

DOI: https://doi.org/10.48009/3_iis_2026_123

Exploring the Moderating effects on the Dark Side of Trust in Organizational Security Practice and User Security Decision Level

Linwu Gu, *Slippery Rock University*, linwu.gu@sru.edu
Jianfeng Wang, *Kutztown University*, jwang@kutztown.edu

Abstract

Despite growing interest in employee cybersecurity behavior, prior research has largely viewed trust as a uniformly beneficial construct. Consequently, little is known about the potential dark side of trust in organizational cybersecurity contexts. Drawing on the dark side of trust perspective and Social Cognitive Theory, this study examines whether security self-efficacy moderates the relationship between trust in organizational security practices and user security decision levels. Survey data from 120 participants were analyzed using partial least squares structural equation modeling (PLS-SEM). The results demonstrate that security self-efficacy significantly weakens the negative relationship between trust in organizational security practices and user security decision levels, suggesting that employees with higher security self-efficacy remain vigilant despite high levels of organizational trust.

Keywords: Dark Side of Trust, Security Self-Efficacy, Organizational Security Practice, User Security Decision Level

Introduction

Organizations today face significant cybersecurity challenges as the rapid proliferation of IT systems has introduced numerous vulnerabilities. Each successful cyber breach is estimated to cost organizations an average of \$7.91 million, emphasizing the urgent need for effective cybersecurity defenses (Ampel et al., 2024). Recent research defines trust in organizational cybersecurity as individuals' beliefs regarding cybersecurity protections within organizational environments, including situational normality and structural assurance (Anderson et al., 2010; McKnight et al., 2011). Similarly, trust in organizational security practices refers to employees' beliefs regarding the effectiveness and reliability of organizational security-related practices (Lowry et al., 2015).

Trust helps employees reduce uncertainty and vulnerability by relying on organizational cybersecurity structures and protections (Rousseau et al., 1998). Although trust can support cooperative and secure behaviors, excessive trust may also create unintended negative consequences associated with the dark side of trust. In high-trust environments, employees may rely too heavily on organizational protections, resulting in reduced personal vigilance (Klöpper & Rowe, 2026). Consequently, employees may overlook phishing emails, disclose credentials, download malicious software, or ignore other security threats (Workman, 2008).

Security self-efficacy is an important predictor of secure behavior and security technology use. Prior studies have shown that self-efficacy positively influences individuals' intentions to engage in protective security behaviors, including using anti-spyware software, reducing susceptibility to phishing attacks, and adopting

other cybersecurity practices (Anderson et al., 2010). Chen and Zahedi (2016) further demonstrated that self-efficacy strengthens adaptive security behaviors and reduces avoidance responses. Individuals with high security self-efficacy are more likely to believe they can successfully identify and respond to cyber threats, thereby encouraging proactive and vigilant security behaviors (Tong et al., 2021). Importantly, security self-efficacy may reduce the negative consequences associated with excessive trust. Therefore, this study examines the moderating role of security self-efficacy in the relationship between trust in organizational security practices and user security decision levels.

Drawing on the dark side of trust literature, this study proposes that excessive trust in organizational security practices may negatively affect user security decision levels (see Figure 1). In addition, security self-efficacy is proposed as a moderating factor that weakens the negative effect of excessive trust. To test the proposed model, survey data **were** collected and analyzed using PLS-SEM.

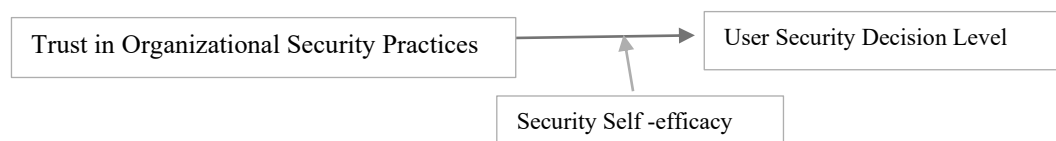


Figure 1: Research Model

Theory Foundation and Literature Review

Prior information security research has primarily focused on factors that encourage employees to engage in secure behaviors and comply with organizational security policies (Raju et al., 1995). Among these factors, trust in organizational security practices has generally been viewed as beneficial because it reduces uncertainty and increases cooperation. However, emerging research suggests that excessive trust may also create negative consequences, including complacency and reduced vigilance (Greulich et al., 2024). Drawing on the dark side of trust perspective and Social Cognitive Theory, this study examines how trust in organizational security practices influences user security decision levels and how security self-efficacy moderates this relationship.

Trust in Organizational Security Practices

Previous research has generally portrayed trust in organizational security practices as beneficial. Studies suggest that trust increases employees' commitment to security practices and encourages compliance with organizational security procedures (Cram et al., 2019; Lowry et al., 2015). Trust has also been associated with reduced perceptions of uncertainty and risk (Mayer et al., 1995; Burns et al., 2019). Consequently, most information security studies emphasize the "bright side" of trust, including reduced computer abuse, fewer policy violations, and stronger peer-monitoring behaviors (Liu et al., 2020; Yazdanmehr & Wang, 2021).

However, trust is not always beneficial. Researchers increasingly acknowledge the "dark side" of trust, in which excessive or misplaced trust leads to complacency, overreliance, and reduced vigilance (Gargiulo & Ertug, 2006; Pavlou et al., 2007). Studies show that employees who place a high level of trust in their coworkers are more likely to ignore security precautions (Tan & Lim, 2009), while interpersonal trust may increase susceptibility to phishing attacks (Karjalainen et al., 2019; Martin et al., 2021). Excessive trust in organizational security practices may diminish individuals' security concerns, increase non-malicious

security violations, and ultimately weaken compliance with security policies (Stafford, 2022; Atkinson, 2007; Patzelt & Shepherd, 2008; Tan & Lim, 2009). Despite these concerns, the dark side of trust remains underexplored in information security research. In cybersecurity contexts, misplaced trust may reduce user perceptions of risk and lead to reduced vigilance given the high-risk nature of the domain (Langfred, 2004; Lee et al., 2004). The limited attention devoted to the dark side of trust in cybersecurity research represents an important opportunity for future research, especially as organizations increasingly rely on user compliance to prevent security breaches (Pienta et al., 2020).

Security Self-Efficacy

Security self-efficacy refers to an individual's belief in their capability to successfully perform cybersecurity tasks and protective behaviors (Li et al., 2026). Rooted in Social Cognitive Theory (Bandura, 1986), security self-efficacy shapes individuals' motivation, judgments, and responses to cybersecurity threats (Bahreini et al., 2023; Kumar et al., 2025).

Prior research consistently identifies security self-efficacy as an important predictor of security-related behaviors. Within Protection Motivation Theory (PMT), self-efficacy influences whether individuals adopt protective actions in response to threats (Rogers, 1975). Similarly, Technology Threat Avoidance Theory suggests that self-efficacy predicts compliance with information security behaviors (Nacarelli & Gefen, 2021; Rowe & Merminod, 2023). Individuals with high security self-efficacy are more likely to install updates, create strong passwords, avoid suspicious links, and comply with security policies (Rhee et al., 2009; Chen & Zahedi, 2016). In contrast, individuals with low security self-efficacy may become more dependent on organizational protections and trusted others, thereby increasing their susceptibility to risky security behaviors (Ng et al., 2021).

Previous studies indicate that employees with higher security self-efficacy feel more capable of taking security-related actions and are more likely to believe that effective security decisions can mitigate threats (Silica & Lowry, 2020). While high trust in organizational security practices may reduce attentiveness and encourage overreliance on organizational protections, individuals with high security self-efficacy may remain attentive to potential threats because they are confident in their ability to manage security risks. Accordingly, security self-efficacy may weaken the negative effects of excessive trust by encouraging continued vigilance and proactive security decision-making.

User Security Decision Level

User security decisions refer to deliberate actions employees take to protect organizational IT resources, such as enabling multifactor authentication, reporting suspicious emails, and managing privacy settings (Bahreini et al., 2023; Burns et al., 2019). These individual decisions collectively determine an employee's overall level of cybersecurity protection. Accordingly, User Security Decision Level refers to the extent to which a user accumulated security decisions result in stronger or weaker cybersecurity protection.

Prior research suggests that User Security Decision Level reflects the overall degree of protection resulting from user combined security choices (Bahreini et al., 2016; Wagner & Mesbah, 2019). Research also shows that default settings strongly influence user security decisions because of status quo bias (Acquisti & Gross, 2006; Hsieh et al., 2015). Decisions regarding two-factor authentication (2FA), login alerts, automatic updates, and privacy controls collectively determine user security decision levels, where even a few insecure decisions may substantially weaken overall cybersecurity protection (Watson et al., 2015; Kim & Kankanhalli, 2009).

Within organizational settings, excessive trust in organizational security practices may lower user security decision levels. Employees who place excessive trust in organizational protections—such as antivirus systems, automatic updates, and IT departments—may reduce their personal vigilance and become less likely to adopt additional security precautions (De Luca et al., 2015; Dogruel et al., 2017). In contrast, individuals with high security self-efficacy are more likely to remain vigilant despite high organizational trust, whereas those with lower security self-efficacy may become more susceptible to complacency and risky security decisions (Chen & Liang, 2019).

Drawing on the dark side of trust perspective and Social Cognitive Theory, this study proposes that excessive trust in organizational security practices may reduce user security decision levels by encouraging overreliance on organizational safeguards and reducing personal vigilance. Social Cognitive Theory further suggests that individuals' beliefs in their capabilities influence how they respond to potential cybersecurity threats. Employees with high security self-efficacy are therefore expected to remain vigilant and proactive even when they strongly trust organizational security practices. Consequently, security self-efficacy is expected to weaken the negative relationship between trust in organizational security practices and user security decision levels.

Therefore, this study proposes the following hypotheses:

H1: Trust in organizational security practices negatively affects user security decision levels.

H2: Security self-efficacy moderates the relationship between trust in organizational security practices and user security decision levels.

Research Methodology

A survey method was employed to test the research model. The survey included measures of trust in organizational security practices, security self-efficacy, and user security decision levels. We used Google Forms to distribute the online questionnaire through our social media networks and to participants enrolled in cybersecurity courses in a professional master's program. A total of 120 valid responses were collected. Among the participants, 62.5% were male and 37.5% were female. The participants had an average of 12.5 years of computer usage experience.

This study employed three constructs measured using seven-point Likert-type scales. All measurement items (see Table 1) were adapted from previously validated instruments reported in the information security literature. Minor wording adjustments were made to reflect the organizational cybersecurity context while preserving the original meaning of the constructs. The adapted questionnaire was reviewed for clarity prior to data collection.

Table 1: Survey Items

Constructor	Measures	Items
Trust in Organizational Security Practices	Greulich, et al 2024	My organization treats me fairly in security-related matters. I feel comfortable raising security concerns. My organization communicates clearly and openly about its security policies. I trust that my organization will support me if I report a potential security issue.
<i>Security Self-Efficacy</i>	Adapted from li, et al 2026	My knowledge to deal with Internet security is adequate. I feel confident handling virus-infected files. I feel confident getting rid of malware. I feel confident learning the method to secure my computer I feel confident using different programs to secure my computer.
User Security Decision level	Adapted from Bahreini, et al 2023	I prefer that the app automatically updates its software. I prefer that the app automatically updates its plugins. I prefer to block downloads from unknown sources. I want to be alerted whenever a login occurs from a new device. I want to require two-factor authentication every time I log in from a new device. I prefer to block pop-ups and redirects in the news and social network sections. I prefer to block third-party ads from being shown within the app. I do not want the app to save cookies from my search history.

Results

Partial least squares structural equation modeling (PLS-SEM) was employed to test the hypotheses, and the model was analyzed using SmartPLS 3.0. Compared with covariance-based approaches, PLS requires fewer assumptions regarding model identification and data distribution (Fornell & Bookstein, 1982).

Table 2- Correlation, AVEs and Reliabilities of Constructs

Constructs	CR	AVE	1	2	3
Trust in Organizational Security Practice	0.8745	0.8447	0.9191		
Security Self-Efficacy	0.8002	0.7835	0.2186	0.8852	
User Security Decision Level	0.8680	0.8010	0.110	0.4314	0.8950
Note: CR= composite reliability, diagonal elements represent square roots of AVEs					

The validity and reliability of the measurement model were evaluated using conventional criteria. As shown in Table 2, all constructs' average variance extracted (AVE) values exceeded the recommended threshold of 0.50, indicating adequate convergent validity. Table 3 further shows that all factor loadings exceeded 0.70 on their respective constructs (Fornell & Larcker, 1981). Regarding discriminant validity, Table 2 indicates that the square roots of the AVEs were greater than the correlations among constructs, while all construct correlations were below the recommended cutoff value of 0.90. Additionally, Table 3 shows that each item loaded more strongly on its corresponding construct than on other constructs, further supporting discriminant validity.

Composite reliability values ranged from 0.8002 to 0.8745, exceeding the recommended threshold of 0.70 and thereby demonstrating satisfactory internal consistency reliability. Average variance extracted (AVE) values ranged from 0.7835 to 0.8447; as all values were above the 0.50 cutoff, adequate convergent validity is demonstrated (Baron & Kenny, 1986; Hair et al., 2010).

Table 3 -Cross loadings

	Mean	SD	TOSP	SSE	USDL
TOSP1	6.2812	1.431	0.822		
TOSP2	6.7657	1.415	0.817		
TOSP3	5.8872	1.422	0.866		
TOSP4	6.2784	1.426	0.845		
SSE1	5.3671	1.524	0.572	0.755	
SSE2	5.2568	1.556	0.367	0.837	
SSE3	6.4468	1.495	0.268	0.821	
SSE4	6.1255	1.522	0.211	0.791	
SSE5	6.6042	1.525	0.377	0.831	
USDL1	4.0744	1.315	0.423	0.130	0.861
USDL2	4.2235	1.461	0.257	0.241	0.803
USDL3	4.1382	1.294	0.364	0.512	0.754
USDL4	4.3206	1.395	0.225	0.448	0.774
USDL5	3.9525	1.356	0.101	0.540	0.828
USDL6	4.5201	1.453	0.201	0.389	0.826
USDL7	4.2163	1.478	0.203	0.267	0.833
USDL8	4.2847	1.356	0.101	0.521	0.789
<i>Note:</i> Trust in Organizational Security Practice=TOSP; Security Self-Efficacy= SSE; User Security Decision Level =USDL					

Structural Model Results

Figure 2 presents the PLS test results. The research model explains 35.2% of the variance in user security decision levels. To test H1, we first estimated the direct relationship between trust in organizational security practices and user security decision levels. The results indicate a significant negative relationship ($\beta = -0.330$, $p < 0.01$), suggesting that higher trust is associated with lower security decision levels.

To test the moderating effect of security self-efficacy, an interaction term between trust in organizational security practices and security self-efficacy was added to the model. The interaction effect was significant ($\beta = -0.216$, $p < 0.05$), indicating that the relationship between trust and user security decision levels varies depending on the level of security self-efficacy. Thus, H2 is supported, suggesting that security self-efficacy weakens the negative effect of excessive trust on user security decision levels.

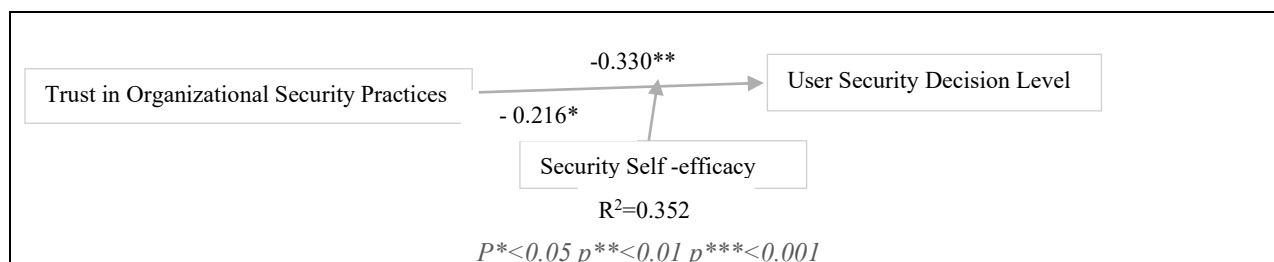


Figure -2: PLS Test Results

Simple slope analysis (see Figure 3) further shows that when security self-efficacy is low, the relationship between trust and user security decision levels is significantly negative ($\beta = -0.52$, $p < 0.05$), supporting H₂. In contrast, when security self-efficacy is high, the relationship becomes weaker and statistically insignificant ($\beta = 0.105$, $p > 0.05$). The findings suggest that security self-efficacy mitigates the negative effects associated with the dark side of trust. Employees with low security self-efficacy are more likely to rely excessively on organizational protections, resulting in lower security decision levels when trust is high. In contrast, employees with high security self-efficacy remain more vigilant and proactive in their security behaviors, thereby weakening the negative effect of excessive trust.



Figure 3 – The moderation effects of Security Self-Efficacy

Table 4 - Hypotheses Testing

Hypotheses	Path	β	T- value	P-value	Result
H ₁	Trust in Organizational Security Practice → User Security Decision Level	-0.330	-2.756	P<0.01	H ₁ Supported
H ₂	Security Self-Efficacy × Trust in Organizational Security Practice → User Security Decision Level	-0.216	-2.035	P<0.05	H ₂ Supported

Contributions to Practice, Limitations, and Future Research

This study contributes to the information security literature by extending research on trust in organizational security practices. While prior studies primarily emphasize the positive effects of trust, this study demonstrates that excessive trust may negatively affect user security decision-making by reducing vigilance and encouraging overreliance on organizational protections. The findings provide empirical support for the dark side of trust, identifying an important boundary condition under which trust becomes detrimental. Moreover, integrating Social Cognitive Theory with the dark side of trust perspective provides a richer explanation of employee cybersecurity behavior. The results suggest that security self-efficacy functions as an important psychological resource that offsets the negative behavioral consequences associated with excessive organizational trust.

The study further identifies security self-efficacy as an important moderating factor. Employees with high security self-efficacy are less likely to become complacent even when they strongly trust organizational security practices. This finding highlights the importance of considering both organizational trust and individual capability beliefs when examining employee cybersecurity behavior. Specifically, the moderation results indicate that the negative effect of trust in organizational security practices is stronger

among individuals with low security self-efficacy but becomes weaker and statistically insignificant among individuals with high security self-efficacy. In addition, security self-efficacy functions as a protective factor that reduces employees' vulnerability to the dark side of trust.

From a practical perspective, organizations should avoid assuming that secure technical infrastructure alone is sufficient to improve employee cybersecurity behavior. Although organizational security practices remain essential, organizations should simultaneously empower employees by strengthening their cybersecurity capabilities and training. Non-technical mechanism such as least privilege, separation of duties, and prevention of privilege escalation, etc., should be seriously implemented and followed. Regular phishing simulations, hands-on security exercises, scenario-based training, and continuous feedback can improve employees' security self-efficacy, enabling them to remain vigilant even in highly trusted organizational environments. These findings suggest that effective cybersecurity depends not only on organizational protections but also on employees' confidence in making sound security decisions.

Despite these contributions, this study has several limitations. First, the study relied on cross-sectional survey data from 120 participants, limiting generalizability and causal interpretation. Future research should employ longitudinal or experimental designs. Second, the study relied on self-reported perceptions and behaviors, which may introduce common method bias. Future studies could incorporate objective behavioral security measures.

Finally, this study examined trust in organizational security practices as a general construct. Future research could distinguish between different forms of trust—such as trust in management, coworkers, or security technologies—and examine additional moderating factors, including cybersecurity experience, organizational culture, and perceived threat severity.

References

- Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, 34(3), 613–643.
- Ampel, B. M., Samtani, S., Zhu, H., & Chen, H. (2024). Creating proactive cyber threat intelligence with hacker exploit labels: A deep transfer learning approach. *MIS Quarterly*, 48(1), 137-166.
- Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In G. Danezis & P. Golle (Eds.), *Privacy enhancing technologies* (pp. 36–58). Springer.
- Atkinson, S. (2007). The role of trust in information security. *Information Security Technical Report*, 12(3), 165-171.
- Bahreini, A. F., Cavusoglu, H., & Cenfetelli, R. T. (2023). How “What you think you know about cybersecurity” can help user make more secure decisions. *Information & Management*, 60(7), 103860.
- Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory*. Prentice-Hall.

- Baron, R.M., & Kenny, D.A. (1986). The moderator-mediator variable distinction in social psychological research: conceptual, strategic, and statistical considerations. *J Pers Soc Psychol.*, 1986 Dec;51(6):1173-82.
- Burns, A. J., Roberts, T. L., Posey, C., & Lowry, P. B. (2019). The adaptive roles of positive and negative emotions in organizational insiders' security-based precaution taking. *Information Systems Research*, 30(4), 1228-1248.
- Bahreini, K., Nadolski, R., & Westera, W. (2016). Information security awareness and behavior: A theory-based literature review. *Journal of Information Security and Applications*, 26, 52–60.
- Bassellier, G., Benbasat, I., & Reich, B. H. (2003). The influence of business managers' IT competence on championing IT. *Information Systems Research*, 14(4), 317–336.
- Chen, D. Q., & Liang, H. (2019). Wishful thinking and IT threat avoidance: An extension to the technology threat avoidance theory. *IEEE Transactions on Engineering Management*, *66*(4), 552–567.
- Chen, Y., & Zahedi, F. M. (2016). Individuals' Internet security perception and behaviors: Polycontextual contrasts between the United States and China. *MIS Quarterly*, *40*(1), 205–222.
- 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.
- De Luca, A., Hang, A., Von Zezschwitz, E., & Hussmann, H. (2015). I feel like I'm taking selfies all day! Towards understanding biometric authentication on smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (pp. 1411–1414). Association for Computing Machinery.
- Dogruel, L., Joeckel, S., & Vitak, J. (2017). The valuation of privacy premium features for smartphone apps: The influence of defaults and expert recommendations. *Computers in Human Behavior*, 77, 230–239.
- Fornell, C., & Bookstein, F. L. (1982). Two structural equation models: LISREL and PLS applied to consumer exit-voice theory. *Journal of Marketing Research*, 19(4), 440–452.
- Fornell, C., & Larcker, D. (1981). Evaluating structural equation models with unobservable and measurement error. *Journal of Marketing Research*, 18(1), 39–50.
- Gargiulo, M., & Ertug, G. (2006). The dark side of trust. In R. Bachmann & A. Zaheer (Eds.), *Handbook of trust research* (pp. 165-186). Edward Elgar Publishing.
- Greulich, M., Lins, S., Pienta, D., Thatcher, J. B., & Sunyaev, A. (2024). Exploring contrasting effects of trust in organizational security practices and protective structures on employees' security-related precaution taking. *Information Systems Research*, 35(4), pp. 1586-1608.
- Hair, J., Black, W., Babin, B., & Anderson, R. (2010). *Multivariate Data Analysis* (7th ed.). Upper Saddle River, NJ: Prentice-Hall, Inc.

- Karjalainen M, & Sarker S, Siponen M (2019) Toward a theory of information systems security behaviors of organizational employees: A dialectical process perspective. *Inform. Systems Res.* 30(2):687–704
- Kim, H. W, & Kankanhalli, A(2009). Investigating user resistance to information systems implementation: A status quo bias perspective. *MIS Quarterly*, 33(3), 567-582.
- Klöpffer, M., & Rowe, F. (2026). People analytics, trust erosion and intention to leave: The role of information asymmetry. *Information & Management*, 63(4), 104346.
- Kumar, N., Kumar, R. R., & Raj, A. (2025). Establishing Antecedents and Outcomes of Human-AI Collaboration: Meta-Analysis. *Journal of Computer Information Systems*, 1–15.
- Langfred, C. W. (2004). Too much of a good thing? Negative effects of high trust and individual autonomy in self-managing teams. *Academy of Management Journal*, 47(3), 385–399.
- Lee, J. D., & See, K. A. (2004). Trust in automation: Designing for appropriate reliance. *Human Factors*, 46(1), 31.
- Li, Y., Wang, X., Li, Y., & Khasraghi, H. J. (2026). Lost at the cyber-crossing? Understanding individuals' internet security threat ambivalence and its impact on threat avoidance and approach behavior. *Information & Management*, 63(4), 104328.
- Liu, Y., Wang, J., & Chen, Y. (2020). Trust and security behavior: The role of reciprocity. *Computers & Security*, 92, 101756.
- Lowry, P. B., Posey, C., Bennett, R. J., & Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies. *Journal of the Association for Information Systems*, 16(10), 807-854.
- Mayer, R. C., & Davis, J. H. (1999). The effect of the performance appraisal system on trust for management: A field quasi-experiment. *Journal of Applied Psychology*, 84(1), 123.
- McKnight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a specific technology: An empirical investigation of its components and measures. *ACM Transactions on Management Information Systems*, 2(2), Article 12, 1-25.
- Ng, K. C., Zhang, X., Thong, J. Y., & Tam, K. Y. (2021). Protecting against threats to information security: An attitudinal ambivalence perspective. *Journal of Management Information Systems*, 38(3), 732–764.
- Nacarelli, V., & Gefen, D. (2021). Trustworthiness and the adoption of business analytics. *Information Systems Management*, 38(3), 185–199.
- Patzelt, H., & Shepherd, D. A. (2008). The decision to persist with underperforming alliances: The role of trust and control. *Journal of Management Studies*, 45(7), 1217-1243.
- Pienta, D. A., Tams, S., & Thatcher, J. (2020). Can trust be trusted in cybersecurity? In *Proceedings of the 53rd Hawaii International Conference on System Sciences (HICSS)*.

<https://doi.org/10.24251/hicss.2020.522>

- Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quarterly*, 31(1), 105-136.
- Raju, P. S., Lonial, S. C., & Mangold, W. G. (1995). Differential effects of subjective knowledge, objective knowledge, and usage experience on decision making: An exploratory investigation. *Journal of Consumer Psychology*, 4(2), 153-180.
- Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end user information security practice behavior. *Computers & Security*, 28*(8), 816-826.
- Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, 23(3), 393-404.
- Rowe, F., Te'eni, D., & Merminod, V. (2023). The maturation of digital objects in innovation projects: The role of interpersonal networks and team sharing atmosphere. *European Journal of Information Systems*, 32(3), 434-461.
- Silica, 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.
- Stafford, T. (2022). Security complacency and nonmalicious violations. *Information & Computer Security*, 30(2), 221-238.
- Tan, H. H., & Lim, A. K. H. (2009). Trust in coworkers and trust in organizations. *Journal of Psychology*, 143(1), 45-66.
- Tong, S., Jia, N., Luo, X., & Fang, Z. (2021). The Janus face of artificial intelligence feedback: Deployment versus disclosure effects on employee performance. *Strategic Management Journal*, 42(9), 1600-1631.
- Wagner, A., & Mesbah, N. (2019). Too confident to care: Investigating overconfidence in privacy decision making. In *Proceedings of the 27th European Conference on Information Systems (ECIS)*. https://aisel.aisnet.org/ecis2019_rp/56
- Watson, J., Lipford, H. R., & Besmer, A. (2015). Mapping user preference to privacy default settings. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 22(6), 1-20.
- Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology*, 59(4), 662-674.
- Yazdanmehr A, & Wang J (2021) Can peers help reduce violations of information security policies? The role of peer monitoring. *Eur. J. Inform. Systems* 32(3):508-528.