ISSN: 2473-4901
v12 n6943

Experiential and Dispositional Drivers of Phishing Susceptibility: A Cross-Nation Replication-Plus-Extension Study Fifteen Years Later

Wei Xie
xiew1@appstate.edu
Appalachian State University
Boone, NC, 28608, USA

Xin Deng
dengxin@hutb.edu.cn
Hunan University of Technology and Business
Changsha, Hunan, China

Abstract

Information Systems (IS) scholarship emphasizes systematic replication to strengthen theory by testing the reliability and boundary conditions of prior findings. Phishing remains the most common cyberattack entry point, and human susceptibility remains a critical vulnerability. Guided by the Replication plus Extension framework, this study replicates and extends Wright and Marett's influential model of phishing susceptibility, originally developed under markedly different socio-technical conditions 15 years ago. Using a *longitudinal field experiment* and simulated phishing emails *targeting undergraduates in China and the United States*, this study assesses the original model's robustness in a contemporary setting. Additionally, it extends the model by addressing the originally recognized limitations and investigating new factors that may have contributed to the high susceptibility rate observed in the original study. Specifically, this study reconceptualizes risk as a dispositional trait, conceptualizes and incorporates authority compliance as a key mechanism, and analyzes response latency as a behavioral predictor. This is a study in progress. The findings are expected to refine the understanding of phishing susceptibility and advance theory development in this domain.

Keywords: Phishing susceptibility, replication and extension, social influence theory, risk propensity, authority, cultural dimensions theory

Experiential and Dispositional Drivers of Phishing Susceptibility: A Cross-Nation Replication-Plus-Extension Study Fifteen Years Later

Wei Xie and Xin Deng

1. INTRODUCTION

Phishing remains the number one crime type reported by the Federal Bureau of Investigation's (2026) Internet Crime Report. Despite advances in technical defenses, such as email filtering, multifactor authentication, and AI-driven detection tools, attackers continue to succeed by exploiting human decision-making processes. For example, people continue to be vulnerable to email phishing attacks, with a phishing simulation clicking rate close to 33% for untrained employees, and 5% for trained teams (Madhurendra, 2026); and approximately one in ten people had been found to click on URLs or to open attachments during internal phishing tests (Verizon, 2024). Humans continually fall prey to phishing emails and remain a weak link in security, raising questions about whether we possess innate characteristics that predispose us to phishing susceptibility and whether greater experience with technology and cybersecurity training can enhance our resilience to phishing.

To accumulate evidence that strengthens and advances theory, replication studies that test prior findings across diverse contexts are essential. Foundational academic reviews call for systematic replication practices to evaluate the reliability and boundary conditions of scientific claims (Dennis & Valacich, 2015; Wright & Sweeney, 2016; Shrout & Rodgers, 2018; Singh et al., 2003; Berthon et al., 2002). Among behavioral investigations of phishing susceptibility, Wright and Marett (2010) offered one of the earliest and most influential empirical models, demonstrating that experiential factors, such as computer self-efficacy, Web experience, and security knowledge, played a stronger role in phishing susceptibility than dispositional traits. Their study remains one of the most cited behavioral examinations of phishing deception and serves as a theoretical foundation for subsequent research.

However, the socio-technical environment (Baxter & Sommerville, 2011) in which phishing occurs has evolved substantially over the past 15 years. Increased security controls, standardized security training, more sophisticated attack strategies, and heightened public awareness of cyber threats may have changed how experiential and dispositional factors influence phishing susceptibility. If experiential knowledge has become more widespread, its explanatory power may diminish; alternatively, dispositional characteristics may now play a stronger role in differentiating vulnerability. Furthermore, cultural nuances may shape how people perceive and respond to phishing susceptibility. Despite the growth of behavioral phishing research, empirical findings have not converged on which factors reliably predict susceptibility (Vishwanath et al., 2011; Ribeiro et al., 2024). This lack of convergence underscores the need to reassess foundational models in contemporary conditions to advance the maturation of theories of phishing susceptibility. Accordingly, this study builds upon Wright and Marett (2010) to ask the following research questions:

1. Do the effects of original dispositional and experiential factors hold when the same procedures are applied to a different contemporary context?
2. Do additional dispositional factors yield significant explanatory power beyond the original model?
3. Are there differences between Chinese and Americans in responding to phishing?

This replication study adopts a replication-plus-extension framework (Berthon et al., 2002). First, the study replicates the original longitudinal procedures as closely as feasible. Then, the study conceptually extends the model to address limitations identified by Wright and Marett (2010) by testing two new dispositional factors of risk propensity and authority compliance, and incorporates cultural boundaries. By doing so, the study evaluates the robustness of foundational findings while advancing contemporary phishing theory.

2. THEORETICAL BACKGROUND AND ORIGINAL THEORY

Replication is widely recognized as foundational to scientific progress because it transforms tentative

empirical findings into cumulative knowledge. As Berthon et al. (2002) argue, replication is the mechanism through which research moves from belief or opinion ("doxa") to accepted knowledge ("episteme"), serving as a verification leg in the scientific process (Berthon et al., 2002). Without verification, findings remain unstable and potentially context-bound. Similarly, Dennis and Valacich's (2015) Replication Manifesto emphasizes that independent replication increases confidence in findings and enables scientific consensus to emerge within Information Systems (IS) research. They argue that IS has lagged behind the physical sciences in embracing replication and call for a cultural shift that values replication as a normal stage of disciplinary maturation. Beyond IS, Singh et al. (2003) make a strong case that replication is essential for reliability, validity, and rigorous theory development, especially in emerging or pre-paradigmatic fields. They further note that replication protects against uncritical acceptance of empirical results and enhances generalizability across contexts. Wright and Sweeney (2016) reinforce this concern within organizational research, documenting extremely low replication rates (1–2%) in top journals and uses two studies to argue that replication and extension designs would provide a viable path toward cumulative scientific understanding. Taken together, these calls converge on a shared concern: knowledge accumulation requires systematic replication, yet replication remains under-institutionalized.

Dennis and Valacich (2015) distinguish among Exact, Methodological, and Conceptual replications. Conceptual replication tests the same research questions while altering measures, treatments, analyses, or context. Singh et al. (2003) likewise distinguish among forms of replication, introducing the concept of good-enough extensions—studies designed to approximate the original as closely as possible in order to strengthen overall rigor and generalizability in social science research—while acknowledging that exact duplication is rarely feasible. Berthon et al. (2002) provide the most comprehensive theoretical scaffold. They conceptualize replication, extension, and generation as distinct dimensions of a broader "research space" framework. In their framework, Replication verifies existing knowledge claims, Extension generalizes or refines theory across contexts, and Generation develops novel theoretical contributions. Crucially, Berthon et al. (2002) argue that replication and extension are not inferior to generation; rather, they are complementary strategies necessary for theory consolidation. These prior works directly support this study's replication-and-extension design as a legitimate and theoretically grounded research strategy.

Two 2025 publications in the Communications of the Association for Information Systems (CAIS) offer concrete examples of replication-with-extension contributions. Michel Costa de Brito et al. (2025) conduct a conceptual replication of Zaitsev et al. (2020), addressing the same research questions while varying the organizational context to verify the robustness of the original theory. Similarly, Yuan et al. (2025) replicate Chau et al.'s (2020) methodological approach and show that contextual factors influence machine learning model selection. Consistent with Dennis and Valacich (2015) and Singh et al. (2003), both studies are characterized as replications with extensions, broadening and deepening insights into domain understanding.

Wright and Marett (2010) grounded their research on Phishing Susceptibility in Interpersonal Deception Theory (IDT), adapting it to the asynchronous, non-interactive nature of phishing emails. Unlike face-to-face deception, phishing emails rely on a single, carefully crafted "bait" message, often without iterative feedback or relational context. Their model categorized antecedents of phishing susceptibility into two groups. First, the experiential factors include Computer Self-Efficacy (CSE), Web Experience, and Internet Security Knowledge. Second, dispositional factors include Disposition to Trust, Risk Belief, and Suspicion of Humanity. The dependent variable, deception success, was a binary indicator of whether participants disclosed sensitive information in response to a phishing email. The original findings revealed strong negative effects of experiential factors on deception success, while dispositional trust and perceived risk were not significant predictors.

3. METHODOLOGY

Drawing on the Replication plus Extension (Berthon et al., 2002), this study adopts a two-phase design. In Phase One, this study closely replicates the original investigation. The replication introduces a single degree of freedom to the original study - context-only extension, due to a changed study context 15 years later - and focuses on verifying and generalizing the theory. In Phase Two, this study conceptually extends it by addressing its identified limitations. The extension adds two degrees of freedom by introducing new constructs alongside the contextual changes – theory and context extension,

broadening the theoretical scope of the original model (Berthon et al., 2002). Furthermore, we conduct experiments across the US and China to identify cultural nuances in how individuals perceive and respond to phishing, particularly how authority mechanisms operate within a compliance environment.

3.1 Phase one: Replication of the Experiment in a Contemporary Context

The replication phase closely follows the deception procedures of Wright and Marett (2010), including: (1) a semester-long field experiment; (2) issuance of a "Secure Submission Code" (SSC), signing of a fake non-disclosure agreement (NDA) at the outset, and administration of a pre-experiment survey; (3) repeated SSC use as reinforcement, along with ongoing security awareness training throughout the semester; (4) a simulated phishing email sent by IT requesting SSC disclosure at the conclusion; (5) a post-experiment survey and debriefing; and (6) binary coding of deception success. The original six hypotheses remain unchanged, except for updating "web experience" to a broader "online experience" to align with the current user experience (Table 2). We also made procedural updates to align with the current technological context while preserving the original logic and structure. For example, we replaced the paper NDA with a digital version, now standard practice, to reduce students' questions and suspicions. Additionally, unlike the original study, which coincided with a real phishing incident, this replication was conducted without concurrent security breaches, thereby eliminating an undue external influence present in the original study.

3.2 Phase two: Theory and Model Extensions

Phase two extends the theory and model to address limitations explicitly noted in the original study.

Extension 1: Risk as a Dispositional Trait

Wright and Marett (2010) acknowledged that their perceived risk measure of information sharing online reflected a situational belief rather than a stable disposition. This study introduces the concept of risk propensity to reflect the authors' intention to test dispositional factors. In the context of phishing emails, risk propensity is a theoretically relevant individual difference. Phishing success often hinges on whether users will tolerate uncertainty and potential loss long enough to click, reply, open attachments, or disclose information. Individuals with higher risk propensity are generally more willing to engage in behaviors with uncertain outcomes and to discount potential negative consequences, which can translate into a greater willingness to "see what it is" when confronted with ambiguous or enticing email cues. IS phishing research has explicitly examined individual susceptibility factors and includes risk propensity as a human-factor predictor of phishing vulnerability (Moody et al., 2017). Consistent with domain-based conceptualizations of risk propensity (i.e., stable tendencies to take risks across domains), a higher risk propensity should therefore increase the likelihood of engaging with phishing emails and reduce cautious verification behavior (Nicholson et al., 2005). We hypothesize:

H7: Higher risk tolerance increases the likelihood that a person will be deceived by a phishing e-mail

Extension 2: Authority Compliance in Message Sender

Phishing frequently exploits legitimate-seeming authority (e.g., IT departments, universities). Wright and Marett (2010) questioned whether their higher phishing response rate was due to the absence of an embedded web link "bait." However, a closer look shows that the original email contains an action-engaging sentence, "Please respond to this e-mail with your SSC code," which is legitimate, action-inducing bait. We argue that a situational factor of perceived authority, as reflected in the professor-student classroom relationship and university setting, substantially changes the motivation of compliance, increases the threat depiction and appraisal alignment (Chen et al., 2021), and thus reduces students' vigilance and increases the response rate (Schuetz et al., 2026).

Research on authority compliance remains relatively limited in the Information Systems (IS) literature. Compliance with authority refers to the extent to which an individual is willing to follow instructions, recommendations, or directives issued by a trusted authority figure or system. This construct serves as a proxy for individuals' behavioral responses to authoritative cues. Milgram and Gudehus's (1974) Obedience to Authority theory suggests that authority primarily prompts action rather than belief, indicating that individuals may comply with directives from legitimate authorities even amid uncertainty.

ISSN: 2473-4901
v12 n6943

A small number of IS studies draw on Social Influence Theory (SIT) to examine how authority and power affect users' compliance with security-related requests. For example, Bansal et al. (2023) investigate how authority conveyed through coercive power and expert power influences users' willingness to comply with requested security behaviors. SIT explains how individuals are persuaded through three primary social influence processes—internalization, compliance, and identification (Allport, 1985; Kelman, 1958; Turner, 1991). Schuetz et al. (2026) adopt these three SIT processes to the context of security message compliance and conceptualize them as perceived sender's authority characteristics. Specifically, they show that expertise (internalization), coercion (compliance), and similarity (identification) significantly predict users' intentions to comply with security messages.

Building on these perspectives, this study conceptualizes compliance with authority as a situational factor embedded in the study context, where the message sender is perceived as credible (expert power), legitimate (coercive power), and acting in the best interests of the individual or organization (identificative power). Table 1 below shows the original SIT concepts and their adoptions. Examining this factor allows us to assess whether and how additional authority mechanisms operate within a compliance environment, and how the message sender's characteristics influence compliance with security messages. We argue that the perceived high levels of credibility (expert), legitimacy (coercive), and ethical obligation (identificative) in a classroom setting critically reduce scrutiny and increase compliance. We hypothesize:

H8a, b, c: The perceived powers of expertise, coercion, and similarity in ethical obligation in authority increase the likelihood that a person will be deceived by a phishing email.

Processes of Social Influence Theory	Sender Characteristics Kelman (1958)	Constructs Shuetz et al. (2025)	Our Study	Definitions of three Authority Dimensions
Internalisation: A recipient accepts a message because it aligns with their beliefs.	Credibility	Perceived cybersecurity expertise	Perceived expertise	A recipient compliant to a phishing message because he or she believes that the sender is credible and possesses relevant, valuable cybersecurity knowledge.
Compliance: A recipient accepts a message because they want to appease.	Power	Perceived coercive power	Perceived coercion	A recipient compliant to a phishing message because doing so appeases a powerful sender and prevents punishment or disapproval.
Identification: A recipient accepts a message because they want to belong.	Attractiveness	Perceived similarity, based on Turner (1991)	Perceived similarity in ethical obligation	A recipient compliant to a phishing message because doing so helps one act in the best interests of the organization.

Table 1. Three Dimensions of Authority

Extension 3: Authority Compliance in Different Cultures

Building on prior findings that perceptions of authority vary across populations, this study also extends the authority–compliance mechanism by incorporating Cultural Dimensions Theory (Hofstede, 2011), particularly the power distance dimension. We argue that individuals in high power-distance cultures are more likely to accept hierarchical order and comply with directives from perceived authority figures without extensive scrutiny. China, characterized by relatively high power distance, emphasizes respect for authority, social hierarchy, and obedience to institutional roles, whereas the United States, with lower power distance, values individual autonomy and critical evaluation of authority. These cultural differences have important implications for phishing susceptibility. For example, in high power-distance contexts, authority cues embedded in phishing messages—such as institutional affiliation, formal tone, or perceived expertise—may more strongly trigger compliance behavior, reducing skepticism and increasing the likelihood of disclosure. This perspective aligns with IS research on social influence and compliance, which shows that authority-based cues (e.g., expert and coercive power) significantly shape users' security-related behaviors (Bansal et al., 2023; Schuetz et al., 2026). Accordingly, integrating Hofstede's cultural lens with IS compliance literature provides a theoretically grounded explanation for cross-national variation in authority-driven phishing responses and highlights the importance of culturally contingent security interventions.

H9a, b, c: The effect of perceived power in expertise, coercion, and similarity in ethical obligation on phishing susceptibility is stronger in China than in the United States.

ISSN: 2473-4901
v12 n6943

Extension 4: Response Latency

Furthermore, the original study did not capture the response times for phishing emails. With support from new technology, this study will record two key response latencies in phishing susceptibility: (1) the interval between the email being sent and received at the IT desk, and more critically (2) the time between email opening and responding. Prior work shows that repeated security messages and warnings can produce habituation - cybersecurity warning fatigue (Kirwan et al., 2020; Reeves et al., 2023). Evidence from large-scale enterprise settings further suggests that the recency of annual training may not reliably predict lower phishing-click rates (Patrigenaru, 2025), raising concerns about desensitization effects. Accordingly, response latency serves not only as an objective behavioral indicator of phishing susceptibility but also as a lens into temporal dynamics in security behavior. Examining response latency advances theory by clarifying whether it should remain a dynamic temporal factor in studies of repeated exposure and training fatigue, or be best conceptualized as a stable dispositional trait, thereby redefining how temporal behavior should be modeled in future phishing research.

3.3 Hypotheses & Models

The replication hypotheses follow Wright and Marett (2010) exactly in construct definition, directionality, and expected effects. While the replication phase assesses the temporal robustness of Wright and Marett's (2010) findings, the extension hypotheses address two explicit limitations acknowledged in the original study and are theoretically additive rather than corrective: (1) the conceptual mismatch between perceived risk belief and dispositional risk, and (2) the absence of authority-based compliance mechanisms in an institutional context with power distance. Table 2 includes all the hypotheses, of which Hypotheses H1–H6 are direct replications; no reinterpretations are introduced at this stage. H7-H9 hypotheses are about the new extension.

This study models replication and extension variables separately to preserve analytical clarity. Consequently, this study runs two models. Figure 1 depicts the replicated research model adapted from Wright and Marett (2010). Figure 2 presents the replication-plus-extension model. The original replication constructs are retained, except that Perceived Risk Belief will be replaced with risk propensity, and authority compliance is introduced to address limitations identified in prior research. The extended model is evaluated separately to preserve the analytical distinction between replication and extension effects.

Hypothesis	Antecedent Constructs	Relationship with Deception Success	Prediction
H1	Computer Self-Efficacy	Negative (–)	Higher perceptions of Computer Self-Efficacy decrease the likelihood a person will be deceived by a phishing email.
H2	Web Experience	Negative (–)	Online experience decreases the likelihood that a person will be deceived by a phishing email.
H3	Internet Security Knowledg	Negative (–)	Security awareness decreases the likelihood a person will be deceived by a phishing email.
H4	Disposition to Trust	Positive (+)	Disposition to trust increases the likelihood a person will be deceived by a phishing email.
H5	Perceived Risk Belief	Negative (–)	Higher perceived risk decreases the likelihood a person will be deceived by a phishing email.
H6	Suspicion of Humanity	Negative (–)	Suspicion of humanity decreases the likelihood a person will be deceived by a phishing email.
H7	Risk Propensity	Positive (+)	Higher risk tolerance increases the likelihood a person will be deceived by a phishing email.
H8a, b, c	Authority Perception	Positive (+)	The perceived expertise, coercion, and similarity in ethical obligation increase the likelihod that a person will be deceived by a phishing email.
H9a, b, c	Authority Compliance	Positive (+)	The effect of perceived power in expertise, coercion, and similarity in ethical obligation on phishing susceptibility is stronger in China than in the United States.

Table 2. Hypotheses

ISSN: 2473-4901
v12 n6943

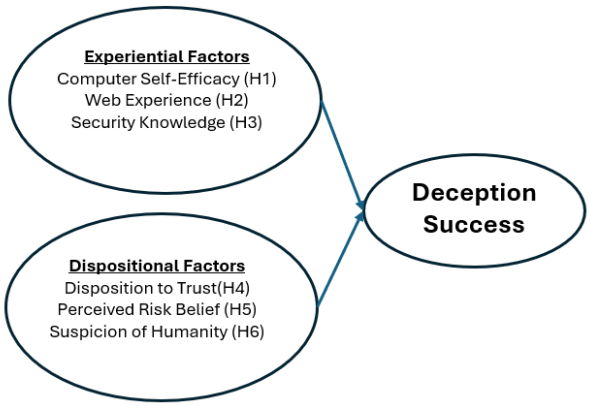

Figure 1: Replication Model Figure

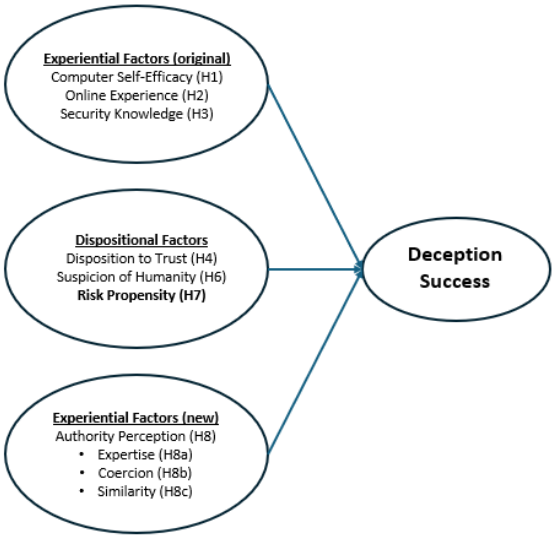

Figure 2: Replication-Plus-Extension Model

4. ANTICIPATED CONTRIBUTIONS

This research is anticipated to make five primary contributions to the literature on phishing and information security.

First, this research rigorously replicates Wright and Marett's (2010) seminal phishing susceptibility theory, conducted 15 years after the original study. Replication studies remain rare in Information Systems security research, despite increasing calls for reproducibility and cumulative theory building. By closely following the original procedures, measures, and analytical logic, this study evaluates the temporal robustness of foundational behavioral findings in a substantially evolved technological and threat environment. *Second*, this research extends the original theory by clarifying risk as a dispositional construct. While the prior study operationalized the perceived risk belief in an information-sharing context, these measures did not adequately capture stable individual differences in risk tolerance. Introducing and examining risk propensity offers a meaningful theoretical explanation of phishing susceptibility. *Third*, this research extends phishing models by incorporating authority compliance as a behavioral mechanism. Modern phishing attacks frequently exploit institutional and authority legitimacy. Drawing on authority-compliance theory, this research hypothesizes that individuals are more likely to comply with phishing requests when they perceive the sender as a legitimate and trusted authority, even with security awareness training. *Fourth*, human behaviors are a function of values and underlying culture. By conducting two experiments in two countries, this study demonstrates the significance of cultural influences and verifies culture theory. *Fifth*, by keeping replication and extension methodologically separable, this study demonstrates the value of replication-plus-extension designs for advancing cybersecurity research: preserving the integrity of the original findings while responsibly advancing theory. This approach responds directly to calls for cumulative, transparent, and reproducible research in information systems.

5. STUDY DEVELOPMENT PROGRESS

The study's theoretical framework has been fully developed, as outlined in this paper, providing a clear foundation for empirical investigation. In parallel, we have completed the design and construction of the survey instrument in both English and Chinese, ensuring cross-cultural equivalence and methodological rigor. We have completed data collection in China. We expect to complete comprehensive analyses before the ISCAP 2026 conference and present results from China. We aim to finalize the manuscript before the conference and submit it to the Journal of Information Systems Applied Research and Analytics (JISARA) for publication consideration.

6. REFERENCES

Allport, G. W. (1985). The historical background of social psychology. In G. Lindzey & E. Aronson (Eds.), Handbook of social psychology (Vol. 1, pp. 1–46). New York: Random House.

Bansal, G., Thatcher, J., & Schuetz, S. W. (2023). Where authorities fail and experts excel: Influencing internet users' compliance intentions. Computers & Security, 128, 103164. https://doi.org/10.1016/j.cose.2023.103164

Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. Interacting with Computers, 23(1), 4–17. https://doi.org/10.1016/j.intcom.2010.07.003

Berthon, P., Pitt, L., Ewing, M., & Carr, C. L. (2002). Potential research space in MIS: A framework for envisioning and evaluating research replication, extension, and generation. Information Systems Research, 13(4), 416-427. https://doi.org/10.1287/isre.13.4.416.71

Chau, M., Li, T. M. H., Wong, P. W. C., Xu, J. J., Yip, P. S. F., & Chen, H. (2020). Finding people with emotional distress in online social media: A design combining machine learning and rule-based classification. MIS Quarterly, 44(2), 933–955. https://doi.org/10.25300/MISQ/2020/14110

Chen, Y., Galletta, D. F., Lowry, P. B., Luo, X., Moody, G. D., & Willison, R. (2021). Understanding inconsistent employee compliance with information security policies through the lens of the extended parallel process model. Information Systems Research, 32(3), 1043-1065. https://doi.org/10.1287/isre.2021.1014

Dennis, A. R., & Valacich, J. S. (2015). A replication manifesto. AIS Transactions on Replication Research, 1(1), 1. https://doi.org/10.17705/1atrr.00001

Federal Bureau of Investigation. (2026). 2025 IC3 annual report. Internet Crime Complaint Center. https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

Hofstede, G. (2011). Dimensionalizing cultures: The Hofstede model in context. Online readings in Psychology and Culture, 2(1), 8. https://doi.org/10.9707/2307-0919.1014

Kelman, H. C. (1958). Compliance, identification, and internalization three processes of attitude change. Journal of Conflict Resolution, 2(1), 51-60. https://doi.org/10.1177/002200275800200106

Kirwan, C. B., Bjornn, D. K., Anderson, B. B., Vance, A., Eargle, D., & Jenkins, J. L. (2020). Repetition of computer security warnings results in differential repetition suppression effects as revealed with functional MRI. Frontiers in Psychology, 11, 528079. https://doi.org/10.3389/fpsyg.2020.528079

Michel Costa de Brito, B., Olinto de Almeida Alves, J., Staudt Rodrigues, M., & Terlizzi, M. A. (2025). Replication of Coordination Artifacts in Agile Software Development in the Brazilian Context. Communications of the Association for Information Systems, 57(1), 1085-1110. https://doi.org/10.17705/1CAIS.05747

Madhurendra. (2026, August 10). Average phishing click rate: 2026 benchmarks by industry. PhishGrid. https://phishgrid.com/blog/average-phishing-click-rate/

Milgram, S., & Gudehus, C. (1974, June). Obedience to authority.

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

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. https://doi.org/10.1080/1366987032000123856

Patrigenaru, I. (2025, September 17). Cybersecurity training programs don't prevent employees from falling for phishing scams. UC San Diego Today. https://today.ucsd.edu/story/cybersecurity-training-programs-dont-prevent-employees-from-falling-for-phishing-scams

Reeves, A., Calic, D., & Delfabbro, P. (2023). "Generic and unusable" 1: Understanding employee perceptions of cybersecurity training and measuring advice fatigue. Computers & Security, 128, 103137. https://doi.org/10.1016/j.cose.2023.103137

Ribeiro, L., Guedes, I. S., & Cardoso, C. S. (2024). Which factors predict susceptibility to phishing? An empirical study. Computers & Security, 136, 103558. https://doi.org/10.1016/j.cose.2023.103558

Schuetz, S. W., Bansal, G., Weng, Q., Lowry, P. B., & Thatcher, J. B. (2026). Heeding the Messenger: The Influence of Sender Characteristics on Security Message Compliance Intentions. Information Systems Journal, 36(3), 410-434. https://doi.org/10.1111/isj.70013

Shrout, P. E., & Rodgers, J. L. (2018). Psychology, science, and knowledge construction: broadening perspectives from the replication crisis. Annual Review of Psychology, 69, 487–510. https://doi.org/10.1146/annurev-psych-122216-011845

Singh, K., Ang, S. H., & Leong, S. M. (2003). Increasing replication for knowledge accumulation in strategy research. Journal of Management, 29(4), 533-549. https://doi.org/10.1016/S0149-2063(03)00024-2

Turner, J. C. (1991). Social influence: Thomson Brooks/Cole Publishing Co.

Verizon. (2024). 2024 data breach investigations report: Executive summary. https://www.verizon.com/business/resources/reports/2024-dbir-executive-summary.pdf

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. https://doi.org/10.1016/j.dss.2011.03.002

Williams, E. J., Hinds, J., & Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. International Journal of Human-Computer Studies, 120, 1-13. https://doi.org/10.1016/j.ijhcs.2018.06.004

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), 273-303. https://doi.org/10.2753/MIS0742-1222270111

Wright, T. A., & Sweeney, D. A. (2016). The call for an increased role of replication, extension, and mixed - methods study designs in organizational research. Journal of Organizational Behavior, 37(3), 480-486. https://doi.org/10.1002/job.2059

Yuan, A., Gao, Y., Edlin, G. C., & Samtani, S. (2025). Identifying emotional distress on social media: A replication study. Communications of the Association for Information Systems, 57, 1134-1146. https://doi.org/10.17705/1CAIS.05749

Zaitsev, A., Gal, U., & Tan, B. (2020). Coordination artifacts in agile software development. Information and Organization, 30(2), 100288. https://doi.org/10.1016/j.infoandorg.2020.100288