Nudging Towards Compliance? Assessing the Impact of Nudging Strategies on Information Security Policy Adherence

Theresa Pfaff [1,2]

[1] *University of Goettingen, Goettingen, Germany*
[2] *University of Paderborn, Paderborn, Germany*

Abstract

Data breaches pose a significant economic risk to companies in their daily business. To mitigate this risk, organizations implement information security policies (ISPs) to guide their employee's behavior. However, employees often fail to comply with these policies. To address this issue and promote desired behavior, the concept of nudging has emerged as a potential strategy. By leveraging insights from the dual-process theory, which recognizes two distinct cognitive systems involved in decision-making, this ongoing research aims to explore the effectiveness of nudging strategies through an online experiment. Specifically, it investigates whether information security policy messages can nudge employees towards adopting more secure behaviors by targeting their intuitive responses (System 1) or invoking critical thinking (System 2). This research seeks to advance our understanding of behavioral interventions in the context of information security and has the potential to provide valuable insights for designing effective strategies to promote ISP compliance.

Keywords

ISP Compliance, Digital Nudging Strategies, Dual-Process Theory

1. Introduction

One of the most prominent threats to organizational information assets comes from employees who have regular access to these resources [1, 2]. To mitigate the risks posed by insider threats, organizations adapt their risk management by implementing ISPs as a crucial instrument to reduce vulnerabilities and guide employee behavior. ISPs are a documented set of rules and guidelines that outline how an organization protects its sensitive information and manages information security risks [3]. It is a necessary tool as organizations face significant risks from cyberattacks and data breaches targeting their internal information, resulting in substantial costs for the affected company [4].

Research indicates that individuals often exhibit inappropriate and insecure behavior because they often prioritize convenience over adhering to information security policies [5]. Prior studies have examined various factors influencing employee compliance from a rational standpoint. Recent studies looked at employee's behavior by focusing on costs and benefits of compliance based on rational choice theory [6], threat and coping assessment by utilizing protection motivation theory [7, 8], and exerting pressure by using general deterrence theory including the assessment of potential sanctions [9, 10, 11]. While these studies provide valuable insights, they often focus on factors to explain certain behavior or to understand employees decision-making processes in a work environment. For example, most studies in this field specifically focus on employees' attitudes, knowledge, and intentions towards ISP compliance. They, furthermore, often explore the role of individual factors, such as awareness, perception of risk, and organizational support, in order to make the black-box of humans' decision-making-processes more transparent [12, 13]. While research has provided valuable insights into the factors that

CIISR 2023: 3rd International Workshop on Current Information Security and Compliance Issues in Information Systems Research, co-located with the 18th International Conference on Wirtschaftsinformatik (WI 2023), September 18, 2023, Paderborn, Germany

theresa.pfaff@uni-goettingen.de; tpfaff@mail.uni-paderborn.de (T. Pfaff)

0009-0005-1263-1760 (T. Pfaff)

contribute to understanding security behavior, the question how to get employees towards the desired behavior has not been investigated yet. Deterrence measures for example, like punishment may effectively force employees towards the desired outcome [11]. Still, they also provoke a work environment built on fear and dissatisfaction. Surprisingly and to the best of our knowledge, no study has thought about the concept of nudging in this context i.e., how to strategically nudge employees towards the desired behavior. A recent study by [14] has shown that different types of employees react differently in their compliance behavior to certain deterrents. Therefore, it is reasonable to assume that this could also be the case with different nudge messages addressing different systems. In this context, nudging refers to the use of certain design elements in a user interface to influence users' choices while using IS [15].

At the same time, most studies only focus on factors affecting employee compliance on both a rational and deliberated level. Consequently, there is a need to delve deeper into the less-explored dimensions of employee compliance, also considering non-rational and automated aspects that may influence their behavior. This research aims to fill this gap by investigating the dual-process nature of employees' cognitive responses to information security nudge messages. Therefore, this study seeks to answer the research question (RQ):

RQ: How can information security policy (ISP) messages nudge employees towards a more compliant behavior?

The aim of this research is to investigate whether and how information security policy messages can effectively nudge employees towards enhanced compliance with ISPs as this is the desired behavior from an organizational perspective. The study further seeks to uncover the mechanisms through which these policy messages influence employees' cognitive processes, specifically their gut reactions (System 1) and/or critical thinking (System 2). By unraveling the impact of information security policy messages on employees' cognitive processes, the research aims to contribute to the understanding of behavioral interventions in the context of information security and provide insights for designing more effective strategies to promote ISP compliance. The aim of this research in progress paper is to present a status quo of current undertakings and to provide an outlook on further actions.

2. Theoretical Background

2.1. Dual-Process Theory

First The dual-process theory posits that human cognition and decision-making involve two distinct cognitive processes: System 1 and System 2. System 1 thinking is automatic, intuitive, and fast, driven by heuristics and immediate emotional responses. On the other hand, System 2 thinking is reflective, deliberate, and analytical, involving conscious reasoning and cognitive effort [16, 17]. In the context of investigating information security policy compliance, the dual-process theory provides a suitable theoretical lens for several reasons. In order to understand employees' compliance behavior, it requires examining both, their automatic, intuitive responses (System 1) and their reflective, deliberative processes (System 2). By considering the interplay between these cognitive processes, insights into the factors influencing employees' decision-making can be gained. For example, [18] found that presenting fact-checking results in a combined approach targeting both systems, automatic cognition via symbols and deliberate cognition via text phrases, was twice as effective in detecting fake news compared to settings where only one system was primarily addressed. Additionally, the theory helps to explain why employees may exhibit inconsistent compliance behavior. System 1 responses, driven by heuristics and emotions, can lead to impulsive or careless actions that deviate from established policies [19]. System 2 thinking, on the other hand, allows employees to engage in conscious reasoning and critically evaluate the implications of their behavior in terms of information security. The dual-process theory also highlights the potential conflicts and trade-offs between System 1 and System 2 processes [20, 21]. Employees may face cognitive biases, such as cognitive dissonance or anchoring, that influence their decision-making and adherence to security policies.

Understanding these conflicts can provide valuable insights for designing effective nudging strategies that target both automatic and reflective cognitive processes.

Overall, the dual-process theory provides a comprehensive framework for examining the cognitive mechanisms underlying employees' compliance behavior and offers guidance for designing interventions that effectively promote information security policy compliance.

paragraph in every section does not have first-line indent. Use only styles embedded in the document.

2.2. Digital Nudging towards Desired Behavior

Digital nudging refers to the strategic use of subtle and non-intrusive digital interventions aimed at guiding individuals' decision-making and influencing their behavior towards desired outcomes [15]. Rooted in behavioral economics and psychology, digital nudging leverages principles of choice architecture to shape decisions without resorting to strict regulations or mandates. In the context of employees' compliance with ISPs, investigating nudging strategies becomes imperative due to the persistent challenge of motivating employees to adhere to established security protocols. Traditional approaches, such as training programs and enforcement measures, often fall short in effectively modifying employees' behavior. By exploring the potential of digital nudging techniques, organizations can harness the power of choice architecture to nudge employees towards more secure behaviors.

This research endeavors to examine the efficacy of nudging strategies in the realm of ISP compliance, aiming to provide valuable insights into the design of interventions that align with employees' decision-making processes, thereby fostering a culture of enhanced information security while respecting individuals' autonomy and decision-making agency. Nudging strategies are applied in various contexts, such as public health decisions, consumer behavior, or tax compliance [15, 22, 23]. While there is an upcoming trend of examining nudging in privacy and security context, research primarily focuses on privacy settings, password creation or phishing detection [24, 25, 26]. However, recent literature claims to further extend the design of nudges to other scenarios in cybersecurity, such as protection of data [26].

3. Hypotheses Development and Research Model

The goal of an intervention aiming to influence cognitive functions in System 1 is to provide an intuitively clear stimulus, according to [18]. Simple visual signs can be understood fast and with less cognitive effort [21] making it a suitable nudge strategy, triggering heuristic and immediate responses. Contrary to this, textual detailed information will more likely trigger System 2 as it takes more time and effort to process the given information. Understanding text arguments and connecting them to prior knowledge requires deliberate attention to detail, which is usually part of System 2 cognition [17]. In their study, [24] revealed that a security nudge text-message can increase users security behavior. Especially messages emphasizing the threat and the corresponding coping behavior were most effective. Therefore, it is expected:

H1a: Employees' ISP compliance behavior with a System 1 nudge strategy is enhanced when compared to decision settings in which no nudge is applied.

H1b: Employees' ISP compliance behavior with a System 2 nudge strategy is enhanced when compared to decision settings in which no nudge is applied.

However, system 1 and system 2 cannot be strictly separated as both systems are considered rather complements than substitutes [18]. An intervention that combines the two theories will likely have a greater effect than the two single-interventions if they are both, primarily, acting through one theoretical route. If both single interventions primarily act through one theoretical route, then an intervention that combines the two strategies and triggers both systems simultaneously will likely have a better effect than the single-interventions [15]. Therefore, it is stated:

H2: The combination of both nudging strategies is more effective than no nudge or a single nudge applied.

Information security policy compliance is more likely to occur if employees believe their managers, IT personnel, or peers expect them to comply [12]. However, work environments are dynamic environments with arising situational characteristics such as demanding colleagues and finding workarounds [27]. Conversely, if peers, IT personnel, or managers themselves do not adhere to policies this, then employees might adapt this behavior. Moreover, if these peers put colleagues into demanding situations this, can result in peer pressure which is defined as influencing or urging individuals to do something, regardless of whether they personally want to or not [28]. It can be argued that peers not following ISPs will cause other employees to break the rules and diminish the effect of nudge messages towards ISP compliance, leading to the following hypotheses:

H3: The perceived peer pressure from colleagues to deviate from the ISP will negatively impact employees' ISP compliance behavior.

H4a: The perceived peer pressure from colleagues to deviate from the ISP will weaken the impact of the System 1 nudge strategy on employees' ISP compliance.

H4b: The perceived peer pressure from colleagues to deviate from the ISP will weaken the impact of the System 2 nudge strategy on employees' ISP compliance.

H5: The perceived peer pressure from colleagues to deviate from the ISP will weaken the impact of the combined nudge strategy on employees' ISP compliance.

Figure 1 presents the proposed research model.

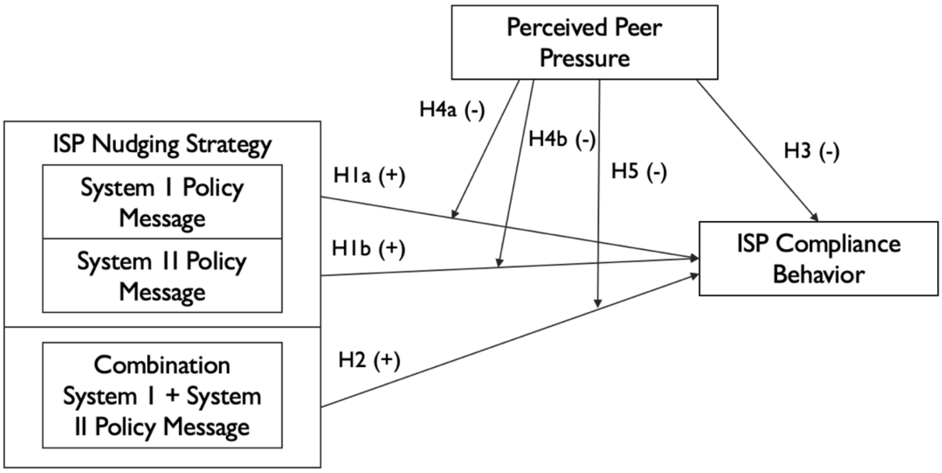
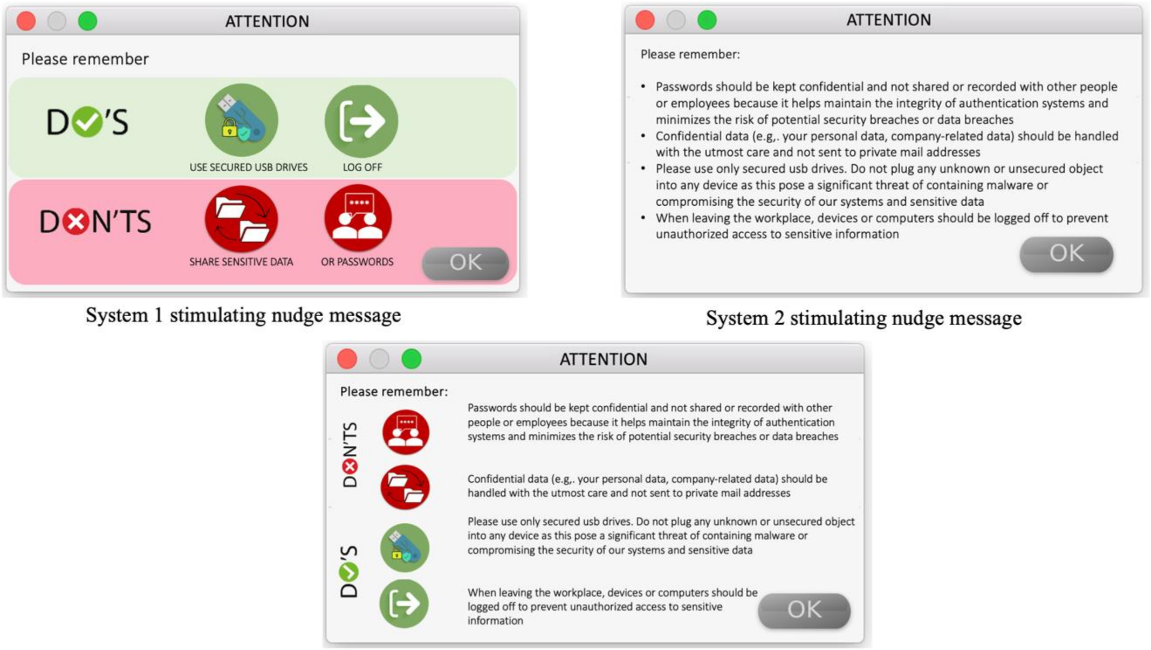


Figure 1: Research Model

4. Methodology

To test the proposed model, a four-condition between-subjects design will be applied in an online experiment where ISP compliance will be measured through an in-basket task. Participants will be required to respond to incoming mails from fictive colleagues, assessing their compliance behavior. An in-basket task with emails provides a realistic simulation of employees' work environment, allowing researchers to assess compliance behavior in authentic scenarios [29]. Emails, being a common communication mode in organizations, offer a relevant context for measuring ISP compliance. The design for this email task will follow [13], [30], [31]. For evaluation, a binary coding scheme will be used, assigning a value of "0" for non-compliance and "1" for compliance. The design of the ISP nudge messages is based on the approaches of [18], [32],

[33] and will appear right before participants start with their task. Perceived peer pressure will be assessed using a 7-point Likert scale ranging from 1="strongly disagree" to 7="strongly agree". The specific items, as well as the complete in-basket task, are currently under development and will be presented in a future research paper. A potential challenge in this study is the power of the nudge message, which needs to be strong enough to interfere across multiple mails. Therefore, a pilot study will be carried out first. To conduct data analysis and test the proposed research model, H1a/b will be evaluated using unpaired t-tests while H2 will be assessed with a one-way ANOVA. Hypotheses 3 to 5 will be tested using structural equation modelling (SEM) with the software SmartPLS.



System 1 stimulating nudge message

Please remember:

- Passwords should be kept confidential and not shared or recorded with other people or employees because it helps maintain the integrity of authentication systems and minimizes the risk of potential security breaches or data breaches
- Confidential data (e.g,. your personal data, company-related data) should be handled with the utmost care and not sent to private mail addresses
- Please use only secured usb drives. Do not plug any unknown or unsecured object into any device as this pose a significant threat of containing malware or compromising the security of our systems and sensitive data
- When leaving the workplace, devices or computers should be logged off to prevent unauthorized access to sensitive information

System 2 stimulating nudge message

Please remember:

Passwords should be kept confidential and not shared or recorded with other people or employees because it helps maintain the integrity of authentication systems and minimizes the risk of potential security breaches or data breaches

Confidential data (e.g,. your personal data, company-related data) should be handled with the utmost care and not sent to private mail addresses

Please use only secured usb drives. Do not plug any unknown or unsecured object into any device as this pose a significant threat of containing malware or compromising the security of our systems and sensitive data

When leaving the workplace, devices or computers should be logged off to prevent unauthorized access to sensitive information

Combined nudge message

Figure 2: Nudge Message Designs

5. Conclusion

In conclusion, this study aims to investigate the effectiveness of different nudging strategies in enhancing employees' ISP compliance behavior. Building upon the dual-process theory, which suggests that individuals' decision-making can be influenced by both intuitive (System 1) and reflective (System 2) processes, the study explores the impact of System 1 and System 2 digital nudge messages on employees' ISP compliance behavior. A potential challenge in this study is the power of the nudge message, which needs to be strong enough to interfere across multiple mails. By examining the individual and combined effects of visual and textual nudges, the study seeks to provide insights into the mechanisms through which these nudges influence employees' cognitive processes. The findings of this study will contribute to the understanding of behavioral interventions in the context of information security. Ultimately, the study aims to advance knowledge in the field and provide practical recommendations for organizations seeking to improve their employees' adherence to information security policies.

References

[1] M. Warkentin and R. Willison, “Behavioral and policy issues in information systems security: The insider threat,” Eur. J. Inf. Syst., vol. 18, no. 2, pp. 101–105, 2009, doi: 10.1057/ejis.2009.12.

[2] R. Willison and M. Warkentin, “Beyond deterrence: An expanded view of employee computer abuse,” MIS Q. Manag. Inf. Syst., vol. 37, no. 1, pp. 1–20, 2013, doi: 10.25300/MISQ/2013/37.1.01.

[3] D. Ormond, M. Warkentin, and R. E. Crossler, “Integrating cognition with an affective lens to better understand information security policy compliance,” J. Assoc. Inf. Syst., vol. 20, no. 12, pp. 1794–1843, 2019, doi: 10.17705/1jais.00586.

[4] H. Cavusoglu, B. Mishra, and S. Raghunathan, “A model for evaluating IT security investments,” Commun. ACM, vol. 47, no. 7, pp. 87–92, 2004, doi: 10.1145/1005817.1005828.

[5] J. D’Arcy and P. B. Lowry, “Cognitive-affective drivers of employees’ daily compliance with information security policies: A multilevel, longitudinal study,” Inf. Syst. J., vol. 29, no. 1, pp. 43–69, 2019, doi: 10.1111/isj.12173.

[6] H. Li, J. Zhang, and R. Sarathy, “Understanding compliance with internet use policy from the perspective of rational choice theory,” Decis. Support Syst., vol. 48, no. 4, pp. 635–645, 2010, doi: 10.1016/j.dss.2009.12.005.

[7] G. D. Moody, M. Siponen, and S. Pahnila, “Toward a unified model of information security policy compliance,” MIS Q. Manag. Inf. Syst., vol. 42, no. 1, pp. 285–311, 2018, doi: 10.25300/MISQ/2018/13853.

[8] K. Masuch, S. Hengstler, S. Trang, and A. B. Brendel, “Replication Research of Moody, Siponen, and Pahnila’s Unified Model of Information Security Policy Compliance,” AIS Trans. Replication Res., vol. 6, no. 13, pp. 1–16, 2020, doi: 10.17705/1atrr.00056.

[9] J. D’Arcy and T. Herath, “A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings,” Eur. J. Inf. Syst., vol. 20, no. 6, pp. 643–658, 2011, doi: 10.1057/ejis.2011.23.

[10] J. D’Arcy, T. Herath, and M. K. Shoss, “Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective,” J. Manag. Inf. Syst., vol. 31, no. 2, pp. 285–318, 2014, doi: 10.2753/MIS0742-1222310210.

[11] S. Trang and B. Brendel, “A Meta-Analysis of Deterrence Theory in Information Security Policy Compliance Research,” Inf. Syst. Front., vol. 21, no. 6, pp. 1265–1284, 2019, doi: 10.1007/s10796-019-09956-4.

[12] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, “Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness,” MIS Q. Manag. Inf. Syst., vol. 34, no. 3, pp. 523–548, 2010.

[13] L. Jaeger and A. Eckhardt, “When colleagues fail: Examining the role of information security awareness on extra-role security behaviors,” 26th Eur. Conf. Inf. Syst. Beyond Digit. - Facet. Socio-Technical Chang. ECIS 2018, 2018.

[14] S. Hengstler, S. Kuehnel, K. Masuch, I. Nastjuk, and S. Trang, “Should I Really do That? Using Quantile Regression to Examine the Impact of Sanctions on Information Security Policy Compliance Behavior,” Comput. Secur., vol. 133, p. 103370, 2023, doi: 10.1016/j.cose.2023.103370.

[15] M. Mirbabaie, J. Marx, and J. Germies, “Conscious Commerce-Digital Nudging and Sustainable E-commerce Purchase Decisions,” Australas. Conf. Inf. Syst., pp. 1–11, 2021.

[16] K. E. Stanovich and R. F. West, “"Individual differences in reasoning: Implications for the rationality debate?,” Behav. Brain Sci., vol. 26, no. 4, p. 527, 2003, doi: 10.1017/S0140525X03210116.

[17] D. Kahneman, “A Perspective on Judgment and Choice: Mapping Bounded Rationality,” Am. Psychol., vol. 58, no. 9, pp. 697–720, 2003, doi: 10.1037/0003-066X.58.9.697.

[18] P. L. Moravec, A. Kim, and A. R. Dennis, “Appealing to sense and sensibility: System 1 and system 2 interventions for fake news on social media,” Inf. Syst. Res., vol. 31, no. 3, pp. 987–1006, 2020, doi: 10.1287/ISRE.2020.0927.

[19] J. S. B. T. Evans and K. E. Stanovich, “Dual-Process Theories of Higher Cognition: Advancing the Debate,” Perspect. Psychol. Sci., vol. 8, no. 3, pp. 223–241, 2013, doi: 10.1177/1745691612460685.

[20] J. S. B. T. Evans and J. Curtis-Holmes, “Rapid responding increases belief bias: Evidence for the dual-process theory of reasoning,” Think. Reason., vol. 11, no. 4, pp. 382–389, 2005, doi: 10.1080/13546780542000005.

[21] J. S. B. T. Evans, “Dual-processing accounts of reasoning, judgment, and social cognition,” Annu. Rev. Psychol., vol. 59, pp. 255–278, 2008, doi: 10.1146/annurev.psych.59.103006.093629.

[22] J. Wisdom, J. S. Downs, and G. Loewenstein, “Promoting Healthy Choices : Information versus Convenience Author (s): Jessica Wisdom , Julie S . Downs and George Loewenstein Published by : American Economic Association Stable URL : https://www.jstor.org/stable/25760210 REFERENCES Linked references a,” Am. Econ. J. Appl. Econ., vol. 2, no. 2, pp. 164–178, 2010.

[23] A. Antinyan and Z. Asatryan, “Nudging for Tax Compliance: A Meta-Analysis,” SSRN Electron. J., no. 8500, 2021, doi: 10.2139/ssrn.3680357.

[24] R. van Bavel, N. Rodríguez-Priego, J. Vila, and P. Briggs, “Using protection motivation theory in the design of nudges to improve online security behavior,” Int. J. Hum. Comput. Stud., vol. 123, no. September 2018, pp. 29–39, 2019, doi: 10.1016/j.ijhcs.2018.11.003.

[25] V. Zimmermann and K. Renaud, “The nudge puzzle: Matching nudge interventions to cybersecurity decisions,” ACM Trans. Comput. Interact., vol. 28, no. 1, 2021, doi: 10.1145/3429888.

[26] K. Hartwig and C. Reuter, “Nudge or restraint: How do people assess nudging in cybersecurity - A representative study in germany,” ACM Int. Conf. Proceeding Ser., pp. 141–150, 2021, doi: 10.1145/3481357.3481514.

[27] I. Kirlappos, S. Parkin, and M. A. Sasse, “Learning from ‘Shadow Security:’ Why Understanding Non-Compliant Behaviors Provides the Basis for Effective Security,” USEC’14 Work. Usable Secur., no. February, 2014, doi: 10.14722/usec.2014.23007.

[28] D. R. Clasen and B. B. Brown, “The multidimensionality of peer pressure in adolescence,” J. Youth Adolesc., vol. 14, no. 6, pp. 451–468, 1985, doi: 10.1007/BF02139520.

[29] D. S. Kiker and S. J. Motowidlo, “Main and interaction effects of task and contextual performance on supervisory reward decisions,” J. Appl. Psychol., vol. 84, no. 4, pp. 602–609, 1999, doi: 10.1037/0021-9010.84.4.602.

[30] M. Siponen and A. Vance, “Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations,” MIS Q. Manag. Inf. Syst., vol. 34, no. 3, pp. 487–502, 2010.

[31] S. Trang and I. Nastjuk, “Examining the role of stress and information security policy design in information security compliance behaviour: An experimental study of in-task behaviour,” Comput. Secur., vol. 104, p. 102222, 2021, doi: 10.1016/j.cose.2021.102222.

[32] C. Schneider, M. Weinmann, and J. Vom Brocke, “Digital nudging: Guiding online user choices through interface design Designers can create designs that nudge users toward the most desirable option,” Commun. ACM, vol. 61, no. 7, pp. 67–73, 2018, doi: 10.1145/3213765.

[33] T. Mirsch, C. Lehrer, and R. Jung, “Making digital nudging applicable: The digital nudge design method,” Int. Conf. Inf. Syst. 2018, ICIS 2018, no. 2009, pp. 1–16, 2018.