Conceptualizing Mobile Security Mindfulness: A Mixed-Methods Research

Bowen Guan
Business Information Systems, University of Sydney, Sydney, NSW, Australia

Yangting Li
Business Information Systems, University of Sydney, Sydney, NSW, Australia

Carol Hsu[1]
Business Information Systems, University of Sydney,
Sydney, NSW, Australia

ABSTRACT

This paper focuses on conceptualizing a new construct called mobile security mindfulness (MSM) through a mixed-methods design. Individual mindfulness in the context of mobile security threats has not been studied systematically. Developing a context-specific construct in the mobile security domain will contribute to enhancing defense strategies for mitigating mobile security threats (MSTs). Phase 1 of the design is a qualitative interview study to conceptualize MSM. Phase 2 of the design includes a group of quantitative studies to develop and validate a scale for MSM and examine its role in individual behavioral responses to MSTs.

Keywords: Mobile security mindfulness, dynamic trait, mixed-methods research, scale development, multidimensional construct, mobile security threats defense

INTRODUCTION

Mobile security threats (MSTs), a set of InfoSec attacks specifically targeting mobile device users, have increasingly grown more sophisticated with the rise of smartphone use and advancements in artificial intelligence (AI) technologies (Dong et al. 2023). For example, modern phishing attacks have expanded from email in the computing setting to SMS (Smishing), social networking apps, voice communication (Vishing), and QR codes in the mobile device setting (Abbasi et al. 2021). In 2022, over 50% of personal mobile devices globally were

[1] Corresponding author. carol.hsu@sydney.edu.au

exposed to a mobile phishing attack (Lookout 2023). Addressing these emerging MSTs requires defense strategies to evolve beyond traditional computer-based security countermeasures.

The concept of mindfulness in the InfoSec field has drawn great research attention and has become a significant emerging topic in recent years. For example, Jensen et al. (2017) found that mindfulness training is more effective than traditional rule-based training, as mindfulness interventions allow for a more dynamic allocation of human attention during security threat evaluation. Greulich et al. (2024) suggested that mindful employees who trust their organization's security practices are more likely to follow organizational security precautions. Despite evidence of being mindful in detecting InfoSec threats and taking prevention measures, the theoretical understanding of mindfulness as a mobile security-specific individual-level construct remains scarce. This echoes Thatcher et al. (2018)'s research on IT mindfulness, which called for further understanding of individual mindfulness in other promising IS-related contexts and developing its "domain-specific individual-level" measures (p. 832).

Accordingly, we aim to theoretically conceptualize mobile security mindfulness (MSM) and answer the question: *How would an individual's MSM be formed and influence one's behavioral responses to MSTs?* We broadly define MSM as *a conscious mindset in which a person focuses on and is aware of the issues surrounding a mobile security threat* and will follow the guidelines for new construct conceptualization (Compeau et al. 2022) to develop and validate the construct of MSM. Following Venkatesh et al. (2013), a mixed-methods approach is appropriate to our research given the unclear nature of individual MSM and the difficulty of drawing significant insights from existing theories and perspectives.

THEORETICAL BACKGROUND

Mindfulness, first proposed by Langer (1989) at the individual level in psychology, is characterized by *alertness to distinction* (the ability to compare, contrast, and make judgments about similarities and differences), *awareness of multiple perspectives* (the ability to engage in dialectical thinking), *openness to novelty* (the ability to reason with relatively novel stimuli), and *orientation in the present* (the ability to pay more attention to the immediate surroundings).

Mindfulness in IS has gained attention at the organizational level, and been positively linked to organizational IT innovation (Fichman 2004), IS reliability (Butler and Gray 2006), security training (Jensen et al. 2017), and security culture formation in high-reliability organizations (Hassandoust and Johnston 2023). At the individual level, Thatcher et al. (2018) developed IT mindfulness as "an overarching mental mindset driven by individual awareness of the context, and openness to value-adding applications of IT" (p. 832) and demonstrated its role in IT adoption and use. Building on mindfulness's impact on security threat defense (Greulich et al. 2024; Jensen et al. 2017), we argue that a mobile-security mindful individual may be more aware of constantly evolving MSTs, allowing for better protection against MSTs susceptibilities. We aim to systematically develop the concept of MSM in this mixed-methods research.

THE MIXED-METHODS DESIGN

Our mixed-methods design follows Venkatesh et al. (2013) and comprises two phases. Phase 1 involved interviews with individual mobile device users to identify traits of a mobile-security-mindful individual. Phase 2 will focus on developing, validating, and demonstrating the value of an MSM scale, offering significant potential to inform future InfoSec research.

Phase 1: The Qualitative Study

Data Collection & Analysis

Semi-structured interviews, our primary qualitative data source (Walsham 2006), were conducted face-to-face or virtually by three researchers between December 2023 and January

2024. To align with our objective of exploring MSM at the individual level, participant selection criteria (Palinkas et al. 2015) were set as (1) daily mobile device aged from 18 to 60, reflecting the predominant demographic for smartphone and/or tablet ownership, (2) diverse in demographics and professions for broader generalizability (Robinson 2014). A total of 22 interviewees (including five InfoSec experts) from Australia, China, Germany, the UK, and the US, were recruited. The interviews focused on users' routine mobile device usage, security settings on mobile devices, and prior MST experience, with all sessions digitally recorded, transcribed, and collated to ensure data accuracy and completeness.

We drew on the conceptual foundation of mindfulness (Langer and Moldoveanu 2000) to guide our data analysis while also allowing new insights to emerge (Sarker et al. 2018). We iteratively analyzed the data for evidence about the characteristics of a mobile security-mindful individual. Theoretical saturation was reached when associations were made through rigorous iterative analysis alongside the empirical literature (Glaser et al. 1968).

Preliminary Findings

From our qualitative data analysis, we define mobile security mindfulness (MSM) as *a dynamic trait driven by an individual's overarching awareness of MSTs, whereby the mobile device user can stay updated about novel MSTs, adaptively manage mobile device access, and dynamically allocate their attention and efforts to verify and mitigate MSTs*. Specifically, we conceptualized four reflective first-order dimensions of MSM (see Figure 1) detailed as follows.

Sensitivity to Mobile Security Threat (MST) Novelty**:** It refers to an individual's willingness to keep updated and learn about evolving MSTs. For instance, Interviewee #17 stated, "*I am quite sensitive to some new mobile security incidents or novel ways to protect my mobile data. For example, I saw an incident of someone's passwords being breached by a technician when his or* *her phone was sent in for repair [on social media]. It alerted me to learn and use advanced password management ways to protect my password saved on my mobile devices*". This aligns with literature linking novelty seeking to an individual's mindful trait, such as an individual's openness to technology novelty (new features of a technology or a system), which is a significant IT mindfulness trait (Sun et al. 2016; Thatcher et al. 2018). Therefore, these responses were categorized under sensitivity to MST novelty, as a unique trait of being mindful of MSTs.

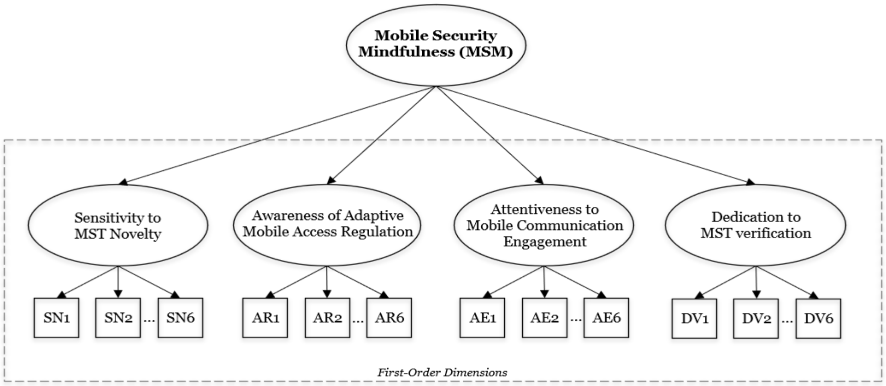
Mobile Security Mindfulness (MSM)
Sensitivity to MST Novelty
Awareness of Adaptive Mobile Access Regulation
Attentiveness to Mobile Communication Engagement
Dedication to MST verification
SN1
SN2
...
SN6
AR1
AR2
...
AR6
AE1
AE2
...
AE6
DV1
DV2
...
DV6
First-Order Dimensions

Figure 1. A Superordinate Second-Order Conceptualization of MSM

Awareness of Adaptive Mobile Access Regulation**:** It refers to the degree to which an individual is aware of regulating their mobile data, internet, or device access to minimize the likelihood of exposure to MSTs. Several participants shared strategies like personalizing their mobile app access, avoiding insecure networks, and preventing shoulder-surfing. For example, Interviewee #3 explained her rationale behind granting access permissions to mobile apps: "*I tend to reject authorization requests that I consider unnecessary for security reasons. I generally decline to allow contact, camera, and microphone access for most apps on my mobile phone*". This aligns with literature indicating that mindfulness involves "forestalling actions" (Jensen et al. 2017, p. 602), enabling individuals' preventative measures before negative consequences occur. Hence, we conceptualized the characteristic of adaptively adjusting and regularly reviewing the mobile access settings to avoid any potential MSTs as one aspect of being mindful of MSTs.

Attentiveness to Mobile Communication Engagement**:** It refers to the degree to which an individual is able to dedicate one's attention when responding to mobile text notifications and phone calls to minimize MST exposure. Our interviews revealed that mobile-security-mindful individuals dynamically allocate attention to sensitive mobile communications, even in distracting situations. For example, Interviewee #11 noted: "*I would not do it [respond to a message] when I am in a meeting because I find it hard to switch my brain... I find it more effective and concentrated when not multitasking, thereby avoiding me making wrong decisions in my mind when responding to some important messages.*" This aligns with literature emphasizing that a mindful individual can "bring one's conscious attention and focus to internal and external experiences occurring in the present moment to respond in a reflective manner" (Jarjoui 2023, p. 2). It applies to the mobile security context, where a mobile-security-mindful user remains attentive and focused during mobile communications to ensure secure responses. Thus, attentiveness to mobile communication engagement is a key dimension of MSM.

Dedication to Mobile Security Threat (MST) Verification**:** It refers to the extent to which an individual is willing to devote efforts to verify the authenticity and legitimacy of mobile communications. Our data showed that mobile-security-mindful individuals possess an awareness of verifying suspicious links or urgent requests on mobile devices. For example, interviewee #7 stated: "*I would not click on any links sent by unknown phone numbers. Even if I see a very official-looking link sent by a seemingly official source, I won't click on it directly. Instead, I prefer to access official channels to verify and complete relevant tasks*". This proactive approach aligns with the mindful trait of continuously scrutinizing distinctions (Langer 1989). Thus, proactively verifying potential MSTs is considered a strong MST mindfulness indicator.

Overall, we identified four dimensions of individual MSM, proposing that users with higher levels of MSM will report higher levels of the four characteristics. Consistent with the conceptualization of IT mindfulness (Thatcher et al. 2018), our MSM is also a superordinate second-order construct with reflective first-order dimensions. In Phase 2, we will validate the multidimensionality of MSM through a quantitative study.

Phase 2: The Quantitative Phase & Future Research Plan

We designed Study 1 to develop and validate our MSM scale. Based on the findings from the qualitative study, we developed a scale for MSM with 5 items for each dimension initially. After several rounds of card-sorting procedure and pilot test, we modified some items to improve clarity and deleted some items loading at less than 0.60 in a principal components analysis with a varimax rotation. Finally, 16 items with satisfactory factor loadings remain (5 items for SN, 4 items for AR and AE respectively, and 3 items for DV). We surveyed 395 mobile phone users worldwide to further test the discriminant and convergent validity (see Table 1) and the multidimensionality of the 16-item MSM scale. A second-order multidimensional model demonstrated a better fit with the data (χ^2=174.336, *d.f.* = 100, CFI = 0.974, RMSEA = 0.043) compared to a unidimensional model (χ^2=1531.917, *d.f.* = 104, CFI = 0.497, RMSEA = 0.187).

Table 1. Construct Means, Standard Deviations, Reliabilities, and Correlation of Constructs

Construct	Mean	S.D.	Cronbach's Alpha	Composite Reliability	AVE	MSM-SN	MSM-AR	MSM-AE	MSM-DV
MSM-SN	4.386	0.832	0.854	0.866	0.564	**0.751**			
MSM-AR	4.066	1.049	0.861	0.864	0.614	0.400	**0.784**		
MSM-AE	4.354	0.836	0.864	0.868	0.623	0.396	0.393	**0.790**	
MSM-DV	4.421	0.865	0.744	0.759	0.513	0.208	0.419	0.275	**0.716**

Currently, we are working on evaluating the dynamic nature of MSM which will be examined through an experiment study (Study 2). We aim to test whether an individual with a higher level of MSM would resist MSTs (e.g., a smishing attack) even in a relatively distracting situation. In the next step, we will run an additional survey study (Study 3) to examine the role of MSM in individual behavioral responses to MSTs and further test the utility of our MSM scale.

Conclusion

Overall, this research systematically conceptualizes individual MSM, develops and validates a scale for MSM, and examines the role of MSM in mitigating MSTs. We believe that our research not only contributes to a domain-specific understanding of individual mindfulness in the context of MSTs defense, but also offers practical implications by providing innovative insights into defense strategies to mitigate increasingly sophisticated mobile security issues.

REFERENCES

Abbasi, A., Dobolyi, D., Vance, A., and Zahedi, F. M. 2021. "The Phishing Funnel Model: A Design Artifact to Predict User Susceptibility to Phishing Websites," *Information Systems Research* (32:2), pp. 410-436.

Butler, B. S., and Gray, P. H. 2006. "Reliability, Mindfulness, and Information Systems," *MIS quarterly* (30:2), pp. 211-224.

Compeau, D., Correia, J., and Thatcher, J. 2022. "When Constructs Become Obsolete: A Systematic Approach to Evaluating and Updating Constructs for Information Systems Research," *MIS quarterly* (46:2), pp. 679-712.

Dong, J., Wang, Y., Lai, J., and Xie, X. 2023. "Restricted Black-Box Adversarial Attack against Deepfake Face Swapping," *IEEE Transactions on Information Forensics and Security* (18), pp. 2596-2608.

Fichman, R. 2004. "Going Beyond the Dominant Paradigm for Information Technology Innovation Research: Emerging Concepts and Methods," *Journal of the Association for Information Systems* (5:8), pp. 314-355.

Glaser, B. G., Strauss, A. L., and Strutzel, E. 1968. "The Discovery of Grounded Theory; Strategies for Qualitative Research," *Nursing Research* (17:4), p. 364.

Greulich, M., Lins, S., Pienta, D., Thatcher, J. B., and Sunyaev, A. 2024. "Exploring Contrasting Effects of Trust in Organizational Security Practices and Protective Structures on Employees' Security-Related Precaution Taking," *Information Systems Research* (0:0), p. null.

Hassandoust, F., and Johnston, A. C. 2023. "Peering through the Lens of High-Reliability Theory: A Competencies Driven Security Culture Model of High-Reliability Organisations," *Information Systems Journal* (33:5), pp. 1212-1238.

Jarjoui, S. 2023. "Mindfulness: The First Line of Defense in Cyberspace." IntechOpen.

Jensen, M. L., Dinger, M., Wright, R. T., and Thatcher, J. B. 2017. "Training to Mitigate Phishing Attacks Using Mindfulness Techniques," *Journal of Management Information Systems* (34:2), pp. 597-626.

Langer, E., and Moldoveanu, M. 2000. "The Construct of Mindfulness," *Journal of Social Issues* (56), pp. 1-9.

Langer, E. J. 1989. *Mindfulness*. Reading, Mass: Addison-Wesley Pub. Co.

Lookout. 2023. "Mobile Threat Landscape Report: 2023 in Review."

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., and Hoagwood, K. 2015. "Purposeful Sampling for Qualitative Data Collection and Analysis in Mixed Method Implementation Research," *Administration and policy in mental health and mental health services research* (42), pp. 533-544.

Robinson, O. C. 2014. "Sampling in Interview-Based Qualitative Research: A Theoretical and Practical Guide," *Qualitative Research in Psychology* (11:1), pp. 25-41.

Sarker, S., Xiao, X., Beaulieu, T., and Lee, A. S. 2018. "Learning from First-Generation Qualitative Approaches in the Is Discipline: An Evolutionary View and Some Implications for Authors and Evaluators (Part 2/2)," *Journal of the Association for Information Systems* (19:9), pp. 909-923.

Sun, H., Fang, Y., and Zou, H. M. 2016. "Choosing a Fit Technology: Understanding Mindfulness in Technology Adoption and Continuance," *Journal of the Association for Information Systems* (17:6), pp. 377-412.

Thatcher, J. B., Wright, R. T., Sun, H., Zagenczyk, T. J., and Klein, R. 2018. "Mindfulness in Information Technology Use: Definitions, Distinctions, and a New Measure," *MIS Quarterly* (42:3), pp. 831–848.

Venkatesh, V., Brown, S. A., and Bala, H. 2013. "Bridging the Qualitative-Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems," *MIS quarterly* (37:1), pp. 21-54.

Walsham, G. 2006. "Doing Interpretive Research," *European Journal of Information Systems* (15:3), pp. 320-330.