

An Investigation on Users' In-group Password Reuse Behavior

Early stage paper

Botong Xue
Kennesaw State University
Bxue1@kennesaw.edu

Zhenya Tang
University of Northern
Colorado
Robin.Tang@unco.edu

Feng Xu
University of Michigan-
Dearborn
fengxu@umich.edu

Xin (Robert) Luo
The University of New
Mexico
xinluo@unm.edu

ABSTRACT

Password reuse has long been a significant concern for users' information security in daily life. This research shifts the focus from general password reuse behavior to a specific type known as in-group password reuse, which involves the use of identical passwords across accounts perceived by users as belonging to the same category. Through a mixed-method research design, this study aims to elucidate the critical factors and antecedents of in-group password reuse. This approach includes sequential qualitative interviews (phase 1) and a quantitative online survey (phase 2). The findings are expected to contribute to the literature on information security and inform users' security practices.

Keywords

Information security, password reuse, account similarity, cognitive load

INTRODUCTION

In the modern digital era, the proliferation of online services has necessitated the management of an increasing number of passwords by users. This has led to the widespread and concerning practice of password reuse, where individuals utilize identical or similar passwords across multiple platforms. Studies reveal that in modern society, an individual holds 30 accounts on average, and a substantial proportion of users engage in password reuse behavior among those accounts despite the well-documented risks and the availability of alternative security measures, such as password managers and multi-factor authentication (MFA) (Florêncio & Herley, 2007; Das et al., 2014). The implications of password reuse are profound and far-reaching. High-profile data breaches demonstrate the cascading effects of compromised credentials across services, leading to significant financial losses, identity theft, and erosion of user trust. 1997 incidents were occurred in the past year, and a good portion of them were happened due to poor password security (Verizon, 2024). Attack vectors such as credential stuffing, where attackers exploit reused credentials to gain unauthorized access to multiple accounts, have become increasingly prevalent and sophisticated (Haq & Shiple, 2019).

Despite the critical nature of this issue, there remains a significant gap in understanding the full scope of password reuse behaviors and the efficacy of current mitigation strategies. Extensive research has put effort into investigating users' password reuse behaviors, and underscores the prevalence of password reuse. As attention has been paid to the user's password reuse behavior, much of the existing research has treated such behavior as a simple and one-dimensional behavior but ignored the complexity and variety of such misbehavior. For example, research has investigated different situational and dispositional factors that motivate individual password reuse behavior, such as protection motivation, personal traits, potential consequences,

neutralization, and so on (Aiswarya, et al., 2022); however, considering the complexity of behaviors, there is lack of research to further discuss the different types of reuse behavior.

To address this research gap, this paper aims to explore a specific type of password reuse behavior, referred to as "in-group password reuse behavior." This behavior is defined as the practice of reusing passwords across accounts that users perceive as similar. The perceived similarity can be assessed across multiple dimensions, which will be elaborated upon in subsequent sections. The primary objective of this research is to scrutinize this unique behavior and investigate the factors that motivate individuals to engage in it within their everyday contexts. Specifically, this study seeks to answer the following research questions:

RQ1: What are the underlying reasons for users engaging in in-group password reuse behavior?

RQ2: Which factors are critical in motivating users' in-group password reuse behavior?

To achieve a comprehensive understanding of this behavior, this study employs a multi-study mixed-method research approach that incorporates sequential qualitative and quantitative studies including multiple semi-structured interviews, and an online cross-sectional survey. The methodology section will provide an in-depth explanation of this research design. As this research is ongoing, the qualitative phase has been completed, culminating in a developed research model and hypothesis. The quantitative phase will be conducted in the near future.

The remainder of the paper is structured as follows: a comprehensive review of existing literature on password reuse behavior is presented, followed by a detailed exposition of the research design. The research model and hypotheses developed from the qualitative phase are introduced. Finally, the paper outlines the future research plan, anticipated contributions, and limitations of the study.

LITERATURE REVIEW

Password reuse has been recognized as a significant information security misbehavior for several decades, attracting considerable research attention. Wash et al. (2016) examined the association between password types and password reuse. Ur et al. (2015) explored password composition and creation behaviors in a laboratory setting. Shay et al. (2010) investigated users' password creation and reuse behaviors through the lens of user attitudes. Das et al. (2014) analyzed the risks and consequences of password reuse from an attacker's perspective, identifying password types and transformation methods that pose security risks.

Additional research has explored various dimensions and aspects of password reuse. For instance, Stobert and Biddle (2018) focused on the password lifecycle, while Hanamsagar et al. (2019) examined bad password behavior and habits. Hanamsagar et al. (2016) also addressed the issue of password fatigue. Aiswarya et al. (2022) considered the impact of different personal traits on password reuse. Seitz et al. (2017) investigated differences in password policies, Woods and Siponen (2019) focused on password memorability, and Jenkins et al. (2014) studied monitoring and real-time warnings. Overall, these studies provide a comprehensive overview of the multifaceted nature of password reuse and its implications for information security.

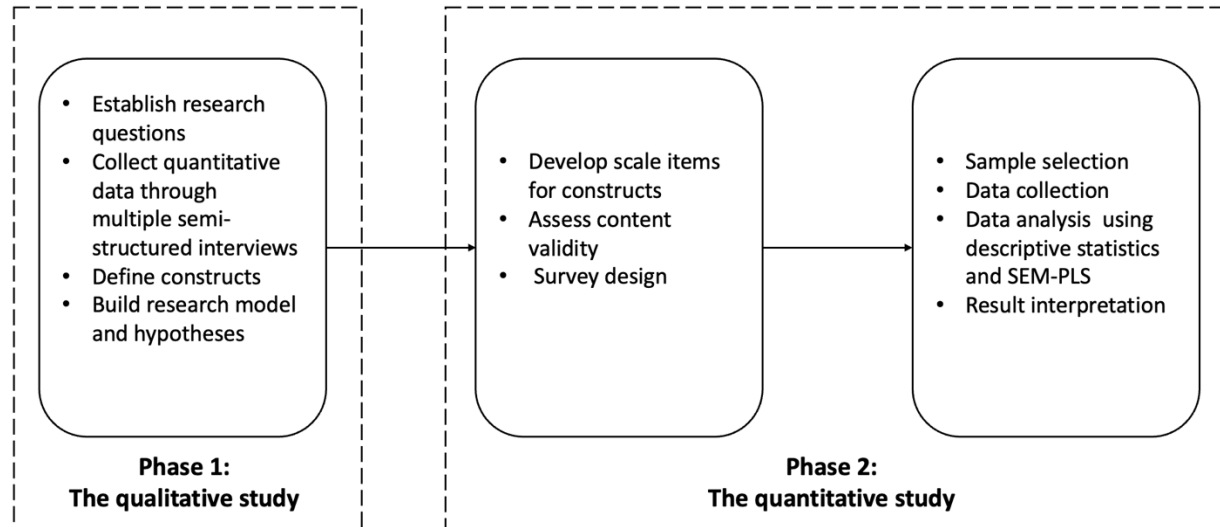
In this research, rather than examining general password reuse behavior, we specifically focus on the password reuse behavior that occurs among accounts perceived as similar by users, termed in-group password reuse behavior. To provide a comprehensive understanding of this behavior and address the research questions, we employed a two-phase mixed-method research approach. The details of the research design are presented in the following section.

METHOD

This research applied a mixed-methods design, which combined a qualitative interview and quantitative cross-sectional survey method to develop a deeper insight into the interest field (Harrison & Reilly, 2011; Venkatesh et al., 2013; Venkatesh et al., 2016). According to Venkatesh et al. (2016), mixed-methods design provides three benefits, including the ability to “address confirmatory and explanatory research questions,” to “provide stronger inferences than a single method or worldview,” and to “produce a greater assortment of divergent and/or complementary views”. In the context of information security policy compliance, it is especially useful to adopt the mixed-method research design since the technology and related security problems change frequently and it is difficult to draw insight from the current theoretical framework and perspective. Given the purpose of this research and the research questions, the mixed-method design is a good fit for our study.

In this research, we paid attention to the in-group password reuse behavior with its associated factors. To better investigate such behavior under an information security context, we followed a developmental process and conducted a qualitative study first, which revealed the factors that influence in-group password reuse behavior in information security from an interpretive perspective, and conducted a second quantitative study by adopting the positivist perspective in order to test the research model and developed hypotheses. Overall, the mixed-methods design was divided into two phases in this research, and influenced by the contextual research study guideline (Pluye & Hong, 2014). In the first phase, we conducted semi-structured interviews with individual organizational employees to identify factors associated with in-group password reuse behavior and performed data analysis to help build our research model for the

following quantitative study. In the second phase, a quantitative cross-sectional study will be conducted subsequently to test the research model in order to have a better understanding of the target phenomenon.



Phase 1: The qualitative phase (study 1)

Data Collection

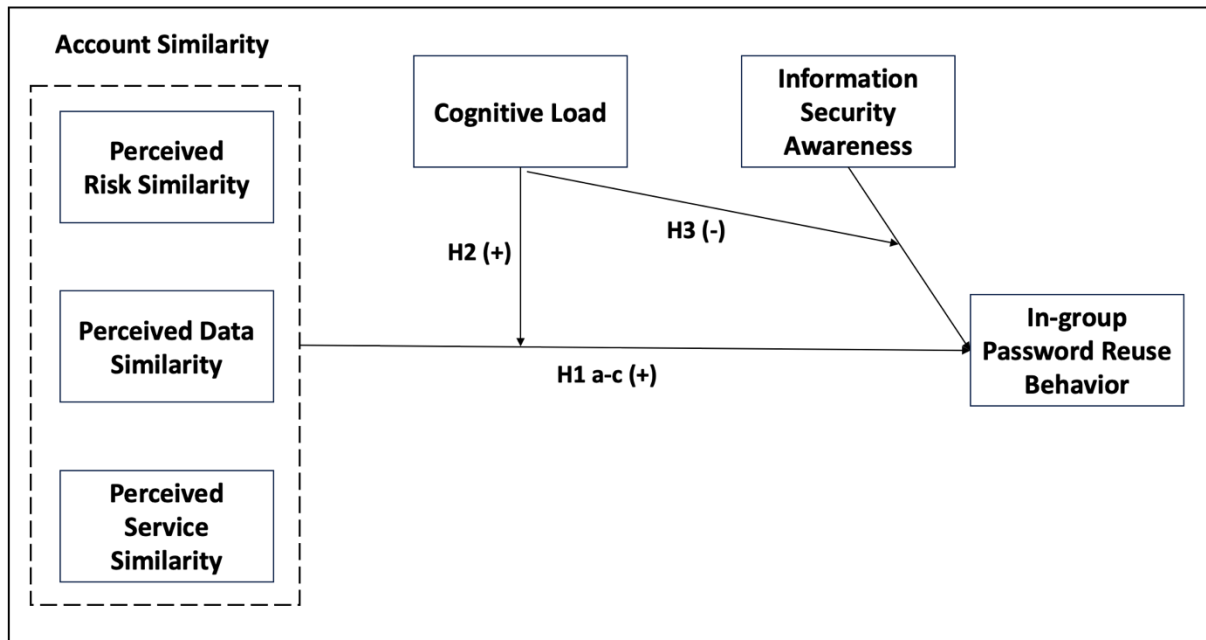
In this phase, we conducted 14 semi-structured and open-ended interviews with full-time employees between May 2024 to June 2024. The researcher of this study played the role of a “neutral outside researcher” (Walsham, 1995). We used a snowball technique to recruit participants once the initial interviews were finished, and all 14 interviewees were from different professions, including college faculty, data analyst, government staff, IS major student, retailing operation manager, etc. Although their professional background varies, they all mentioned that they hold multiple accounts at the same time, and have password reuse behavior at different levels during the interview. The purpose of this phase is to gain more insight into password reuse

behavior, especially the in-group password reuse behavior under daily settings, and the last several interviews did not provide any new radical insight into the phenomena, where the theoretical saturation was met, the number of participants was considered as sufficient in the current stage (Hennink, 2017). Therefore, we stopped the interview process at the number of 14. Interviews were carried out through both online communication software and in-person conversation. All interviews lasted approximately 20 – 30 minutes and were either audiotaped or recorded and subsequently transcribed by the first author of this research within 24 hours (Eisenhardt, 1989). During the interview, the interviewer also took notes as supplemental materials. As interviews were semi-structured and open-ended, we divided questions into three folds: job description, password reuse behavior, and specifically focusing on in-group password reuse behavior and experience. Before the interview, consent about personal information and interview content privacy was sent to each participant, and all the necessary information about the interview and research was well acknowledged by all interviewees.

Data Analysis

To analyze the collected data, we followed Corbin and Strauss (2014) and conducted a multi-step data analysis process. First of all, we conducted the initial coding in order to break down the transcript into meaningful discrete parts. Afterward, we conducted axial coding and found logical connections between the results from the first step. Finally, we conducted the selective coding and identified the themes that connected all the codes, and summarized the essence of interview research. Key codes, categories, and themes were identified through this analysis process, which was repeated until no more additional themes could be identified (Charmaz 2006). After the coding process, we identified four critical factors that uniquely contribute to users' in-

group password reuse behavior. The first three revealed variables that were repetitively mentioned during several interviews are about the assessment of accounts, including the potential risk assessment, service type assessment, and input information assessment when those accounts and passwords were created. We also revealed the role of cognitive load as the fourth that influences users' in-group password reuse behavior. For example, participants mentioned "I will evaluate the risk of the system being compromised. That being said if I use the password for the financial institute, I won't use that password in a low-trust system or website like Spotify or Facebook or something, I would try to, you know, I tried to isolate the different passwords from highly trusted system to those low trusted system." People also mentioned that "I actually use the same password for all of them for the same category because I feel it's impossible for human pain to remember, you know, people who have may have access to multiple data sort of website every day. So I use the same password." "...I do have a lot of knowledge about cybersecurity and reusing the password. But it's just impossible to use different passwords on every single website. So, I try to diversify my password. But I think eventually I have to limit them into like a handful of different passwords based on the category of the system, right?" Other participants also concluded that "If I conclude this a conversation so far, it's more about the perception of the risk, or the security of the account..., and my trust in the company's cybersecurity practices as well". Overall, five variables were revealed from the data analysis, and we developed a research model and hypotheses based on the result of data analysis in phase one.



Hypothesis development

The direct effect of perceived accounts similarities

The first three hypotheses proposed that users will assess different accounts in three dimensions, including the potential risk, the type of data need to be provided, and the service type when the accounts are created, especially when deciding whether to use the same password as the other accounts that in the similar level of evaluation. During the interview, multiple participants repetitively mentioned that they would briefly evaluate the potential risk of information loss and data breach in the new accounts, along with the consequences in order to determine the password and password patterns. When the risk among accounts is evaluated as similar or at the same level, users tend to assign the same password for the accounts in the same group.

In addition, according to protection motivation theory (PMT), individuals will evaluate different aspects of security risk and protection behavior, including the threat appraisal and coping

appraisal in order to determine whether to perform suggested protection behavior (Herath & Rao, 2009; Bulgurcu et al., 2010). Along with the theoretical framework, when individuals are creating passwords for new accounts, they will evaluate the risk of being compromised on the service provider/APP/website based on various cues and evidence, categorize it into different groups, and assign different passwords among groups as an information security protection behavior, comparing to reuse password everywhere.

In addition, participants indicated that the type of information and data that need to be provided and used in the Apps/service/website is another important aspect that needs to be evaluated when the password is created. Multiple people highlighted the type of data is a critical concern when their personal identity data, financial data, and other sensitive data is required, “my standard is that if anything related to my you know, identity information and then there's something I need to pay attention and if the level of personal information involves some like financial data or social security number, then I will consider that is the that's the most important systems.” Previous research has paid enormous attention to personal identity privacy and security, and indicated personal identity data security privacy and security are listed as top concerns when people interact with the internet (Beldad et al., 2011; Belanger & Carter, 2008; Pavlou, 2003; Milne et al., 2004). Therefore, when passwords are created, users will evaluate and categorize the accounts by the data type and the sensitivity level since the account will be considered as in the same security level under a similar security risk, and use the same password within the group. In addition, participants also categorize the account based on the service type, such as government, school, financial institution, or social media accounts because the service/app/website in a similar group is perceived to use the same type of data and under the similar security risk, hence use the same

password in the same group as well. Based on the evidence and argument above, we proposed the following hypotheses:

H1a: Perceived risk similarity among accounts is positively associated with in-group password reuse behavior.

H1b: Perceived data similarity among accounts is positively associated with in-group password reuse behavior.

H1c: Perceived service similarity among accounts is positively associated with in-group password reuse behavior.

The moderating effect of cognitive load

Besides the similarities among accounts that will be evaluated while the password is created, another critical factor to users' in-group password reuse behavior is cognitive load, which refers to the information processing ability of a human being with working memory and storage memory (Sweller, 1988). In the past decade, the role of cognitive load has been investigated in users' password reuse and choice behavior literature. According to cognitive load theory (CLT), information processing demands significant "mental energy" (Feinberg & Murphy, 2000), where researchers argued that creating, using, and remembering unique passwords significantly increased users' cognitive load (Adams & Sasse, 1999; Mujeye et al., 2016; Woods & Siponen, 2019). To mitigate cognitive overload when interacting with multiple passwords, users tend to use weak passwords or reuse passwords among accounts as a coping strategy (Grawemeyer and Johnson, 2011; Zhang et al., 2009).

However, in this research, we argue that the cognitive load does not directly associate with in-group password reuse behavior; instead, it moderates the relationship between the perceived accounts similarities and in-group password reuse behavior. While the number of accounts increases, the cognitive load of remembering different passwords increases accordingly. When users are creating new accounts and assessing the similarities among a great number of existing accounts, the high level of cognitive load will further encourage them to use the same passwords between accounts that share similarities as a mitigating method to reduce the heavy mental load. On the other hand, when the cognitive load is at a lower level, or the number of accounts is relatively few, users' motivation to use the same password in the same group is not as strong as it is at a high level although similarities are addressed among accounts. Hence, we propose that

H2: Cognitive load respectively strengthens the relationships between perceived risk similarity, data type similarity, service similarity, and in-group password reuse behavior.

In addition to the cognitive load's moderation effect on the association between account similarities and in-group password reuse behavior, we argue that the cognitive load will also further weaken the association between information security awareness and in-group password reuse behavior. During the interview, most participants claimed that they have strong information security awareness, and understand the potential risk of using the same password across accounts. In addition, most of them have information security backgrounds and related experiences, which further solidify their self-statement of security awareness. For example, participants mentioned "do have a master's degree, focus on information systems and cybersecurity. So I consider myself a person with an intermediate level of knowledge about information security. My current position

is an IT position in a government organization ... I do have a lot of code of conduct about information security plays, and there are many cybersecurity practices that I need to comply with every in my daily work.” “... At my job I deal a lot with password problems. People getting their accounts hacked Okta, issues with it. Is the authentication multi-factor authentication software we use.”

In the past decades, information security awareness has been tested as an effective variable to strengthen people's information security protection behavior and demotivate their intention of security misbehaviors (Siponen, 2000; Lebek et al., 2014; Bulgurcu et al., 2010; Hwang et al., 2021). However, most participants who have a strong information security awareness in this research performed in-group password reuse behavior, which is also going to put accounts at risk. The top reason for their action is the effort to remember different passwords. For example, they mentioned “I tend to use the same password for everything (note: it is under the context of accounts in the same group). I know it's not good for security, but it's easy for me to remember ...” Another participant also mentioned that “I actually use the same password for all of them for the same category because I feel it's impossible for human beings to remember, you know, people who have may have access to multiple data sort of website every day. So I use the same password.” According to those answers and quotes, the cognitive load significantly diminished the role of information security awareness in terms of security protection. While the security risk is well assessed and acknowledged due to security awareness and knowledge, the mental stress of remembering different passwords still compromised the intention of using different passwords for each account, and the interaction between cognitive load and information security awareness encouraged users to perform in-group password reuse as a weakened security protection behavior.

In other words, while information security awareness has a negative association with in-group password reuse behavior, the presence of cognitive load, especially when the load is at a high level will reduce the association between information security awareness and in-group password reuse behavior. Hence, we proposed the following hypothesis as

H3: Cognitive load negatively moderates the association between information security awareness and in-group password reuse behavior.

FUTURE RESEARCH

Phase 2: The qualitative phase (study 2)

We have developed a research model and hypotheses in Study 1 through multiple semi-structured interviews and data analysis. In our next step, we will perform a qualitative study in order to empirically test our research model and hypotheses through an online cross-sectional survey. Our target participants will be adult internet users in the United States due to the purpose of the research is to investigate individuals' password reuse behavior in the daily setting; therefore, no special requirements are needed, such as skill, occupation, race, gender, etc.. All measurement items will be adopted or well-adapted from previously published works. The measurement model test and structural analysis will be performed while the data collection is finished. In order to mitigate the common method bias, we will perform the mitigation techniques during and after the survey design and data collection (Podsakoff et al., 2003).

Potential contribution and conclusion

In this research, we focused on a unique password reuse behavior, the in-group password reuse behavior, and investigated the critical factors that influence users' decision-making in terms of such behavior. Through this research, we make a contribution to information security literature and users' information security protection practices. To our knowledge, this research is one of the earliest efforts that paid attention to such unique password reuse behavior, hence extending the research stream of information security behavior, and providing an alternative view to understand users' password reuse behavior. In addition, we revealed the antecedents of in-group password reuse behaviors through a mixed-method approach. By revealing the antecedents, we provided a path for future research that is interested in similar behaviors and for users and managers who want to improve account security.

REFERENCES

- Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, 42(12), 40-46.
- Aiswarya, Raveendran, J., & Banahatti, V. (2022, November). Behavioral attributes in password reuse: Analysis of password practices in work and personal spaces. *In Proceedings of the 13th Indian Conference on Human-Computer Interaction* (pp. 1-19).
- Bélanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. *The Journal of Strategic Information Systems*, 17(2), 165-176.
- Beldad, A., De Jong, M., & Steehouder, M. (2011). I trust not therefore it must be risky: Determinants of the perceived risks of disclosing personal data for e-government transactions. *Computers in Human Behavior*, 27(6), 2233-2242.
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 523-548.

- Charmaz, K. (2006). *Constructing grounded theory: A practical guide through qualitative analysis*. sage.
- Das, A., Bonneau, J., Caesar, M., Borisov, N., & Wang, X. (2014, February). The tangled web of password reuse. In *NDSS* (Vol. 14, No. 2014, pp. 23-26).
- Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of Management Review*, 14(4), 532-550.
- Feinberg, S., & Murphy, M. (2000, September). Applying cognitive load theory to the design of web-based instruction. In *18th annual conference on computer documentation. Ipcc sigdoc 2000. Technology and teamwork. Proceedings. IEEE professional communication society international professional communication conference an* (pp. 353-360). IEEE.
- Florêncio, D., & Herley, C. (2007, October). Evaluating a trial deployment of password re-use for phishing prevention. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit* (pp. 26-36).
- Grawemeyer, B., & Johnson, H. (2011). Using and managing multiple passwords: A week to a view. *Interacting with Computers*, 23(3), 256-267.
- Hanamsagar, A., Woo, S., Kanich, C., & Mirkovic, J. (2016). How users choose and reuse passwords. *Information Sciences Institute*.
- Harrison, R. L., & Reilly, T. M. (2011). Mixed methods designs in marketing research. *Qualitative Market Research*, 14(1), 7-26.
- Hennink, M. M., Kaiser, B. N., & Marconi, V. C. (2017). Code saturation versus meaning saturation: how many interviews are enough? *Qualitative Health Research*, 27(4), 591-608.
- Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of information systems*, 18(2), 106-125.
- Hwang, I., Wakefield, R., Kim, S., & Kim, T. (2021). Security awareness: The first step in information security compliance behavior. *Journal of Computer Information Systems*, 61(4), 345-356.
- Jenkins, J. L., Grimes, M., Proudfoot, J. G., & Lowry, P. B. (2014). Improving password cybersecurity through inexpensive and minimally invasive means: Detecting and deterring password reuse through keystroke-dynamics monitoring and just-in-time fear appeals. *Information Technology for Development*, 20(2), 196-213.
- Lebek, B., Uffen, J., Neumann, M., Hohler, B., & H. Breitner, M. (2014). Information security awareness and behavior: a theory-based literature review. *Management Research Review*, 37(12), 1049-1092.

- Milne, G. R., Pettinico, G., Hajjat, F. M., & Markos, E. (2017). Information sensitivity typology: Mapping the degree and type of risk consumers perceive in personal data sharing. *Journal of Consumer Affairs*, 51(1), 133-161.
- Mujeye, S., Levy, Y., Mattord, H., & Li, W. (2016). Empirical results of an experimental study on the role of password strength and cognitive load on employee productivity. *Online Journal of Applied Knowledge Management*, 4(1), 99-116.
- Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce*, 7(3), 101-134.
- Pluye, P., & Hong, Q. N. (2014). Combining the power of stories and the power of numbers: mixed methods research and mixed studies reviews. *Annual Review of Public Health*, 35(1), 29-45.
- Seitz, T., Hartmann, M., Pfab, J., & Souque, S. (2017, May). Do differences in password policies prevent password reuse?. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (pp. 2056-2063).
- Shay, R., Komanduri, S., Kelley, P. G., Leon, P. G., Mazurek, M. L., Bauer, L., ... & Cranor, L. F. (2010, July). Encountering stronger password requirements: user attitudes and behaviors. In *Proceedings of the sixth symposium on usable privacy and security* (pp. 1-20).
- Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8(1), 31-41.
- Stobert, E., & Biddle, R. (2018). The password life cycle. *ACM Transactions on Privacy and Security*, 21(3), 1-32.
- Sweller, J. (1988). Cognitive load during problem solving: Effects on learning. *Cognitive Science*, 12(2), 257-285.
- Ur, B., Noma, F., Bees, J., Segreti, S. M., Shay, R., Bauer, L., ... & Cranor, L. F. (2015). "I Added!" at the End to Make It Secure": Observing Password Creation in the Lab. In *Eleventh symposium on usable privacy and security (SOUPS 2015)* (pp. 123-140).
- Venkatesh, V., Brown, S. A., & Sullivan, Y. (2016). Guidelines for conducting mixed-methods research: An extension and illustration, *Journal of the AIS* (17: 7), 435-495.
- Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS quarterly*, 21-54.
- Verizon. (2024). 2024 Data Breach Investigations Report. <https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf>

Wash, R., Rader, E., Berman, R., & Wellmer, Z. (2016). Understanding password choices: How frequently entered passwords are re-used across websites. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*(pp. 175-188).

Walsham, G. (1995). Interpretive case studies in IS research: nature and method. *European Journal of Information Systems*, 4(2), 74-81.

Woods, N., & Siponen, M. (2019). Improving password memorability, while not inconveniencing the user. *International Journal of Human-Computer Studies*, 128, 61-71.

Zhang, J., Luo, X., Akkaladevi, S., & Ziegelmayer, J. (2009). Improving multiple-password recall: an empirical study. *European Journal of Information Systems*, 18(2), 165-176.