermeasures. Passive learning, resulting from rigid protocols, can not only be less effective but also lead to adverse effects, such as security stress, burnout, and fatigue (Cram et al., 2021; D'Arcy & Teh, 2019; Pham et al., 2019). Active learning, which requires learners' engagement in higher-order thinking, including analysis, synthesis, and evaluation (Bonwell & Eison, 1991, p. iii), offers a novel approach to designing organizational SETA programs. For active learning, curiosity serves as a critical catalyst (Kang et al., 2009; Lievens et al., 2022). Unlike a few security studies focused on the negative consequences of curiosity (Kuraku, 2022; Ormond et al., 2019), such as susceptibility to phishing clicks and unauthorized access, our research asserts that curiosity encourages employees to actively engage with security learning and practice. This engagement allows them to acquire and assimilate knowledge in ways that suit their learning objectives and styles. Far from being merely detrimental, employees' security curiosity not only fosters the efficient acquisition of security knowledge and skills but also promotes organizational security campaigns and discoveries.

Indeed, organizational and behavioral security research is progressing significantly, as demonstrated by the increased emphasis on human components over purely technological solutions and a pronounced transition from punitive, deterrent measures to employee protection-motivated actions. The research trends acknowledge the positive and proactive employees in bolstering organization information security. Also, it is worthwhile to explore security learning as part of employees' positive and proactive security behaviors. However, current literature in information systems scarcely examines the role of curiosity in security learning. While a myriad of studies investigated students' security skills learning in the classroom setting, there is a lack of

research on curiosity and security learning in the workplace. Further, few studies differentiate between conceptual security learning and in-depth security learning. Given the different cognitive demands of security learning levels, it is essential to explore how curiosity affects these levels. For example, fundamental security concepts like the CIA triad might be sparked by situational curiosity, whereas a deep comprehension of a man-in-the-middle attack in network security might demand more intrinsic motivation and cognitive engagement.

Acknowledging the research gaps in security learning at work and recognizing the importance of curiosity as a catalyst for promoting security learning, we draw upon the theories of curiosity and learning, particularly the information gap theory, to explore the role and impact of employees beyond often rigid compliance and passive learning dictated by potentially rigid and inefficient security frameworks. In essence, our research aims to address two key questions: *1) How does curiosity drive various levels of security learning in the workplace? And 2) What is the mediating role of security cognitive engagement – one's active participation in dealing with security problems – in the relationship between employees' security curiosity and different levels of security learning, ranging from fundamental, conceptual understanding to in-depth, analytical knowledge of organizational information security?*

This paper is structured as follows: First, we present a comprehensive review of curiosity literature and relevant theoretical background that informs our research. Then, we detail the development of our hypotheses and theoretical model. Following that, we explain our research method and discuss the results of the analysis. Finally, we conclude with a discussion of the theoretical and practical implications of our findings as well as potential avenues for future research.

## **THEORETICAL BACKGROUND**

Curiosity can be defined as the desire to acquire knowledge and experience, which drives individuals to explore, seek information, and learn (Berlyne, 1954; Lievens et al., 2022; Litman, 2005; Loewenstein, 1994). This concept has roots extending back to ancient Greek philosophers like Plato and Aristotle. Indeed, Aristotle started off his *Metaphysics* with the famous line that “all men by nature desire to know” (Inan, 2013, p.16), highlighting curiosity as a human’s innate nature to acquire knowledge. Modern curiosity research originated in psychology, where Berlyne (1954; 1960; 1966) laid much foundational work. In his work, Berlyne characterized curiosity as a transient, emotional-motivational state. Also, Berlyne (1954) distinguished between epistemic curiosity, which involves a preference for acquiring new intellectual knowledge, and perceptual curiosity, which is driven by a desire for novel sensory experiences that prompt visual and sensory exploration. Berlyne (1960) further elaborated curiosity theory by proposing three classes of variables that evoke curiosity: psychophysical (e.g., physical intensity), ecological (motivational significance and task relevance), and collative (e.g., novelty, complexity, uncertainty, and conflict). Later on, Naylor (1981) explored individual differences in the capacity of curiosity, developing the measures of trait curiosity. Building on these foundations, Spielberger and Starr (1994) argued that curiosity could manifest both as a transient state and a more enduring trait. Here, we consider “security curiosity” a specific form of epistemic and state curiosity that employees develop through their daily activities related to security. This type of curiosity is often temporary and situation-specific, arising from communications and interactions within organizations, such as conversing with colleagues about data breaches, dealing with phishing emails, and performing security-related tasks like password management and data protection. In

addition, we include employee trait curiosity as a crucial driver of their security curiosity in our examination of curiosity and security learning in organizations.

Berlyne's (1960) work highlighted how situational factors, such as novelty, ambiguity, complexity, and conflicts, can provoke "arousal," thus promoting individuals' engagement in exploratory and learning behaviors. Instead, Loewenstein's information gap theory (1994) considers curiosity as a cognitive process that arises when individuals perceive a discrepancy between their current knowledge and what they aspire to learn. Therefore, this perceived information gap stimulates a desire to bridge it, fueling curiosity-driven behavior. Loewenstein also delineated that curiosity increases with increasing awareness of this gap, reaches a peak, and then declines as the gap closes. Building on these ideas, Litman (2005; 2008) proposed the I/D model, which merges curiosity reduction and induction theories. Here, curiosity manifests as a pursuit of new knowledge expected to increase pleasurable feelings of situational interest, i.e., I-type curiosity. Meanwhile, curiosity can be a drive to alleviate unpleasant experiences of feeling deprived, i.e., D-type curiosity. In security scenarios, I-type curiosity may be sparked among employees who are eager to learn about Kevin Mitnick's hacking and consulting stories. Conversely, D-type curiosity can be triggered by an individual's realization of their limited understanding of how specific technologies, such as antivirus software and intrusion detection and prevention systems, protect their enterprise systems. To sum up, Litman's I/D model can be used to explain how curiosity can either seek information to enrich one's experience or mitigate security knowledge deficiencies.

Intriguingly, curiosity has gained attention in information security research, but it remains underexplored as a principal construct and appears in conceptual papers. It can be explained that information security is predominantly a rule-bound area that demands strict adherence to security

policies and procedures from employees. As a result, these policies' stringent and rigid implementation leaves minimal room for individuals to explore security threats and countermeasures on their own. More often, curiosity within this field is viewed as potentially risky, akin to a "forbidden fruit" or something that can "kill the cat," because it can result in detrimental behaviors, such as clicking on phishing emails, navigating risky websites, or accessing enterprise systems and data without authorization (Frauenstein & Flowerday, 2020; Kuraku, 2022; Moody et al., 2017; Ormond et al., 2019). Nevertheless, there is an increasing recognition of the duality of curiosity in the security setting, acknowledging its potential benefits alongside the risks (Menard et al., 2022; Kam et al., 2022; Safa & Von Solms, 2006; Silic & Lowry, 2020). Hence, the paradoxical nature of curiosity highlights the necessity to channel it constructively, maximizing its potential to bolster organizational information security.

As discussed earlier, it is crucial to distinguish between different levels of security learning in organizations. While a few studies have explored various approaches to security education grounded in behaviorism, cognitivism, and constructivism (Karjalainen & Siponen, 2011; Puhakainen & Siponen, 2010), there remains a deficiency in research specifically classifying security learning based on various cognitive engagement. Therefore, we turn to well-established educational frameworks, such as Bloom's taxonomy of knowledge (1956) and subsequent revisions (e.g., Krathwohl, 2002). According to Bloom's taxonomy, "remembering" refers to the fundamental level of retrieving specific information, "understanding" involves the comprehension of the meaning of the information, "applying" stands for one's ability to apply the information in new situations, "analyzing" means breaking down information into parts while exploring the structure and the relationship among them. Specifically, Krathwohl (2002) incorporated different types of knowledge – conceptual knowledge (i.e., concepts, theories, and relationships among

these essential elements) and procedural knowledge (i.e., how to do something, methods of inquiry, and criteria for applying algorithms, techniques, and methods) into the taxonomy, offering a better understanding of how these forms of knowledge are engaged across learning levels from basic to advanced and simple to complex. In addition, Craik and Lockhart's depth of processing framework (1972) complements the knowledge taxonomy by linking the durability of memory retention to the depth of processing. That is, when deeper semantic engagement leads to more durable memory traces, shallow processing focuses on superficial concepts, resulting in limited learning outcomes. Based on these learning principles, we propose a differentiation in security learning – *conceptual security learning* includes basic security models, concepts, and terminologies, whereas *analytical security learning* is developed from cognitive engagement and information processing on security threats and corresponding defense strategies and countermeasures.

## **HYPOTHESES DEVELOPMENT AND RESEARCH MODEL**

Naylor (1981, 172-173) pointed out that individual variations in the capacity for curiosity experiences suggest a trait formulation. It is presumed that individuals with higher levels of trait curiosity tend to explore and encounter a broader array of stimulating situations compared to those with lower levels of trait curiosity. That is, individuals with innate trait curiosity are more likely to discover new experiences and deal with new things in the workplace, including security threats, countermeasures, and best practices. Also, security itself is intriguing to employees because it is novel and unfamiliar to many non-technical employees, yet closely related to and often discussed in the workplace, sparking their curiosity about security. Therefore, employees are more likely to exhibit a greater inclination toward security curiosity than those less inclined to do so. Hence, we posit:



***Hypothesis 1: Trait curiosity is positively associated with security curiosity.***

According to Berlyne's arousal theory of curiosity (1960), individuals interested in organizational information security are motivated to explore and learn things about security threats, vulnerabilities, countermeasures, and defense strategies. By actively seeking out information and constructing knowledge on security, their curiosity can be satisfied, and relevant perceived uncertainties and complexities can be mitigated as well. Although there can be different levels of security learning, we believe the arousal-driven security curiosity can foster both conceptual security learning and analytical security learning, respectively. Therefore, we posit:

***Hypothesis 2a: Security curiosity is positively associated with conceptual security learning.***

***Hypothesis 2b: Security curiosity is positively associated with analytical security learning.***

According to Loewenstein's information gap theory (1994), curiosity-driven learning contains a critical cognitive engagement where individuals actively seek to address the discrepancy between their existing knowledge and the novel knowledge they aspire to learn. Hence, in addition to the "arousal" link between security curiosity and security learning, we propose that security engagement plays an important mediating role. Based on the insights from creative cognitive engagement (Zhang & Bartol, 2010), we argue that employees may initially acquire basic information about security due to arousal but subsequently engage in more complex cognitive processes, including problem identification, information search, and decoding, as well as the generation of ideas and solutions. Curiosity fosters fundamental security learning, such as basic security concepts and terminologies, usually within a limited timeframe. However, through sustained security cognitive engagement, employees are likely to enhance their conceptual learning and embark on in-depth analytical security learning. Therefore, we posit:

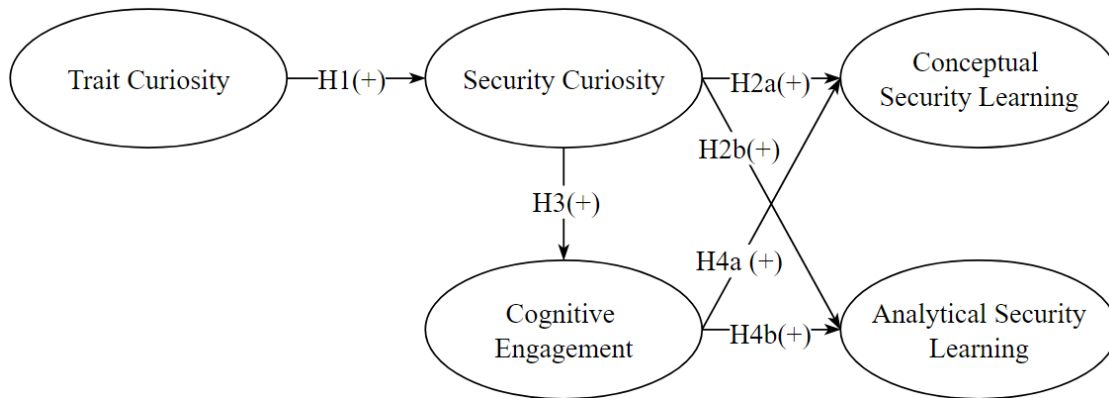
**Hypothesis 3:** *Security curiosity is positively associated with security cognitive engagement.*

As mentioned above, driven by curiosity, an individual is likely to engage in security cognitive activities such as problem identification, environmental scanning, information searching, solution generation and evaluation, and solution implementation (Simon, 1966; Zhang & Bartol, 2010). These cognitive activities are integral to effective security learning, as they enable employees not only to obtain fundamental security knowledge but also to proactively seek out and implement solutions that can better protect organization assets. Hence, we posit:

**Hypothesis 4a:** *Security cognitive engagement is positively associated with conceptual security learning.*

**Hypothesis 4b:** *Security cognitive engagement is positively associated with analytical security learning.*

As a result, the research model and hypotheses are demonstrated in Figure 1.



**Figure 1. Research Model of Curiosity and Security Learning**

## **RESEARCH METHOD**

To empirically evaluate our research model, we conducted an online survey. The survey instrument was developed from existing scales identified through a comprehensive literature review and focus group discussions. While most measurement items were adapted from previously validated constructs, we developed new measurements for “conceptual security learning” and “analytical security learning” due to the lack of existing scales. All measures were rated on a seven-point Likert scale, ranging from 1 (strongly disagree) to 7 (strongly agree). A panel of five domain-expert professors experienced in quantitative research validated all scales’ content validity. The appendix lists the measurement items and their respective sources.

Participants were recruited via the Qualtrics panel in the United States, yielding 530 completed responses. According to Cohen’s (1992) statistical power analysis, a sample size of at least 158 is recommended to achieve 80% statistical power for detecting  $R^2$  values of at least 0.1 with a 1% probability of error when a construct has a maximum of two arrows pointing to it. Therefore, our sample size of 530 was more than adequate for the analysis.

We conducted an exploratory factor analysis (EFA) to explore the factor structure of the two self-developed constructs. Through the factor analysis, we retained 7 out of 8 original measurement items for further use in the study. One measurement item was dropped from the “analytical security learning” construct due to a cross-loading issue. Table 1 shows the factor analysis results.

## **RESEARCH METHOD**

To empirically evaluate our research model, we conducted an online survey. The survey instrument was developed from existing scales identified through a comprehensive literature review and focus group discussions. While most measurement items were adapted from previously validated

constructs, we developed new measurements for “conceptual security learning” and “analytical security learning” due to the lack of existing scales. All measures were rated on a seven-point Likert scale, ranging from 1 (strongly disagree) to 7 (strongly agree). A panel of five domain-expert professors experienced in quantitative research validated all scales’ content validity. The appendix lists the measurement items and their respective sources.

Participants were recruited via the Qualtrics panel in the United States, yielding 530 completed responses. According to Cohen’s (1992) statistical power analysis, a sample size of at least 158 is recommended to achieve 80% statistical power for detecting  $R^2$  values of at least 0.1 with a 1% probability of error when a construct has a maximum of two arrows pointing to it. Therefore, our sample size of 530 was more than adequate for the analysis.

We conducted an exploratory factor analysis (EFA) to explore the factor structure of the two self-developed constructs. Through the factor analysis, we retained 7 out of 8 original measurement items for further use in the study. One measurement item was dropped from the “analytical security learning” construct due to a cross-loading issue. Table 1 shows the factor analysis results.

Variables	Factor 1	Factor 2
C_KNOW1	0.688	
C_KNOW2	0.827	
C_KNOW3	0.897	
C_KNOW4	0.930	
A_KNOW2		0.749
A_KNOW3		0.900
A_KNOW4		0.750

C\_KNOW: Conceptual Security Learning, A\_KNOW: Analytical Security Learning

**Table 1. Factor Analysis Results of Security Learning Constructs**

To mitigate common method bias (CMB), we employed procedural remedies during the survey design. Specifically, we separated the survey questions for exogenous constructs from those for

endogenous constructs to avoid linear ordering (Podsakoff et al., 2003). Additionally, we conducted Harman's single-factor test to assess CMB. According to Podsakoff et al. (2003), significant CMB is indicated if either a single factor emerges from exploratory factor analysis (unrotated) or one general factor accounts for most of the covariance among measures (p. 889). Our results showed that multiple factors emerged to explain the variance, and no single factor accounted for more than half of the covariance among the measures, indicating that CMB was not a significant issue in our study.

To address multicollinearity concerns, we examined the latent variables' variance inflation factor (VIF). The highest VIF score was 3.848, well below the threshold value of 5 (Hair et al., 2021), indicating no collinearity issues.

## **Measurement Validation**

We thoroughly evaluated the measurement models using various criteria, including indicator reliability, internal consistency (measured by both composite reliability and Cronbach's alpha), convergent validity (assessed by average variance extracted, AVE), and discriminant validity. All latent variables in our research models were measured using reflective constructs. For these evaluations, we utilized structural equation modeling with partial least squares (PLS). The findings showed robust consistency and accuracy across all measures.

The outer loadings for most items surpassed the recommended threshold of 0.7 (Hair et al., 2021). Notably, even though one measurement item of the construct "trait curiosity" had a loading of 0.673 and one item of the construct "analytical security learning" had a loading of 0.609, these values were still deemed acceptable and contributed valuable insights. Following the recommendation to carefully assess the impact of removing indicators with loadings between 0.40

and 0.70 (Hair et al., 2021, p. 116), we found that retaining these items maintained the integrity of our measures. Their inclusion ensured that the overall composite reliability remained robust, and our findings were comprehensive.

According to the PLS confirmatory factor analysis, each indicator exhibited stronger loadings on its intended construct than on any other. Besides these promising outcomes regarding cross-loadings, discriminant validity was confirmed using the heterotrait-monotrait ratio (HTMT) of correlations, following the guidelines by Henseler et al. (2015). According to their criteria, an HTMT value below 0.90 reliably indicates a clear distinction between the two factors. As shown in Table 2, all HTMT ratios for factor pairs in both models were below 0.9, affirming robust discriminant validity across all measures.

Construct	AKNOW	ENGA	CKNOW	SCURI	TCURI
AKNOW					
ENGA	0.524				
CKNOW	0.706	0.823			
SCURI	0.491	0.860	0.780		
TCURI	0.596	0.682	0.679	0.671	

CKNOW: Conceptual Security Learning, AKNOW: Analytical Security Learning, ENGA: Security Cognitive Engagement, TCURI: Trait Curiosity, SCURI: Security Curiosity

**Table 2. HTMT Ratio Criterion Test**

Table 3 provides a comprehensive summary of the measurement models' outcomes. For all constructs, composite reliability and Cronbach's alpha values surpass 0.708, indicating strong internal consistency reliability. Additionally, each construct achieves an AVE value of 0.5 or higher, affirming robust convergent validity. Furthermore, the square root of AVE for each construct exceeds its highest correlation with any other construct, underscoring solid discriminant

validity. These outcomes underscore the reliability and validity of our measurement methodology, ensuring the credibility of our findings.

	<b>C<math>\alpha</math></b>	<b>CR</b>	<b>AVE</b>	<b>CKNOW</b>	<b>AKNOW</b>	<b>ENG</b>	<b>TCURI</b>	<b>SCURI</b>
						<b>A</b>		
CKNOW	0.916	0.917	0.734	0.857				
AKNOW	0.852	0.859	0.676	0.703	0.822			
ENG	0.960	0.960	0.706	0.823	0.529	0.840		
TCURI	0.895	0.895	0.550	0.679	0.594	0.682	0.742	
SCURI	0.963	0.964	0.728	0.779	0.496	0.860	0.670	0.853

CKNOW: Conceptual Security Learning, AKNOW: Analytical Security Learning, ENG: Security Cognitive Engagement, TCURI: Trait Curiosity, SCURI: Security Curiosity, C $\alpha$ : Cronbach's Alpha, CR: Composite Reliability, AVE: Average variance extracted

**Table 3. Construct Correlation, Reliability, and Validity**

## Testing the Structural Model

In our structural model testing, we incorporated several control variables into the PLS regression analysis for each construct: security curiosity, cognitive engagement, conceptual security learning, and analytical security learning. Table 4 illustrates several findings regarding the effects of control variables. Age positively affects security curiosity, with older individuals displaying higher levels of interest. Gender differences are also notable: females excel in analytical security learning, whereas males show greater curiosity about security. Additionally, IT proficiency is associated with increased cognitive engagement and security curiosity. Furthermore, work experience influences these traits as well. Individuals with more work experience tend to perform better in analytical security learning but exhibit lower levels of cognitive engagement and curiosity about security. Interestingly, education does not significantly impact any of the four constructs examined.

Control Variables	CKNOW	AKNOW	ENGA	SCURI
Age	0.029	-0.110	0.019	0.105*
Education	-0.029	-0.034	0.022	-0.058
Gender	-0.021	0.130**	-0.013	-0.139***
IT proficiency	0.042	0.017	0.114**	0.286***
Work experience	-0.046	0.21**	-0.122**	-0.158**

\* t-statistic > 1.96, \*\* t-statistic > 2.57, \*\*\* t-statistic > 3.29, CKNOW: Conceptual Security Learning, AKNOW: Analytical Security Learning, ENGA: Security Cognitive Engagement, SCURI: Security Curiosity

**Table 4. Effects of Control Variables**

## Hypothesis Testing

We analyzed the magnitude and significance of the path coefficients, representing the hypothesized relationships among the constructs, to evaluate the structural models. We also assessed the commonly used coefficient of determination ( $R^2$  value) for the exogenous constructs on the endogenous constructs.

After executing the PLS-SEM algorithm, we obtained estimated values for the path coefficients and  $R^2$ . Hair et al. (2021) noted that the  $R^2$  value measures the model's predictive accuracy and indicates the explained variance of the endogenous constructs within the structural model. Additionally, we used bootstrapping to estimate t-values and determine the significance of these relationships.

The research model explained 69.7 percent of the variance in conceptual security learning ( $R^2 = 0.697$ ), 28.6 percent of the variance in analytical security learning ( $R^2 = 0.286$ ), 74 percent of the variance in cognitive engagement ( $R^2 = 0.74$ ), and 44.8 percent of the variance in security curiosity ( $R^2 = 0.448$ ).

We conducted a bootstrapping test using SmartPLS 3 to test the hypotheses. Compared to the traditional approach by Baron and Kenny (1986) for assessing mediation effects, SmartPLS is

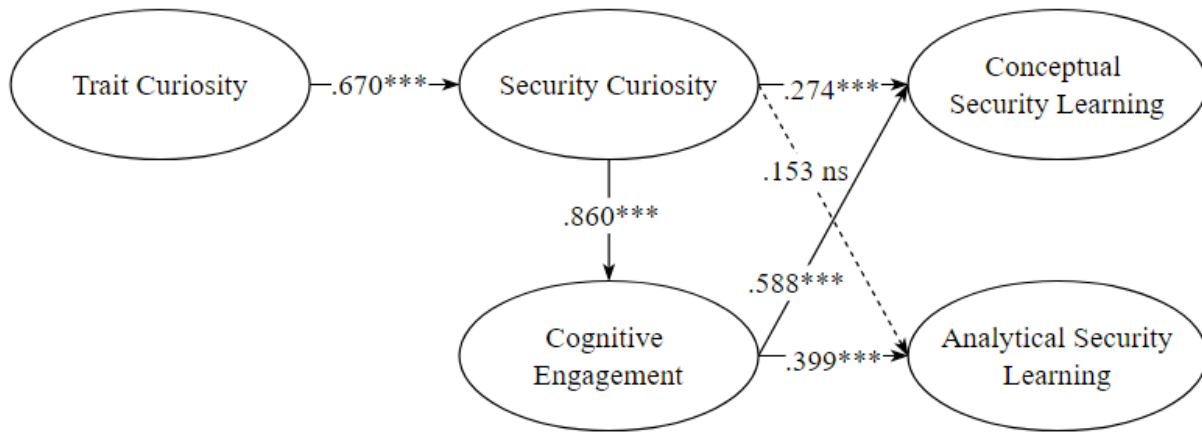


recognized as a more robust method. As discussed by Wang and colleagues (2023), this method specifically addresses competitive mediation and indirect-only mediation. Our findings are summarized as follows with 5,000 bootstrapping samples.

Except for Hypothesis 2b, the empirical results supported all other hypotheses and achieved statistical significance at the 0.01 level. Regarding Hypothesis 2b (H2b), which posits that security curiosity is positively related to analytical security learning, the results reveal that the direct effect is not significant ( $\beta = 0.153$ ,  $p = 0.166$ ). Thus, H2b is not supported. However, the mediating effect of cognitive engagement on the relationship between security curiosity and analytical security learning is significant, indicated by a specific indirect effect of 0.343 ( $p < 0.001$ ). The significance of the indirect effects combined with the non-significance of the direct effect indicates that cognitive engagement exhibits full mediation, or indirect-only mediation, as outlined by Zhao et al. (2010). Table 5 shows the parameters assessed in the structural models.

Hypothesized Path	Coeff	T Stat	P	Results
H1: Trait curiosity $\rightarrow$ Security curiosity	0.670	16.737	0.000	significant
H2(a): Security curiosity $\rightarrow$ Conceptual security learning	0.274	2.912	0.004	significant
H2(b): Security curiosity $\rightarrow$ Analytical security learning	0.153	1.385	0.166	insignificant
H3: Security curiosity $\rightarrow$ Security cognitive engagement	0.860	30.532	0.000	significant
H4(a): Cognitive engagement $\rightarrow$ Conceptual security learning	0.588	6.149	0.000	significant
H4(b): Cognitive engagement $\rightarrow$ Analytical security learning	0.399	3.700	0.000	significant

**Table 5. Structural Parameter Estimates**



Note: \*\*\* $p \leq 0.001$ , ns = insignificant

**Figure 2. PLS-SEM Analysis Results**

## DISCUSSION

In this working paper, we unveil several critical constructs and their relationships that have received limited attention in previous behavioral information security research, including security learning, security cognitive engagement, and security learning. Our exploratory study reveals significant relationships between security curiosity, driven by trait curiosity, and security cognitive engagement, which in turn facilitates security learning. While curiosity stimulates conceptual security learning, fostering analytical security learning requires deeper cognitive engagement like problem identification, information search, and idea and solution generation. As a result, security cognitive engagement exhibits a full mediation effect on the relationship between security curiosity and analytical security learning.

In addition to addressing the gap in security curiosity research, our study sheds light on the processes through which employees engage in acquiring security knowledge, particularly concerning different security learning objectives. Moving forward, we plan to incorporate various antecedents to security curiosity, such as novelty, complexity, and uncertainty of security

phenomena and problems, and explore extrinsic motivation, such as organizational rewards, in promoting employees' security learning. Furthermore, we aim to conduct comprehensive mediation and moderation tests to uncover nuanced relationships among employees' curiosity, security cognitive engagement, and security learning in organizational settings.

## References and Citations

### REFERENCES

- Baron, R. M., & Kenny, D. A. 1986. "The moderator-mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations," *Journal of Personality and Social Psychology* (51:6), pp. 1173-1182.
- Berlyne, D. E. 1954. "A theory of human curiosity," *British Journal of Psychology* (45:3), pp. 180-191.
- Berlyne, D. E. 1960. *Conflict, Arousal, and Curiosity*, New York, NY: McGraw-Hill Book Company.
- Berlyne, D. E. 1966. "Curiosity and Exploration: Animals spend much of their time seeking stimuli whose significance raises problems for psychology," *Science* (153:3731), pp. 25-33.
- Bloom, B. S. (Ed.). 1956. *Taxonomy of Educational Objectives: The Cognitive Domain*, New York, NY: Logman.
- Bonwell, C. C., & Eison, J. A. 1991. *Active Learning: Creating Excitement in the Classroom*, 1991 *ASHE-ERIC Higher Education Reports*, Washington, DC: ERIC Clearinghouse on Higher Education, The George Washington University.
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. 2010. "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," *MIS Quarterly* (34:3), pp. 523-548.
- Craik, F. I., & Lockhart, R. S. 1972. "Levels of processing: A framework for memory research," *Journal of Verbal Learning and Verbal Behavior* (11:6), pp. 671-684.
- Cohen, J. 1992. "Statistical power analysis," *Current Directions in Psychological Science* (1:3), pp. 98-101.
- Cram, W. A., Proudfoot, J. G., & D'Arcy, J. 2021. "When enough is enough: Investigating the antecedents and consequences of information security fatigue," *Information Systems Journal* (31:4), pp. 521-549.
- D'Arcy, J., & Teh, P. L. 2019. "Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization," *Information & Management* (56:7), 103151.
- Dhillon, G., Abdul Talib, Y. Y., & Picoto, W. N. 2020. "The mediating role of psychological empowerment in information security compliance intentions," *Journal of the Association for Information Systems* (21:1), pp. 152-174.
- Forbes. 2023. "Cybersecurity Investment Trends in the U.S.," Available from: <https://www.forbes.com/sites/forbestechcouncil/2023/08/01/cybersecurity-investment-trends-in-the-us/>.

- Frauenstein, E. D., & Flowerday, S. 2020. "Susceptibility to phishing on social network sites: A personality information processing model," *Computers & Security* (94), 101862.
- Gartner. 2023. "Forecast: Information Security and Risk Management, Worldwide, 2021-2027, 2Q23 Update," Available from: <https://www.gartner.com/guest/purchase/registration?resId=4488199>.
- Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. 2011. "Understanding nonmalicious security violations in the workplace: A composite behavior model," *Journal of Management Information Systems* (28:2), pp. 203-236.
- Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. 2021. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)* (3rd ed.), Thousand Oaks, CA: SAGE Publications, Inc. (US).
- Hart, S., Margheri, A., Paci, F., & Sassone, V. 2020. "Riskio: A serious game for cyber security awareness and education," *Computers & Security* (95), 101827.
- Henseler, J., Ringle, C. M., & Sarstedt, M. 2015. "A new criterion for assessing discriminant validity in variance-based structural equation modeling," *Journal of the Academy of Marketing Science* (43), pp. 115-135.
- Inan, I. 2013. *The Philosophy of Curiosity*, London, UK: Routledge.
- 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), pp. 888-926.
- Kang, M. J., Hsu, M., Krajbich, I. M., Loewenstein, G., McClure, S. M., Wang, J. T. Y., & Camerer, C. F. 2009. "The wick in the candle of learning: Epistemic curiosity activates reward circuitry and enhances memory," *Psychological Science*, (20:8), pp. 963-973.
- Kashdan, T. B., Gallagher, M. W., Silvia, P. J., Winterstein, B. P., Breen, W. E., Terhar, D., & Steger, M. F. 2009. "The curiosity and exploration inventory-II: Development, factor structure, and psychometrics," *Journal of Research in Personality* (43:6), pp. 987-998.
- Krathwohl, D. R. 2002. "A revision of Bloom's taxonomy: An overview," *Theory into Practice* (41:4), pp. 212-218.
- Kuraku, S. 2022. "Curiosity Clicks: The Need for Security Awareness," Doctoral dissertation, University of the Cumberland.
- Lievens, F., Harrison, S. H., Mussel, P., & Litman, J. A. 2022. "Killing the cat? A review of curiosity at work," *Academy of Management Annals* (16:1), pp. 179-216.
- Litman, J. 2005. "Curiosity and the pleasures of learning: Wanting and liking new information," *Cognition and Emotion* (19:6), pp. 793-814.
- Litman, J. A. 2008. "Interest and deprivation factors of epistemic curiosity," *Personality and Individual Differences* (44:7), pp. 1585-1595.
- Loewenstein, G. 1994. "The psychology of curiosity: A review and reinterpretation," *Psychological Bulletin* (116:1), pp. 75-98.
- Menard, P., Kam, H. J., Ormond, D. K., & Crossler, R. E. 2022. "Curiosity vs. Curiosity: Striking the Balance between Positive and Negative Outcomes in SETA Programs and Phishing Campaigns," In *Proceedings of the 2022 IFIP 8.11/11.13 Dewald Roode Information Security Research Workshop*, Denver, CO, USA.
- Mussel, P. 2013. "Introducing the construct curiosity for predicting job performance," *Journal of Organizational Behavior* (34:4), pp. 453-472.
- Naylor, F. D. 1981. "A state-trait curiosity inventory," *Australian Psychologist* (16:2), pp. 172-183.

- Ormond, D., Kam, H. J., & Menard, P. 2019. "Eating the Forbidden Fruit: Human Curiosity Entices Data Breaches," In *Proceedings of the Americas Conference for Information Systems, Cancun, Mexico*.
- Pham, H. C., Brennan, L., & Furnell, S. 2019. "Information security burnout: Identification of sources and mitigating factors from security demands and resources," *Journal of Information Security and Applications* (46), pp. 96-107.
- Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. 2003. "Common method biases in behavioral research: A critical review of the literature and recommended remedies," *Journal of Applied Psychology* (88:5), pp. 879-903.
- Puhakainen, P., & Siponen, M. 2010. "Improving employees' compliance through information systems security training: An action research study," *MIS Quarterly* (34:4), pp. 757-778.
- Safa, N. S., & Von Solms, R. 2016. "An information security knowledge sharing model in organizations," *Computers in Human Behavior* (57), pp. 442-451.
- Safa, N. S., Von Solms, R., & Furnell, S. 2016. "Information security policy compliance model in organizations," *Computers & Security* (56), pp. 70-82.
- 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), pp. 129-161.
- Simon, H. A. 1966. "Scientific discovery and the psychology of problem solving," In R. G. Colodny (Ed.), *Mind and cosmos: Essays in contemporary science and philosophy*, pp. 22-40.
- Spielberger, C. D., & Starr, L. M. 2012. "Curiosity and exploratory behavior," In *Motivation: Theory and Research*, pp. 221-243, New York, NY: Routledge.
- Wang, J., Dong, M., Yang, Z., & Li, Y. 2023. "Passing the torch: How parental privacy concerns affect adolescent self-disclosure on social networking sites," *MIS Quarterly*, (47:4), pp. 1585-1614.
- Zhang, X., & Bartol, K. M. 2010. "Linking empowering leadership and employee creativity: The influence of psychological empowerment, intrinsic motivation, and creative process engagement," *Academy of Management Journal*, (53:1), pp. 107-128.
- Zhao, X., Lynch, J., & Chen, Q. 2010. "Reconsidering Baron and Kenny: Myths and truths about mediation analysis," *Journal of Consumer Research*, 37:2, pp. 197-206.

**Appendix. Constructs and Measurement Items**

<b>Construct</b>	<b>Measurement Items</b>
Trait Curiosity (Adapted from Kashdan et al., 2009) “TCURI”	<ol style="list-style-type: none"> <li>1. I actively seek as much information as I can in new situations.</li> <li>2. I am the type of person who really enjoys the uncertainty of everyday life. *</li> <li>3. I am at my best when doing something that is complex or challenging.</li> <li>4. Everywhere I go, I am out looking for new things or experiences.</li> <li>5. I view challenging situations as an opportunity to grow and learn.</li> <li>6. I like to do things that are a little frightening. *</li> <li>7. I am always looking for experiences that challenge how I think about myself and the world.</li> <li>8. I prefer jobs that are excitingly unpredictable.</li> <li>9. I frequently seek out opportunities to challenge myself and grow as a person.</li> <li>10. I am the kind of person who embraces unfamiliar people, events, and places. *</li> </ol>
Security Curiosity (Adapted from Mussel et al., 2012) “SCURI”	<ol style="list-style-type: none"> <li>1. I am interested in how my contribution impacts organizational information security.</li> <li>2. I enjoy developing new ways to protect organizational information assets.</li> <li>3. Besides security practice, I’m also interested in the underlying security theories.</li> <li>4. When confronted with complex security problems, I like to look for new solutions.</li> <li>5. I enjoy pondering and thinking about information security.</li> <li>6. I am eager to learn about information security.</li> <li>7. I keep thinking about an information security problem until I solve it.</li> <li>8. I challenge already existing security theories and methods critically.</li> <li>9. I carry on seeking information until I can understand complex security issues.</li> <li>10. I try to improve the security process by making innovative suggestions.</li> </ol>
Cognitive Engagement (Adapted from Zhang & Bartol, 2010) “ENGA”	<ol style="list-style-type: none"> <li>1. I spent considerable time trying to understand the nature of the security problem.</li> <li>2. I think about the security problem from multiple perspectives.</li> <li>3. I decompose a difficult security problem/assignment into parts to obtain a greater understanding.</li> <li>4. I consult a wide variety of security information.</li> <li>5. I search for security information from multiple sources (e.g., personal memories, others’ experiences, documentation, the Internet, etc.)</li> <li>6. I retain much detailed security information in my area of expertise for future use.</li> <li>7. I look for connections with security solutions used in seemingly diverse areas.</li> <li>8. I generate a significant number of alternatives to address security problems.</li> <li>9. I try to devise potential solutions that move away from established ways of information security.</li> </ol>

---

		10. I spend considerable time searching for information that helps to generate ideas about information security.
Conceptual Learning (self-developed) “CKNOW”	Security	<ol style="list-style-type: none"> <li>1. I want to understand basic security terminology and concepts.</li> <li>2. I want to understand fundamental security theories and models like the triad of the CIA (confidentiality, Integrity, Availability).</li> <li>3. I want to study the main types of information assets, threats, and vulnerabilities.</li> <li>4. I want to understand the security structure and hierarchy in the company.</li> </ol>
Analytical Learning (self-developed) “AKNOW”	Security	<ol style="list-style-type: none"> <li>1. I want to know how to apply security knowledge and skills in the workplace. *</li> <li>2. I want to know how to comply with security policies and procedures.</li> <li>3. I want to know how to address security problems appropriately.</li> <li>4. I want to know how to avoid security threats.</li> </ol>

---

\* Item dropped because of low factor or cross loading