Mobile Identity Protection: The Moderation Role of Self-Efficacy

Yasser Alhelaly
NOVA Information Management School, NOVA University Lisbon, Lisbon, Portugal
yalhelaly@novaims.unl.pt

Gurpreet Dhillon
G. Brint Ryan College of Business, University of North Texas, USA
University of KwaZulu-Natal, Durban, South Africa

Tiago Oliveira
NOVA Information Management School, NOVA University Lisbon, Lisbon, Portugal

Abstract

The rapid growth of mobile applications and the associated increased dependency on digital identity raises the growing risk of identity theft and related fraud. Hence, protecting identity in a mobile environment is a problem. This study develops a model that examines the role of identity protection self-efficacy in increasing users' motivation intentions to achieve actual mobile identity protection. Our research found that self-efficacy significantly affects the relationship between users' perceived threat appraisal and their motivational intentions for identity protection. The relation between mobile users' protection, motivational intentions, and actual mobile identity protection actions was also found to be significant. Additionally, the findings revealed the considerable impact of awareness in fully mediating between self-efficacy and actual identity protection. The model and its hypotheses are empirically tested through a survey of 383 mobile users, and the findings are validated through a panel of experts, thus confirming the impact of self-efficacy on an individual's identity protection in the mobile context.

Keywords: Mobile identity protection, identity theft, self-efficacy, threat appraisal, identity protection awareness, mobile context, motivation.

1 Introduction

Mobile security has gained paramount importance, necessitating our diligent efforts to comprehend its implications and develop effective measures for mitigating mobile security risks (Yao et al., 2018). As mobile devices become increasingly prevalent and digital identities more integral, protecting individual mobile identities has become a pressing issue. Furthermore, the growing adoption of mobile applications like mobile banking and digital wallets in recent years has drawn the focus of cybercriminals toward targeting mobile users. A Mastercard study[1] found that 76% of consumers prefer mobile wallets for convenience. Juniper Research[2] predicts over 5.2 billion global digital wallet users by 2026, indicating substantial growth. This potential revenue has led to increased targeting of mobile identities

[1] https://www.mastercard.com/news/press/2021/april/mastercard-new-payments-index-consumer-appetite-for-digital-payments-takes-off/

[2] https://www.juniperresearch.com/press/digital-wallet-users-exceed-5bn-globally-2026

by hackers and fraudsters. According to a 2022 cybercrime report by LexisNexis Solutions[3] , a portentous 75% of potential cyberattacks focus on mobile digital transactions. This trend underscores that hackers are actively aiming at users' mobile identities, particularly in financial transactions, which are perceived as easier and more lucrative. The report's analysis of 35.5 billion mobile financial transactions further reveals a 32% increase worldwide in automated attacks using bots and a remarkable 50% year-over-year rise in human-initiated attacks using social engineering since 2019.

Mobile devices are integrated information systems with unique characteristics. The National Institute of Standards and Technology (NIST) highlights that, unlike PCs, mobile devices have unique characteristics that require diverse security for organizations and individuals, including bringing your own device (BYOD) against various threats (Souppaya & Scarfone, 2013). Similarly, Zambrano & Rafael (2018) emphasized that companies adopting mobile devices in BYOD setups face heightened security threats. While mobile devices share attack vectors with PCs, they are more susceptible to risks like an advanced persistent threat (APT), social engineering, Malware, loss, and theft. These vulnerabilities expose employees to identity theft and data loss, partly due to mobile devices lacking dedicated IT control and their unique characteristics differing from PCs. These characteristics span software and hardware such as small size, mobility, wireless connectivity, local data storage, full-fledged operating systems, web/mobile apps, GPS, sensors, cameras, biometric authentication (Souppaya & Scarfone, 2013), and mobile payment features through near-field communication (NFC) or quick response code (QRC) technologies (Gong et al., 2020).

Despite having diverse security measures compared to PCs, Souppaya & Scarfone (2013) also noted that mobile devices encounter greater vulnerabilities, including limited physical controls due to their size and mobility, utilization of untrusted devices (such as jailbroken or rooted devices), exposure to untrusted networks, usage of location services, and interactions with untrusted apps. In the same line, Wu et al. (2020) reveal limited user app security awareness. Mobile apps often request broad data access, risking malicious access/sharing. Due to poor mobile security awareness, users trust app stores (e.g., Google Play, App Store), granting all apps data access. This aspect leads to ignoring security controls/alerts, which increases security risks and mobile identity threats (Wu et al., 2020).

Recent research in the Information Systems (IS) field has also shown a keen interest in various facets of mobile security. Notably, scholars have delved into topics like security beliefs during mobile shopping (Venkatesh et al., 2017), trust in mobile payment services (Gong et al., 2020), the influence of mobile security notification design on users' security perceptions (Wu et al., 2020), the usability of security features in mobile apps and users' perceptions of security (Sanyal et al., 2021), safeguarding employee security and privacy through enterprise mobile systems (Choudhary et al., 2022), and more recently, the foundational principles for crafting secure mobile health systems (Lin et al., 2023) and the impact of trust and perceived risks in using mobile payments in micro business transactions (Mombeuil, 2023). While existing studies have touched upon various aspects of mobile security, the area of mobile identity protection remains underexplored.

Given the practical and theoretical underpinnings discussed above regarding the problem of mobile identity protection, it becomes evident that with the growing prevalence of mobile

[3] https://risk.lexisnexis.com/insights-resources/research/cybercrime-report

devices, they have become increasingly susceptible to phishing and identity theft attacks. Consequently, mobile users must possess the efficacy to implement diverse security measures to counter these threats effectively (Verkijika, 2019). This dimension is particularly crucial because, despite technological advancements, individuals continue to be targeted as the weakest links in systems and network security (Khando et al., 2021). This determinant highlights the pressing need to motivate individuals to adopt protection measures against technology-related threats (Ogbanufe & Baham, 2023). In this context, the significance of information security awareness emerges as a critical factor in enhancing individuals' protective behaviour (Khando et al., 2021). Therefore, our study aims to delve deeper into this area by employing the protection motivation concepts (Rogers, 1975; 1983) to comprehensively understand the motivational dynamics related to identity protection in mobile environments. Specifically, our study investigates three pivotal concepts. First, individuals' perception of their efficacy in safeguarding their mobile identities. Second, how the perceived threats of identity theft impact individuals' protective behaviour. Third, how security awareness can improve the relationship between self-efficacy and motivational behaviour toward mobile identity protection.

This research makes four contributions. First, we present a mobile identity protection motivation model that combines the self-efficacy theory of motivation and the protection motivation theory. Second, we examine the proposed conceptual model to see how self-efficacy and threat appraisal play a role in individual motivation intentions. Third, we look at how self-efficacy influences both the relationship between threat appraisals and motivational intentions for identity protection among mobile users, as well as the relationship between motivational intentions and actual identity protection. Finally, we scrutinize the mediation impact of protection awareness on the relationship between self-efficacy and actual identity protection. Our initial model is developed from the literature, but we undertook a qualitative phase to evaluate the findings' validity, efficacy, and relevance.

2 Literature and Theoretical Framing

Four bodies of literature inform our research – how individual identity protection is accomplished in mobile environments, the role of self-efficacy in individual mobile identity protection, how individual threat appraisal for mobile identity protection unfolds, and the role awareness plays in explaining mobile identity protection. The following subsections discuss each of the bodies of literature.

2.1 Mobile Identity Protection

How individual identity protection is accomplished in mobile environments is a topic of immense interest. Several scholars have worked on developing measures, defining different conceptualizations of identity, and implications of technological identity on human behaviour. (Carter & Grover, 2015), for instance, examined the everyday use of technology by individuals (e.g., smartphones, Wi-Fi hotspots, social media, etc.) and how such technology use becomes part of an individual's identity. They proposed that the strength of technological identity rests on the degree to which its past enactment is associated with embeddedness. The arguments are based on the original work on identity management by (McCall George & Simmons, 1978; Stryker & Serpe, 1994), and (McCall George & Simmons, 1978; Stets & Cast, 2007). Other scholars have conceptualized identity along similar lines, albeit in different contexts (for instance, see Ogbanufe & Gerhart (2020)). The consensus view of identity, however, gravitates to the degree to which people regard their use of technology as vital to their sense of self as an emergent form of identity.

In the digital world, an individual's identity is constantly exposed to various security threats and cyberattacks, ranging from identity misuse and personal data theft to privilege escalation, social engineering, hacking, security breaches, and identity theft itself (Ogbanufe & Pavur, 2022; Camp, 2004). Among these identity-related threats, identity theft and fraud stand out as the most frequently reported attacks (FTC, 2020). Identity theft involves another person's unauthorized use of digital identity information, leading to the fraudulent acquisition of victims' personal details (Bose & Leung, 2019).

In response to the escalating menace of identity theft, researchers have delved into understanding the nuances of online identity theft and devising innovative countermeasures. These have ranged from email authentication, identification systems (Bose & Leung, 2019), multi-factor authentication (Ogbanufe & Baham, 2023), evoking fear and threats to push individuals toward protecting their identities (Ogbanufe & Pavur, 2022), and enhancing security self-efficacy (Verkijika, 2019).

2.2 Identity Protection Self-Efficacy

Self-efficacy is defined as the expectation that one will be able to act successfully (Bandura, 1997). Self-efficacy has been widely used in IS literature. Scholars have investigated and operationalized self-efficacy in different contexts (Schunk Dale & Pajares, 2009). Notably, it has been employed to probe into topics like executives' decisions to adopt Anti-Malware software in Small and Medium Businesses (Lee & Larsen, 2009), the impact of fear appeals on users' security compliance (Johnston & Warkentin, 2010), the influence of organizational commitment on information asset protection (Posey et al., 2015), situational factors impacting intent to violate information security policies (ISP) (Johnston et al., 2016), cognitive-affective drivers of employees toward ISP compliance (D'Arcy & Lowry, 2019), and mobile technology identity and intentions to use mobile health applications (Balapour et al., 2019). More recently, employees' work productivity and technostress (Loh et al., 2023) and the role of metacognitive skills in developing low-coded applications (Matook et al., 2023).

Most of these studies adopted self-efficacy from the commonly used computer self-efficacy measure by Compeau & Higgins (1995). Yet, Compeau et al. (2022) highlight the need for context-specific IT-related self-efficacy constructs to capture evolving IT phenomena effectively. The IS literature introduces diverse self-efficacy concepts such as deterrence efficacy (Willison & Warkentin, 2013), email screening self-efficacy (Herath et al., 2014), phishing detection self-efficacy (Wang Li & Rao, 2016), privacy self-efficacy (Belanger & Crossler, 2019; Crossler & Bélanger, 2019; Liu et al., 2023; Soh et al., 2022), and security self-efficacy (Silic & Lowry, 2020; Wang et al., 2023). In mobile security, mobile-specific constructs like mobile-computing self-efficacy (Keith et al., 2015), mobile privacy protection self-efficacy (Belanger & Crossler, 2019), and mobile Anti-Phishing Self-efficacy (Verkijika, 2019) emerge. This study suggests mobile identity protection self-efficacy to understand individuals' capabilities in safeguarding mobile identities.

While most studies have looked at how self-efficacy directly affects outcomes, only a few researchers have explored its role in moderating or mediating relationships. For instance, Reychav et al. (2019) examined the reliability of using mobile apps as a point of contact between patients and healthcare providers. Their findings reveal the significant moderation impact of self-efficacy on mobile technology identity and self-report reliability. Similarly, Soh et al. (2022) emphasized how privacy self-efficacy moderates the connection between social capital bridging/bonding and social media addiction. Recently, Yazdanmehr et al. (2023) highlighted the moderation impact of ISP-related self-efficacy on security-related stress (SRS) and coping responses. Hampel et al. (2023) also utilized self-efficacy to improve digital tech attitudes, showing robot-specific self-efficacy mediating vicarious experience and tech enthusiasm.

In the mobile security context, Verkijika (2018) defined self-efficacy as an individual's perception regarding their skills and ability to perform a given security behavior. Verkijika (2019) argues that while security literature acknowledges self-efficacy as a potential tool for preventing security threats, its role in influencing security behaviours has yielded mixed results. Moreover, the shift from desktop to mobile devices in the last years has captured hackers' attention, prompting the need for security research that explores the connection between self-efficacy and other security aspects tailored to the mobile environment. In this study, we conceptualize the self-efficacy concept in the context of mobile security by suggesting identity protection self-efficacy as a key predictor of an individual's motivational intentions toward actual identity protection. We also examine the moderation impact of identity protection self-efficacy on threat appraisal, motivation, intentions, and actual behavior toward mobile identity protection. Table A1 in the appendix summarizes self-efficacy conceptualization in information systems literature.

2.3 Threat Appraisal and Protection Motivation

The third stream of literature delves into individual threat appraisal and its exploration of motivation-behavioural intention toward mobile identity protection. Threat appraisal reflects people's perceptions of their susceptibility to a threat's perceived severity (Chen & Zahedi, 2016). In the context of mobile identity threats, perceived vulnerability relates to how likely someone believes their identity is to be targeted by a theft threat, while perceived severity relates to the perceived seriousness of the potential consequences of that threat. Both vulnerability and severity are factors that contribute to an individual's overall mobile identity threat appraisal and subsequently influence their protective intentions and behaviours toward identity protective measures.

To explain the influence of threat invocations on an individual’s behaviours, Rogers (1975) developed the protection motivation theory (PMT), which examines how people assess threats and the subsequent influence on their behavior. Rogers based his theory on two cognitive processes: threat assessment and handling assessment (Bada & Sasse, 2014). Notably, Ogbanufe & Baham (2023) emphasize the importance of choosing an adequate theoretical framework that aligns with the specific system type and objectives. They argued that while technology adoption and use theories center around systems that improve individual productivity and performance, security systems primarily address the prevention of pain, damage, risks, and threats associated with technologies. In light of this, Ogbanufe & Baham (2023) suggest using PMT for security studies that aim to explore how motivation drives the adoption of protective measures against technology-related threats. Along the same line, the seminal work of Bandura (1978) suggested that the principle of self-efficacy is given a central function in evaluating improvements in fearful and threat avoidance behavior.

Both threat appraisal and self-efficacy have been correlated and used in PMT to study information security behavior (Maddux & Rogers, 1983; Rogers, 1975; Wittee, 1996). Over the years, PMT has become widely employed in information security research to aid in theorizing about individual motivation to change security-related behaviours to protect themselves and their organizations (Boss et al., 2015). Recently, many researchers have deployed PMT to understand the impact of threat appraisal on protection motivation behavior. For instance, Ogbanufe & Pavur (2022) used perceived threats to explore adaptive protection motivation for identity theft protection. However, their study did not investigate the relationship between motivation intentions and actual behavior in mobile identity protection. In this context, Verkijika (2019) emphasizes the significance of examining real protective behaviours to fully comprehend how security intentions translate into actions. In the same vein, Thompson et al. (2017) encourage deploying models of security intentions to extend and examine the link between intentions and actual security behaviours.

Motivated by the backdrop of the preceding arguments and drawing from the framework of the PMT, this study focuses on exploring perceived threat appraisal to gain a deeper understanding of motivational intentions and subsequent actions related to mobile identity protection against threats and attacks. In the upcoming section, we will discuss the role of identity protection awareness in shaping individuals' behaviours and decisions within the realm of mobile security.

2.4 Identity Protection Awareness

Weixun Li et al. (2023) highlighted the crucial role of information security awareness as the linchpin for integrating comprehensive security solutions. Information security awareness is defined as a unified awareness of security threats and countermeasures, functioning as a foundational element for robust security maintenance (Weixun Li et al., (2023). In the information security context, Jaeger & Eckhardt (2021) recommend using awareness of situations to promote personal security behavior. This strategy empowers individuals to effectively promote identity theft protection and security-related actions. In line with this perspective, Khando et al. (2021) emphasized the significant impact of awareness on information security behavior, underscoring its priority in both the research and practice domains. As discussed earlier, this stems from the recognition that humans frequently represent the most vulnerable aspect when it comes to securing systems, especially mobile devices (Khando et al., 2021).

Similarly, Jaeger (2018) noted the evolving nature of research on information security awareness, highlighting the unexplored territories within the field of Information Systems. Despite the proliferation of studies on information security awareness, a comprehensive understanding of its scope and its interactions with other constructs remained lacking (Jaeger, 2018). Given these considerations, our study finds significance in exploring the role of awareness in elucidating actual identity protection behavior within the mobile environment.

In essence, our study aligns with the current stream of research in IS, shedding light on the intricate dimensions of mobile security. By exploring the nexus between self-efficacy, threat appraisal, awareness, and protection motivation, we strive to advance the comprehension of user intentions and actual behavior toward identity protection within the evolving landscape of mobile security. Consequently, recognizing the critical significance of this intersection, we have undertaken a gap analysis to examine the identity protection behavior of individuals in the mobile environment. This gap analysis addresses a pivotal question: What are the lacunae in our understanding of the roles of self-efficacy, threat appraisal, and protection awareness in motivating individuals to achieve mobile identity protection?

Our gap analysis revealed three gaps in the existing literature. First, we discovered that the context of identity protection is often overlooked in mobile security literature. Second, despite a large body of existing research about self-efficacy in the information systems field (please see Table A2 in the appendix), we discovered that the moderation impact of self-efficacy is also underexplored. Finally, the role of protection awareness as a mediator has been overlooked in the extant literature, especially on the relationship between self-efficacy and actual protection behavior. Table A2 in the appendix summarizes the gap analysis for the four bodies of informing literature.

3 Conceptual Model and Hypotheses Development

Two theories inform our conceptualization of mobile identity protection – the self-efficacy theory (Bandura, 1994) and the protection motivation theory (Rogers, 1975). Integrating both theories allows us to enhance the explanatory power of each model (Robert, 2002). Identity protection self-efficacy was drawn from Kim & Kankanhalli (2009). Perceived severity and perceived vulnerability were drawn from Boss et al. (2015), the identity protection motivational intentions construct was based on Taylor & Todd (1995), and identity protection awareness was informed by Bulgurcu et al. (2010). Finally, actual identity protection was based on Pavlou & Fygenson (2006). Figure 1 shows our conceptual research model. We propose that while threat appraisal only has a positive direct effect on mobile identity motivational intents, self-efficacy has both a direct and a moderating effect. Furthermore, we hypothesize that protection awareness serves as a full mediator between self-efficacy in identity protection and actual mobile identity protection.

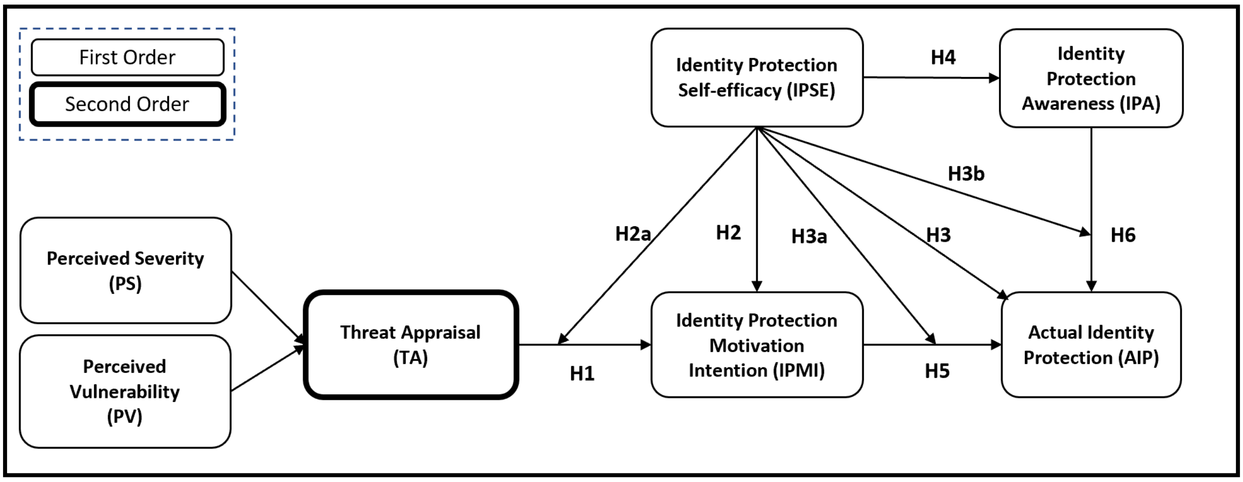
First Order
Second Order
Identity Protection Self-efficacy (IPSE)
H4
Identity Protection Awareness (IPA)
H3b
H2a
H2
H3a
H3
H6
Perceived Severity (PS)
Perceived Vulnerability (PV)
Threat Appraisal (TA)
H1
Identity Protection Motivation Intention (IPMI)
H5
Actual Identity Protection (AIP)

Figure 1. Conceptual motivation model for mobile identity protection

3.1 The Role of Threat Appraisal

The PMT theory was designed to explain how risky behavior can be manipulated and how important it is to understand the components of a motivating message (Rogers, 1975; Rogers, 1983). When faced with a threat, individuals create their perceptions of threat severity and vulnerability (Rogers, 1975; Witte, 1992; Wittee, 1996). Furthermore, fear-inducing persuasive messages are effective in changing people's attitudes, behavioural intent, and actions. Threat appraisal is represented in our model as a second-order reflective-formative type construct. The construct is composed of perceived vulnerability and perceived severity. Perceived vulnerability describes the user's sense of susceptibility to losing mobile personal information, as well as the chance of becoming a victim of identity theft attacks. Perceived severity describes the compromised identity's perceived repercussions due to mobile loss or identity theft attacks. Hence:

H1: *Threat appraisal is a second-order construct of perceived threat appraisal and vulnerability. Threat appraisal positively influences identity protection motivational intentions.*

3.2 The Role of Identity Protection Self-efficacy

Prior research has shown that self-efficacy beliefs are reliable predictors of behavioural outcomes such as performance (Ouweneel et al., 2013) and are positively related to the motivational effects of goals (Bandura & Cervone, 1983). Self-efficacy has proven to be a more consistent predictor of behavioural outcomes than any other motivational construct (Graham & Weiner, 1996). Self-efficacy has been discovered to be a significant predictor of motivational behaviours (Chen & Zahedi, 2016). In this study, we posit that identity protection self-efficacy will affect identity protection motivational intentions, protection awareness, and actual identity protection. Hence:

H2: *Identity protection self-efficacy positively influences identity protection motivational intentions.*

H3: *Identity protection self-efficacy positively influences Actual identity protection.*

H4: *Identity protection self-efficacy positively influences protection awareness.*

We also posit that self-efficacy moderates the relationship between threat appraisal and identity protection motivational intentions, the relationship between identity protection motivational intentions and actual identity protection, and the relationship between identity protection awareness and actual identity protection. Thus:

H2a: *Identity protection self-efficacy negatively moderates the effect of threat appraisal on identity protection motivational intentions.*

H3a: *Identity protection self-efficacy positively moderates the effect of identity protection motivational intentions and actual identity protection.*

H3b: *Identity protection self-efficacy negatively moderates the effect of identity protection awareness on actual identity protection.*

3.3 The Role of Identity Protection Motivational Intentions

Many social psychology researchers employ the theory of expected action (TPB) paradigm to model planned behaviours (Ajzen, 1991). Motivating behavioural intentions measures how hard people are willing to carry out a task. According to TPB, behavioural intention is the most powerful predictor of behaviours; after all, people do what they intend to do (Pavlou & Fygenson, 2006). According to Early & Chaiken (1998), behavioural intentions are a pivotal component in the model relating to the connection between attitudes and behaviours. The immediate cause of conduct is thought to be behavioural intention (Fishbein & Ajzen, 1980). Behavioural intention is a measure of a person's willingness to complete the acts required to attain specific objectives, and it reflects the motivational factors that underpin the actions (Guillon et al., 2004). In the mobile identity protection context, it is therefore critical to measure mobile users' intentions to protect their identity using different protection features such as Face, fingerprint, passwords, or PIN. Hence, we propose the following hypothesis based on the preceding arguments:

H5: *Identity protection motivational intention positively influences actual identity protection.*

3.4 The Role of Identity Protection Awareness

The most significant factor influencing user behavior in terms of steps taken to defend themselves against threats is an individual's awareness (Dhillon & Chowdhuri, 2013; Johnston & Warkentin, 2010). The primary goal of awareness is to raise consciousness and to make people more open to change (Dhillon et al., 2020; Manke & Winkler, 2013). Psychologically, a person who is bombarded with too many warnings and recommendations could be tempted to give up all attempts to defend himself and not be concerned about any threat (Fisher & Rost, 1986). Threatening or intimidating messages are ineffective because they increase the individual's stress level to the point that the individual can become repulsed or deny the existence of any threat (Bada & Sasse, 2014). For the same reason, we found that it is crucial in this study to investigate and measure users' awareness that may influence the actual behavior of protecting their mobile against identity threats. Although smartphones have received considerable attention in the security literature, the relevant studies on the security awareness of mobile identity are currently somewhat limited. Our proposed model includes identity protection awareness not only as a direct predictor of actual identity protection but also as a mediator between the relationship between identity protection self-efficacy and actual identity protection (Kraiger et al., 1993). Therefore, we hypothesize that:

H6: *Identity protection awareness positively influences actual identity protection.*

4 Methods

4.1 Measurement

We first developed our measurement tool and subsequently crafted a questionnaire through the Qualtrics online survey platform. Subsequently, we seamlessly integrated the survey with a Prolific crowdsourcing platform for efficient data collection. Our approach to selecting evaluation items was guided by meticulously considering established constructs within the information systems literature (Bagozzi, 2011). We examined previously validated measures from reputable sources exhaustively to ensure the credibility and relevance of our chosen items. Perceived appraisal items encompassing perceived severity and perceived vulnerability were adopted from Boss et al. (2015). Identity protection self-efficacy items were derived from Kim & Kankanhalli (2009), while identity protection awareness was drawn from Bulgurcu et al. (2010). The measures of identity protection motivation intention were adapted from Taylor & Todd (1995), and finally, the measures of actual identity protection were adopted from Pavlou & Fygenson (2006). By adopting these established measures, we aimed to capture the nuances of each construct accurately, contributing to the overall validity of our research. Finally, a consistent seven-point Likert scale, ranging from 'strongly disagree' to 'strongly agree,' was employed across all measurement items, as illustrated in Table 1.

A panel comprising five experts in Information Systems (IS) was convened to ensure the robustness of our measurement approach for the meticulous evaluation and refinement of our model's content and validity. Among the panel members, two accomplished professionals in the IS security field hold prominent positions. The first individual boasts over two decades of comprehensive experience in information systems, focusing on specialized areas like mobile security and privacy. The second expert, well-versed in information management, contributes a thorough understanding of identity management systems. The remainder of the panel comprises skilled researchers: two Ph.D. students immersed in the nuances of mobile security research and a post-doctoral researcher actively engaged in a research project centered on mobile security and privacy. The panel's expertise spans continents, with the professionals representing the US and the researchers stationed in Europe.

Construct		Items	Instrument	Reference
Threat Appraisal (TA) Second-Order Construct	Perceived Severity (PS)	PS1	If my personal information were stolen from my mobile due to an identity theft attack, I would suffer a lot of pain.	Boss et al. (2015)
		PS2	If my mobile identity were compromised, it would be severe.	
		PS3	If my mobile identity were compromised, it would be serious.	
		PS4	If my mobile identity were compromised, it would be significant.	
	Perceived Vulnerability (PV)	PV1	I am unlikely to lose personal information from my mobile in the future	
		PV2	My mobile is at risk of becoming a victim of identity theft attacks.	
		PV3	My mobile will likely become a victim of an identity theft attack.	
		PV4	My mobile may become a victim of an identity theft attack.	
Identity Protection Self-Efficacy (IPSE)		SE1	Based on my knowledge, skills, and abilities, protecting my mobile identity would be easy for me.	Kim & Kankanhalli (2009)
		SE2	I can protect my mobile identity without the help of others	
		SE3	I can protect my mobile identity reasonably well on my own	
Identity Protection Awareness (IPAW)		IPAW1	Overall, I am aware of the mobile identity threats and their negative consequences.	Bulgurcu et al. (2010)
		IPAW2	I have sufficient knowledge about the cost of potential identity theft problems.	
		IPAW3	I understand the concerns regarding mobile identity protection and the risks they pose in general.	
Identity Protection Motivation Intention (IPMI)		BI1	I intended to protect my mobile identity	Taylor & Todd (1995)
		BI2	I intend to use my mobile using (Face, fingerprint, passwords, or PIN) identity protection features.	
		BI3	I intend to protect my mobile identity frequently.	
Actual Identity Protection (AIP)		AIP1	I expect my mobile identity to be protected when I apply identity protective actions (Strongly disagree/agree)	Pavlou & Fygenson (2006)
		AIP2	Actual protection of my mobile identity information would make it much more (difficult/easier) for me to apply identity-protective actions.	
		AIP3	I feel secure that my personal information is kept private when I protect my mobile identity (Strongly disagree/agree).	
		AIP4	Feeling secure that my mobile identity is protected would make it much more (difficult/easier) for me to apply identity protection actions.	

Table 1. The measurement items

We adopted a structured facilitation approach to mitigate the impact of dominant panel members (O'Sullivan et al., 2015; O'Sullivan et al., 2022), allowing for balanced participation. Anonymous contributions were utilized to ensure unbiased input. Discussion leadership rotated among members, minimizing consistent dominance. We encouraged diverse viewpoints and dissenting opinions to foster inclusive debates. Regular feedback checkpoints ensured everyone's input was considered, maintaining a collaborative environment and preventing undue influence. In response to this panel's insights, we fortified our questionnaire by enhancing item quality in terms of clarity and context. The ensuing questionnaire results not only validated the integrity of our data but also furnished compelling evidence of the instrument's robust validity and reliability.

4.2 Data Collection

Data collection occurred between March and April 2022, facilitated by prolific data collection services. Our approach began with an exploratory pilot involving 80 participants, which yielded valuable insights into the reliability and validity of the employed scales. Building upon the successful pilot, we expanded our sample to encompass 303 additional respondents, resulting in a comprehensive dataset of 383 responses. The online survey, designed to be completed within 10–15 minutes, garnered an average completion time of approximately 12 minutes per participant.

For our sample size, we followed partial least squares structural equation modelling (PLS-SEM) principles and acknowledged the importance of robust analysis (Hair et al., 2014). Considering our scenario, our study encompasses two dependent variables. One of these variables entails three paths (R2= 20.6%), while the other involves five paths (R2= 51.1%). We followed the guidelines of Cohen (1992) for the minimum sample size recommendation to establish the adequacy of our sample size. For significance levels of 5% and R^2 values around 0.25, the recommended minimum sample size is 59 observations. Similarly, for R^2 values around 0.50, the suggested minimum is 42 observations. Notably, our sample size surpasses these thresholds. In this study, we selected 383 responses to increase the precision (i.e., consistency) of PLS-SEM estimations and ensure informed and meaningful results, as well as substantiated inferences (Hair et al., 2021).

Characteristics		Frequency (%)	Respondents (n = 383)	Characteristics		Frequency (%)	Respondents (n = 341)
Gender	Female	48%	185	Educational Degree	No school	3%	11
	Male	52%	198		High School	34%	130
Age	18-24	43%	164		Bachelor	42%	160
	25-44	46%	178		Master	19%	73
	44-68	11%	41		Ph.D.	2%	9

Table 2. Profile of the respondents

Our survey comprised a diverse participant pool, offering insights into our sample's composition. Guided by the Hair et al. (2021) guidelines, our sample size of 383 responses with zero missing values ensured robust statistical power and enhanced estimation precision. Gender distribution was balanced, with 48% females and 52% males. Participants ranged from 18 to 68 years, reflecting varying ages. Educational backgrounds varied, with 34% holding high school degrees, 42% possessing bachelor's degrees, and 21% having post-graduate qualifications. Notably, 3% reported incomplete schooling. Geographically, our participants represented a global presence, with 80% from Europe, 9% from the USA and Canada, and 11% from diverse regions. These characteristics underscore the strength of our statistical methodology, samples' diversity, and amplifying the relevance of our findings within our research context. Table 2 above displays the respondent profile.

Recent work in IS has highlighted the importance of evaluating the influence of common method bias (CMB) on the results of statistical analysis (Chin et al., 2012). CMB occurs when the estimates of the relationships between two or more constructs are biased because they are measured with the same method (Podsakoff & Organ, 1986). We assess CMB with two methods: (1) Harman's one-factor test to identify common method variance (Podsakoff et al., 2003), and (2) the PLS Marker variable approach to analyse data contaminated with method (Lindell & Whitney, 2001). The former confirmed that none of the variables alone accounts for the bulk of the variation. The latter included a potentially unrelated marker variable in the study model, resulting in a maximum mutual variance with other variables of 0.008 (0.8 percent), which is considered a low value (Johnson et al., 2011). As a result, no substantial CMB was discovered.

5 Results of Data Analysis

We used PLS-SEM regression using smart PLS 3.0 to conduct our analysis in this study. The literature has suggested that the approach works best when: 1) the model has never been tested before (Ke et al., 2009), 2) the latent constructs are moulded with formative indicators (Goo et al., 2009), and 3) evaluating path coefficients that are substantially different from zero, it is important to avoid restrictive distributional assumptions (Fornell & Bookstein, 1982).

5.1 Measurement Model

We assessed the construct reliability, convergent validity, indicator reliability, and discriminatory validity of scales for reflective constructs through a measurement model. Given the nature of our approach utilizing PLS analysis, we opted for composite reliability (CR) as our metric for assessing construct reliability. However, it is noteworthy that some researchers may prefer Cronbach's alpha due to its tendency to provide higher reliability estimates. However, a major limitation of Cronbach's alpha is that it assumes all indicator loadings are the same in the population. According to Hair et al. (2021), violating this assumption could result in lower reliability values than those produced by composite reliability. Both constructs provided CR values greater than 0.7 (Table 3), indicating that the constructs were internally consistent and acceptable (Henseler et al., 2009; Straub, 1989). The average variance extracted (AVE) was used to demonstrate convergent validity. All constructs' AVE values are higher than 0.50 (Table 3). As a result, the measurement model's convergent validity is established (Fornell & Larcker, 1981; Hair et al., 2012).

For indication reliability, the loading should be more than 0.7 (Churchill Jr, 1979; Henseler et al., 2009). All loadings in Table 4 are more than 0.7, suggesting that the reliability indicator has been satisfied. We used three criteria to evaluate discriminatory validity: (1) Fornell-Larcker criteria, (2) Cross-loadings, and (3) Heterotrait-Monotrait ratio (HTMT) (Henseler et al., 2015). The Fornell-Larcker criteria assess discriminant validity in structural equation models. It compares the square root of Average Variance Extracted (AVE) with correlations between constructs (Hair et al., 2021). AVE should exceed correlations to ensure distinctiveness. This requirement safeguards against overlapping or redundant constructs and establishes a clear distinction between constructs.

Construct	Mean	SD	CR	IPSE	PV	PS	TA	IPMI	IPA	AIP
Identity protection self-efficacy (IPSE)	4.563	1.472	0.940	**0.916**						
Perceived vulnerability (PV)	3.547	1.194	0.895	-0.290	**0.825**					
Perceived severity (PS)	4.682	1.417	0.936	0.021	0.242	**0.886**				
Threat appraisal (TA)	4.239	1.076	0.865	-0.109	0.628	0.907	**0.676**			
Identity protection mutational intention (IPMI)	5.670	1.128	0.908	0.295	0.013	0.352	0.288	**0.876**		
Identity protection awareness (IPA)	4.821	0.963	0.891	0.282	-0.061	0.308	0.221	0.441	**0.820**	
Actual identity protection (AIP)	5.325	0.946	0.860	0.234	-0.042	0.319	0.238	0.662	0.532	**0.778**

Table 3. Descriptive statistics, correlation, composite reliability (CR), and average variance extracted (AVE)

Construct	items	IPSE	PV	PS	IPMI	IPA	AIP
Identity protection self-efficacy (IPSE)	IPSE1	**0.889**	-0.291	0.008	0.272	0.251	0.218
	IPSE2	**0.926**	-0.261	0.029	0.274	0.260	0.217
	IPSE3	**0.933**	-0.244	0.037	0.264	0.265	0.208
Perceived vulnerability (PV)	PV1	-0.232	**0.756**	0.237	0.041	-0.086	0.012
	PV2	-0.236	**0.881**	0.221	0.010	-0.088	-0.058
	PV3	-0.245	**0.836**	0.173	-0.024	-0.042	-0.070
	PV4	-0.243	**0.822**	0.162	0.013	0.024	-0.020
Perceived severity (PS)	PS1	-0.011	0.184	**0.826**	0.309	0.279	0.291
	PS2	0.041	0.215	**0.908**	0.317	0.304	0.313
	PS3	0.043	0.224	**0.917**	0.324	0.257	0.258
	PS4	-0.002	0.231	**0.889**	0.298	0.252	0.271
Identity protection mutational intention (IPMI)	IPM1I	0.278	0.017	0.362	**0.884**	0.454	0.623
	IPMI2	0.255	-0.016	0.235	**0.811**	0.301	0.494
	IPMI3	0.242	0.027	0.316	**0.929**	0.388	0.609
Identity protection awareness (IPA)	IPA1	0.239	-0.009	0.285	0.389	**0.819**	0.460
	IPA2	0.140	-0.035	0.165	0.332	**0.780**	0.388
	IPA3	0.280	-0.077	0.253	0.374	**0.827**	0.452
Actual identity protection (AIP)	AIP1	0.193	-0.096	0.262	0.487	0.281	**0.758**
	AIP2	0.279	-0.180	0.228	0.512	0.439	**0.769**
	AIP3	0.121	0.062	0.267	0.535	0.329	**0.803**
	AIP4	0.128	0.093	0.309	0.527	0.377	**0.787**

Table 4. Loadings and cross-loadings

Notably, this distinction is established in our model in the case of threat assessment (TA), which operates as a second-order construct comprising perceived vulnerability (PV) and perceived severity (PS). As demonstrated in Table 4, the diagonal elements, representing the square root of AVE for each construct, surpass the correlations between these constructs. This element substantiates the fulfillment of the first criterion for ensuring discriminant validity, as outlined by Fornell & Larcker (1981).

The second criterion is cross-loading, a crucial element for evaluating discriminant validity in structural equation modelling. It involves indicators of one construct loading on other constructs, possibly indicating construct ambiguity (Hair et al., 2021). In this criterion, the loadings (in bold) should be greater than cross-loadings to prove measurement validity (Chin, 1998). Our analysis consistently reveals that loadings (in bold) significantly outperform cross-loadings, as showcased in Table 4. This robust pattern underscores the distinct nature of our indicators, reinforcing the reliability and accuracy of our measurements.

Our third method for evaluating discriminant validity is the Heterotrait-Monotrait (HTMT) ratio of correlations. This approach compares correlations between different constructs to those within the same construct, determining their distinctiveness (Henseler et al., 2009). Table 5 shows that all HTMT values are below the 0.9 threshold, signifying robust discriminant validity. This technique ensures the accurate capture of unique construct variances, reinforcing the measurement model's validity and bolstering confidence in interpreting construct relationships and effects in subsequent analyses.

Construct	IPSE	PV	PS	TA	IPMI	IPA	AIP
Identity protection self-efficacy (IPSE)							
Perceived vulnerability (PV)	**0.333**						
Perceived severity (PS)	0.034	**0.277**					
Threat appraisal (TA)	0.228	**0.922**	**0.928**				
Identity protection mutational intention (IPMI)	0.337	0.035	0.397	**0.295**			
Identity protection awareness (IPA)	0.318	0.089	0.348	0.301	**0.514**		
Actual identity protection (AIP)	0.276	0.171	0.380	0.367	0.807	**0.652**	

Table 5. Heterotrait-Monotrait Ratio (HTMT)
Note. Values in diagonal (bolt) are the AVE square root

We modelled threat appraisal (TA) as a reflective-formative second-order construct (Hair et al., 2012), with reflective perceived severity (PS) and perceived vulnerability (PV). These constructs are TA formative measures. For the formative construct, a measurement model was used to determine multicollinearity, as well as the importance and sign of weights, for the formative build. The variance inflation factor (VIF) statistic is used to assess multicollinearity. Table 6 shows that the VIF values are below the 3.3 mark, implying that the variables are not multicollinear (Lee & Xia, 2010). The two constructs are statistically significant (p 0.01) and have a positive sign. As a result, the structural model can be tested using the formative construct.

Formative construct (second-order construct)	Constructs (first-order reflective)	Weights	VIF
Threat Appraisal (reflective-formative type)	Perceived vulnerability (PV)	0.440***	1.062
	Perceived severity (PS)	0.802***	1.062

Table 6. Formative measurement model evaluation
*Note. *** $p < 0.01$; ** $p < 0.05$; * $p < 0.10$*

5.2 Structural Model

We calculated the multicollinearity of all constructs using the variance inflation factor (VIF). The VIF is 1.062, which is less than the threshold of 3.3, meaning that the variables are not multicollinear (Lee & Xia, 2010). Figure 2 presents that structure model that explains the variation and the path coefficients. Bootstrapping with 5000 resamples was used to determine the statistical significance levels of the hypothesized construct.

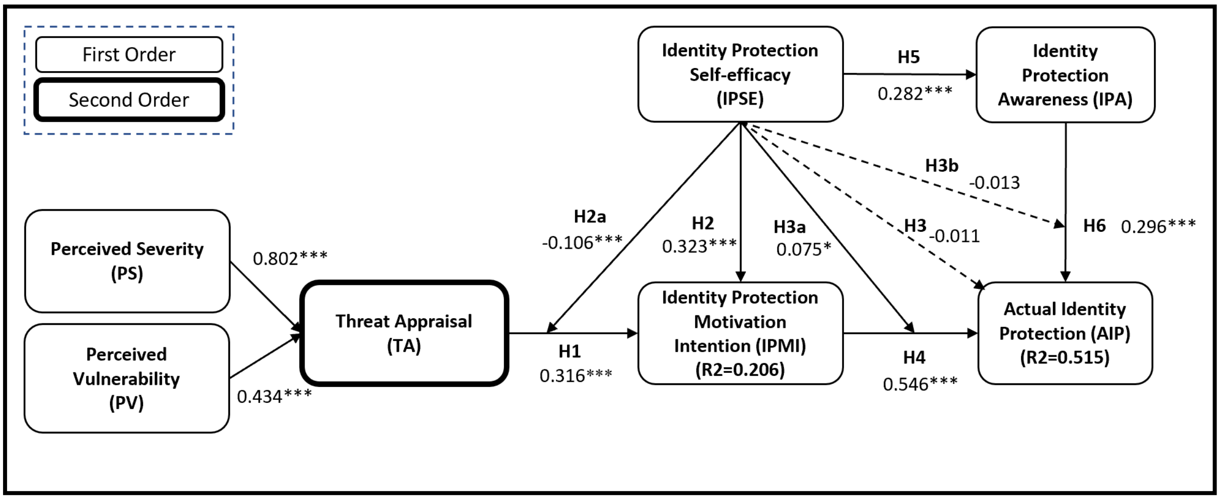
First Order
Second Order
Identity Protection Self-efficacy (IPSE)
H5
0.282***
Identity Protection Awareness (IPA)
H3b
-0.013
H6 0.296***
Perceived Severity (PS)
0.802***
Perceived Vulnerability (PV)
0.434***
Threat Appraisal (TA)
H2a
-0.106***
H2
0.323***
H3a
0.075*
H3
-0.011
H1
0.316***
Identity Protection Motivation Intention (IPMI) (R2=0.206)
H4
0.546***
Actual Identity Protection (AIP) (R2=0.515)

Figure 2. Structural model for mobile identity protection
Note: *** p < 0.01; ** p < 0.05; * p < 0.10

The research model explains 20.6% of identity protection motivational intentions (IPMI). Both perceived severity ($\hat{\beta}$= 0.802; p < 0.01) and perceived vulnerability ($\hat{\beta}$= 0.434; p < 0.01) are statistically significant to form threat appraisal (TA), confirming that TA is a second-order reflective-formative type construct (Ringle, Sarstedt, and Straub 2012). The hypotheses of identity protection self-efficacy ($\hat{\beta}$= 0.323; p < 0.01), and threat appraisal ($\hat{\beta}$= 0.316; p < 0.01) are statistically significant and explain identity protection motivational intentions (IPMI). Hence, H1 and H2 are supported. Also, the hypothesis of identity protection self-efficacy ($\hat{\beta}$= 0.282; p < 0.01) is statistically significant in predicting awareness protection. Hence, H5 is supported. Only the hypothesis (IPSE) is statistically insignificant ($\hat{\beta}$= -0.011; p > 0.01). Hence, H3 is not supported for explaining actual identity protection (AIP).

The structure model explains 51.5 % of the variation in actual identity protection (AIP). Hypothesis identity protection motivational intentions ($\hat{\beta}$= 0.546; p < 0.01), and identity protection awareness ($\hat{\beta}$= 0.296; p < 0.01) are statistically significant to explain actual identity protection (AIP). Thus, H4 and H6 are supported.

The moderating effect between threat appraisal and identity protection motivational intentions is confirmed ($\hat{\beta}$= - 0.106; p < 0.10); and between identity protection motivation intentions and actual identity protection is also confirmed ($\hat{\beta}$= 0.075; p < 0.05); hence H2a and H3a are confirmed. However, identity protection self-efficacy is not a statistically significant moderator ($\hat{\beta}$= - 0.013; p > 0.10) between identity protection motivational awareness and actual identity protection. Hence, H3b is not supported.

6 Implications

Our research has four important theoretical implications: (1) Perceived appraisal of mobile identity threats motivates users to protect their mobile identity. (2) Low identity protection self-efficacy and high perceived threats result in high motivation to engage in identity protection. (3) High identity protection self-efficacy and high perceived threats result in low motivation to engage in identity protection. The protection awareness fully mediates the relationship between identity protection self-efficacy and actual identity protection.

Our findings undoubtedly contribute to reframing the self-efficacy construct in the context of mobile identity protection. However, to ensure what our study revealed, we engaged our panel of experts to discuss the findings. Validation can occur before an instrument is deployed; it can also be done after identifying the quantitative results. As Straub et al. (2004) have argued, "validation guidelines are owned by communities of practice" (p. 417). Venkatesh et al. (2013) discuss mixed methods research and explicitly call for a qualitative assessment following the quantitative phase. During the interviews, we initially presented our study objectives, the measurement tool, and the significant findings to the panel members. We then asked the panellists to evaluate the findings with the content of the corresponding items. In the paragraphs below, we discuss our findings and their theoretical contributions and implications in light of what our panellists considered.

Perceived appraisal of mobile identity threats and identity protection. Our study enhances the understanding of modelling the role of self-efficacy in motivation as an important concern for identity protection (Tubbs, 1994). We do so by assessing the moderating effect of identity protection self-efficacy on motivating mobile users to achieve actual identity protection (O'Leary-Kelly et al., 1994). Furthermore, we find that self-efficacy is also significant in the relationship between identity protection motivation intention and actual mobile identity protection. We presented our findings to the expert panel. All the participants confirmed the results and found them consistent with the resultant constructs, items, and the related content of each item. They all agreed that threat appraisal is a strong positive predictor of the motivational intentions of mobile identity protection. Our findings align with the (Khan et al., 2023) study results, suggesting that PMT-based training effectively increases threat knowledge and individuals' self-efficacy, which significantly predicts cybersecurity behavioural intention. One of the consultants who advises corporate clients about mobile identity protection noted:

> *When I am discussing identity protection issues with my clients, a recurring theme is how well they are versed in the prevalent threats. I usually find that the more the individuals know about the threats, the greater their motivation to protect. I found this to be such an important issue, particularly when many employees of my client organizations are working remotely.*

While the finding may sound intuitive, individuals tend to take identity protection for granted in a mobile environment. As one of our user respondents noted:

> *It is so difficult to work with individual settings of different apps. I just trust the device and the operating system. I am sure there are threats, but IOS and Android have probably figured it out.*

A similar sentiment is found in the extant literature. Maddux & Rogers (1983), for example, posit that a threat's occurrence has a positive effect on an individual's intentions to adopt preventive behavior. Recently, Menard et al. (2017) found that both perceived threat severity and perceived threat susceptibility positively influence an individual's behavioural intention to undertake secure behaviours in their study on user motivations in protecting information security. In a similar vein, Johnston et al. (2023) suggest that to enhance the effectiveness of fear appeals; these should incorporate both threat appraisal and efficacy elements to evoke fear and exert influence on individuals' protective behavioural intentions.

Identity protection self-efficacy and identity protection motivation. Our research found an interesting relationship between identity protection self-efficacy and identity protection motivation. Low self-efficacy results in higher identity protection motivation. Conversely, with high self-efficacy, motivation to engage in identity protection is low. Figure 3 indicates that in a mobile environment with low identity protection self-efficacy, threat appraisal is more important to explain the identity protection motivational intentions. This aspect means that the perceived threat appraisal of mobile identity threats motivates users with low self-efficacy to protect their mobile identity. In such cases, the perceived threats to individuals with low identity protection self-efficacy increase their motivational intentions to protect their mobile identities. All members of our panel found the findings to be relevant. Low self-efficacy and high perceived threat appraisal are indeed strong motivators to achieve identity protection in the mobile context. As one of the respondents noted:

> *In my line of work, I see this all the time. I often find people who have no faith in their capabilities, but when they are made aware of the persistent threats and consequences of their identity loss, they suddenly become motivated to protect their identity. Once, I was conducting a workshop at a large telecommunication firm, and it was surprising to see how even the more technologically advanced individuals had no faith in their ability to protect themselves. When I introduced the range of threats that they were exposed to, their motivation to protect increased.*

The extant literature also suggests a similar orientation. For instance, studies conducted by (Maddux & Rogers, 1983; Rogers, 1975) found perceived threats and self-efficacy to impact users' behavioural intentions for protective actions. Johnston & Warkentin (2010) also posit that threat appraisal impacts individuals' protective behavioural intentions, which are not uniform across all individuals. However, it is influenced by self-efficacy, threat severity, and threat vulnerability, among other factors.

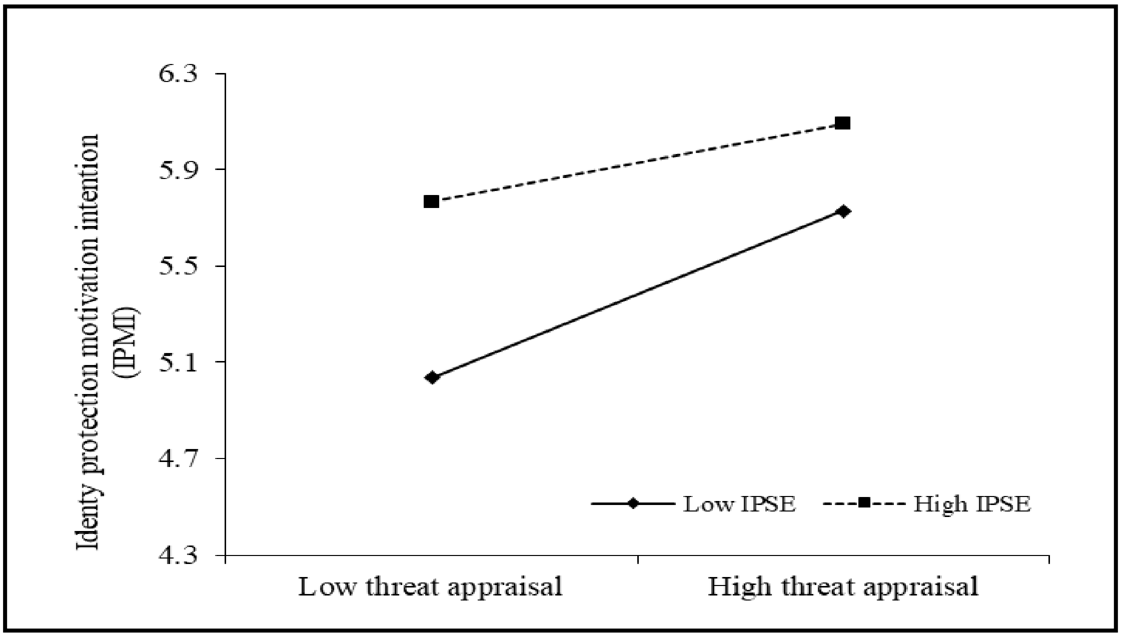

Figure 3. Moderation effect of self-efficacy on the relationship between TA and IPMI

One of the interesting findings in this study shows that in an environment with mobile users with high identity protection self-efficacy, threat appraisal is not so important in explaining identity protection motivational intention. This dimension is in contrast to individuals with low mobile identity protection self-efficacy, where mobile users with high self-efficacy are less motivated to engage in identity protection when they perceive high identity threats (Figure 4).

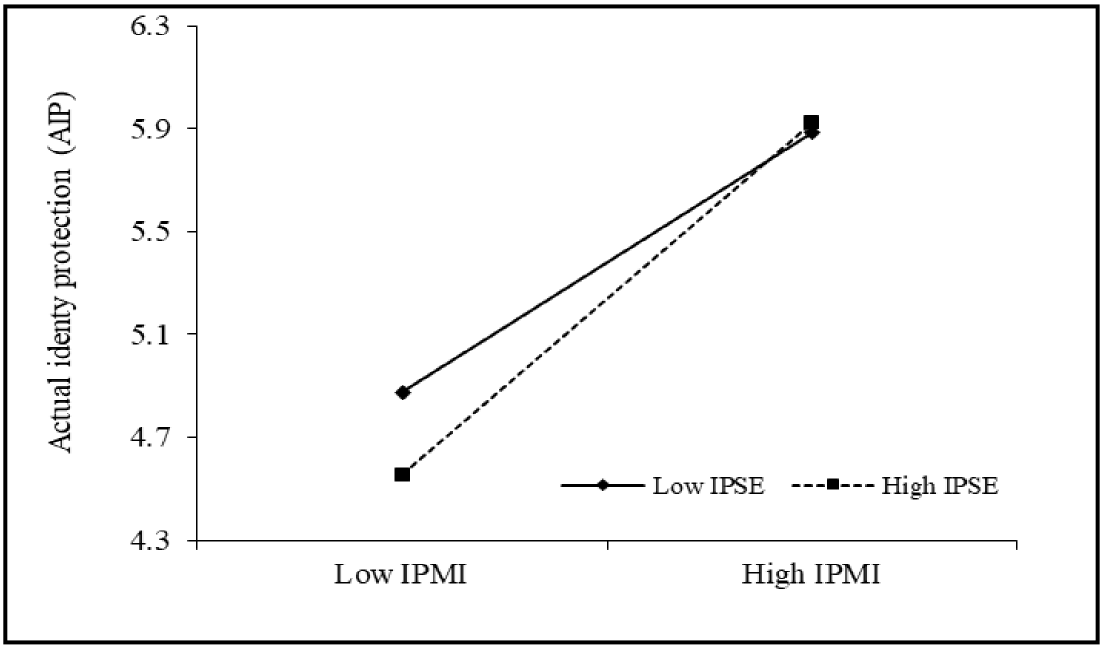

Figure 4. Moderation effect of self-efficacy on the relation between IPMI and AIP

Our panel of experts found no general disagreement. One panellist, for instance, noted:

> *The high self-efficacy of mobile users leads to overconfidence in their efficacy in actual identity protection. In my workplace, overconfidence became a real challenge for our cybersecurity team. In one case, employees claim they have enough knowledge to keep their mobile identity protected. Yet, when they were queried, few employees knew what multi-factor authentication was, and even fewer knew how to use it to protect their identity.*

It is interesting to note that this phenomenon is also pointed out in the literature. Stone (1994) discusses the negative effect of overconfidence on individuals' self-efficacy and performance. According to Stone, mild underconfidence can have a more positive motivational impact than overconfidence and heavy underconfidence. However, one of the panellists had a different explanation. He said:

> *From a psychological perspective, mobile users with high self-efficacy may generate a relaxed attitude that reduces their motivational intentions to protect their mobile identity. High self-efficacy users feel less stressed regarding perceived identity threats, which may eventually affect their intentions to carry out the actual protective behavior. I believe age has something to do with this. I think that youngsters are more relaxed about identity protection practices than the older group. This possibly makes them more vulnerable to mobile identity theft and related threats.*

It is noteworthy that extant literature in education supports the assertion about the negative impact of high self-efficacy on individuals' subsequent behavior. For example, Vancouver et al. (2001) concluded that high self-efficacy creates relaxation in the student's behavior regarding exams, which impacts their performance in later examinations over time. Perhaps a future experimental study can provide a deeper insight.

Threat appraisal, identity protection self-efficacy, and identity protection motivation intention. Our research suggests that self-efficacy positively impacts individual intention for identity protection. Prior studies have indicated that self-efficacy enhances complex task performance and impacts context-oriented dynamic tasks (e.g., mobile identity protection) by increasing individuals' motivation (Thangavelu et al., 2021). Self-efficacy has been shown to boost motivation and affect task success (Ballout, 2009). Individuals with high self-efficacy beliefs put in more effort, which leads to the achievement of their goals (Bandura, 1982; Bandura et al., 1999). We also found appraisal of existing threats helps individuals to protect their mobile identity. Both perceived threat vulnerability and threat severity significantly influence an individual's intention to protect mobile identity. Prior research relates perceived vulnerability and perceived severity and antecedents to threat appraisal (Khan & Das, 2016). This phenomenon suggests that threat appraisal affects individual behavioural intentions to perform recommended individual behaviours, which are partly influenced by self-efficacy perceptions (Johnston & Warkentin, 2010). Our findings are consistent with extant literature, highlighting the importance of threat appraisal in motivating individual behavioural intentions toward mobile identity protection.

The role of protection awareness in mobile identity protection. While the present study affirms the importance of protection awareness in boosting the individual's actual mobile identity protection, our finding revealed the mediation impact of protection awareness on the relationship between an individual's identity protection self-efficacy and actual identity protection in a mobile environment. There were different interpretations of the findings. One panellist suggests that:

> *Low self-efficacy in mobile identity protection may lead to protection procrastination, which indicates that mobile users with low capabilities in safeguarding their mobile identity may delay or put off protection tasks until they detect an identity threat, or their identity being compromised. This explains why self-efficacy has a minor impact on mobile users' real identity protection while having a substantial impact on their motivational intentions. From my experience, awareness of mobile identity threats and their negative consequences may encourage individuals to focus on protection tasks and alleviate the tendency to procrastinate.*

Procrastination is the act of delaying the completion of tasks that must be finished within a particular amount of time (Kirst-Ashman, 2016). In the information security context, procrastination can act as a motivational mechanism, emerging from stress or threat, leading to postponed security protection actions, reduced security behavior, avoidance of security tasks (Xu & Guo, 2019), and increased vulnerability to privacy and security risks (Xiao & Spanjol, 2021). The interpretation of procrastination tendency is consistent with multiple research that implies a link between procrastination and self-efficacy, given the self-regulation concerns that define trait procrastination (Ferrari, 1992; Tuckman, 1991). Self-efficacy is important in the self-regulation of behavior because of its effects on intention formation and strength, as well as action persistence in the face of obstacles (Bandura, 1977; 1986). The relationship between procrastination and self-efficacy is consistent with Bandura's (1986; 1977) theory that strong efficacy beliefs encourage the behavior to start and persist, whereas poor efficacy beliefs contribute to action avoidance. A recent study on the relationship between mindfulness and procrastination (Cheung & Ng, 2019) posits that awareness could minimize people's procrastination by encouraging them to focus on activities they're working on rather than succumbing to distractions. More recently, Ali & Dominic (2022) suggested implementing security awareness through SETA programs to mitigate procrastination behavior and enhance the adoption of protection measures. Another respondent suggested:

> *Using another motivational concept will be useful to examine the effect of the motivational aspect on an individual's protective behavior in the mobile context.*

Identity protection motivation intention and actual identity protection. Our research also found a significant and positive moderating role of self-efficacy on the relationship between individuals' motivational intentions and actual mobile identity protection. As shown in Figure 4, in an environment with high IPSE, the importance of IPMI in explaining actual identity protection is higher than in a low IPSE environment. Thus, an individual with high self-efficacy in mobile identity protection will be intentionally more motivated to achieve actual identity protection. Our finding complements and confirms the extant literature showing that the actual behavior is affected by behavioural intention (Davis, 1989; Davis et al., 1989).

The existing literature also demonstrates similar outcomes. For instance, Ogbanufe & Pavur (2022) investigated the influence of fear on individuals' motivation to safeguard against identity theft, employing concepts such as self-efficacy and protection motivation. However, their inquiry did not explore how self-efficacy impacts protective behaviours, nor did it delve into the predictive role of awareness in fostering motivation against identity theft. Our study contributes valuable insights by addressing these gaps. Our findings reveal that self-efficacy serves as a moderator in the relationship between perceived threats and individuals' intentions to secure their mobile identities. Furthermore, our research uncovers that protection awareness acts as a full mediator, connecting self-efficacy to the actual practice of identity protection.

These newly revealed insights contribute to a more nuanced comprehension of the dynamics that shape mobile identity protection. Moreover, our study significantly enriches the landscape of information security research. For instance, the recent work of Weixun Li et al. (2023) emphasizes the critical role of security awareness as a bridge to implementing comprehensive security measures. Their perspective highlights that an improved grasp of security threats enhances cooperation with security policies, fostering proactive measures to safeguard the security environment.

The absence of individual information security awareness also exerts an impact on organizational security. Khando et al. (2021) underscore this issue, highlighting that organizations often struggle to safeguard information assets as they rely mainly on technical solutions. Nevertheless, they contend that human vulnerabilities are a major factor in many security incidents. Consequently, individuals' information security awareness is pivotal in countering undesirable security behavior. In our study, identity protection awareness is shown to influence an individual's actual identity protection. Despite the vital role of self-efficacy in protecting mobile identity, individuals too often do not realize that they must ensure their mobile protection by themselves. Therefore, the knowledge of mobile identity threats that individuals may face, and the use of protective measures are essential. Knowing the threats leads to the use of necessary mobile identity protection measures. However, ignorance in this field casts doubt on an individual's expertise and ability to take appropriate protective measures (Markelj & Bernik, 2015). Hence, the finding of this study complements previous awareness studies and highlights the practical significance of fostering mobile identity protection to enhance overall information security posture.

Building upon these insights, our findings highlight the tangible benefits of enhancing individuals' awareness regarding various identity threat techniques and corresponding protective measures, thus bolstering their mobile identity protection. Furthermore, our study underscores the crucial interplay of motivational-behavioural factors in shaping the effectiveness of mobile identity protection awareness programs. As our results suggest, this provides a solid foundation for the development of training initiatives and awareness programs aimed at motivating employees to adopt the requisite measures for safeguarding their mobile identities in their workplace. In essence, our study not only underscores the practical implications of security awareness and self-efficacy in bolstering mobile identity protection but also lays the groundwork for actionable strategies to enhance information security in the mobile realm.

7 Conclusions

This study investigates the gaps in mobile identity protection and the roles of self-efficacy and threat appraisal on an individual's motivational intentions. We also study the moderating role of individual identity protection self-efficacy on motivational intentions. Moreover, we examined the mediation impact of awareness on the relationship between self-efficacy and actual identity protection. Our research extends the current understanding of the concept of self-efficacy in the mobile identity protection context. While acknowledging the importance of technical measures for identity protection, we discuss the threat appraisal motivational aspects of mobile identity protection. Our findings offer organizations suggestions for managing mobile identity to protect individuals from identity threats and the associated security attacks, particularly using motivational strategies and techniques. For future research, we suggest using the theory of expectancy-value motivation (Wigfield & Eccles, 2000) in addition to studying mobile identity protection. We also believe that adding expectancy and value constructs to the model could explain the protection motivation behavior in more depth by analyzing the individuals' expected success in protecting their mobile identity based on their protection perceived values.

References

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Ali, R. F., & Dominic, P. (2022). Investigation of information security policy violations among oil and gas employees: A security-related stress and avoidance coping perspective. *Journal of Information Science*, 016555152210876. https://doi.org/10.1177/01655515221087680

Ameen, N., Tarhini, A., Shah, M. H., Madichie, N., Paul, J., & Choudrie, J. (2021). Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. *Computers in Human Behavior*, *114*, 106531. https://doi.org/10.1016/j.chb.2020.106531

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *International Conference on Cyber Security for Sustainable Society*. Coventry University, United Kingdom. https://doi.org/10.48550/arXiv.1901.02672

Bagozzi, R. P. (2011). Measurement and meaning in information systems and organizational research: Methodological and philosophical foundations. *MIS Quarterly*, *35*(2), 261–292. https://www.jstor.org/stable/23044044

Balapour, A., Reychav, I., Sabherwal, R., & Azuri, J. (2019). Mobile technology identity and self-efficacy: Implications for the adoption of clinically supported mobile health apps. *International Journal of Information Management*, *49*, 58–68. https://doi.org/10.1016/j.ijinfomgt.2019.03.005

Ballout, H.I. (2009), "Career commitment and career success: moderating role of self-efficacy", *Career Development International*, *14*(7), 655-670. https://doi.org/10.1108/13620430911005708

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. Psychological Review, *84*(2), 191–215. https://doi.org/10.1037/0033-295X.84.2.191

Bandura, A. (1978). Self-efficacy: Toward a unifying theory of behavioral change. *Advances in Behaviour Research and Therapy*, *1*(4), 139–161. https://doi.org/10.1016/0146-6402(78)90002-4

Bandura, A. (1982). Self-efficacy mechanism in human agency. *American Psychologist*, *37*(2), 122–147. https://doi.org/10.1037/0003-066X.37.2.122

Bandura, A. (1986). *National Inst of Mental Health. (1986). Social foundations of thought and action: A social cognitive theory*. Hoboken, NJ, USA: Prentice-Hall, Inc.

Bandura, A. (1997). *Self-efficacy: The exercise of control*. New York, NY, USA: W H Freeman/Times Books/ Henry Holt & Co.

Bandura, A., Freeman, W. H., & Lightsey, R. (1997). Self-Efficacy: The Exercise of Control. *Journal of Cognitive Psychotherapy*, *13*, 158-166. https://doi.org/10.1891/0889-8391.13.2.158

Bandura, A., & Cervone, D. (1983). Self-evaluative and self-efficacy mechanisms governing the motivational effects of goal systems. *Journal of Personality and Social Psychology*, 45(5), 1017–1028. https://doi.org/10.1037/0022-3514.45.5.1017

Bandura, A., Freeman, W. H., & Lightsey, R. (1999). Self-efficacy: The exercise of control. *Journal of Cognitive Psychotherapy*, *13*(2), 158-166. https://doi.org/10.1891/0889-8391.13.2.158

Bandura, Albert. (1994). Self-efficacy. In *V. S. Ramachaudran (Ed.), Encyclopedia of human behavior* (Vol. 4, Issue 01, pp. 71–81). (Reprinted in H. Friedman [Ed.]), Encyclopedia of mental health. San Diego, CA, USA: Academic Press, 1998. http://happyheartfamilies.citymax.com/f/Self_Efficacy.pdf

Belanger, F., & Crossler, R. E. (2019). Dealing with digital traces: Understanding protective behaviors on mobile devices. *The Journal of Strategic Information Systems*, *28*(1), 34–49. https://doi.org/10.1016/j.jsis.2018.11.002

Bose, I., & Leung, A. C. M. (2019). Adoption of identity theft countermeasures and its short- and long-term impact on firm value. *MIS Quarterly*, *43*(1), 313–327. https://doi.org/10.25300/MISQ/2019/14192

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, *39*(4), 837–864. https://doi.org/10.25300/MISQ/2015/39.4.5

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523–548. https://doi.org/10.2307/25750690

Camp, L. J. (2004). Digital identity issues. *IEEE Technology and Society Magazine*, *23*(3), 34–41. https://doi.org/10.1109/MTAS.2004.1337889

Carter, M., & Grover, V. (2015). Me, myself, and I (T) Conceptualize Information Technology Identity and its Implications. *MIS Quarterly*, *39*(4), 931–958. https://www.jstor.org/stable/26628658

Chen, Y., & Zahedi, F. M. (2016). Individuals' internet security perceptions and behaviors: Polycontextual contrasts between the United States and China. *MIS Quarterly*, *40*(1), 205–222. https://doi.org/10.25300/MISQ/2016/40.1.09

Cheung, R. Y. M., & Ng, M. C. Y. (2019). Being in the moment later? Testing the inverse relation between mindfulness and procrastination. *Personality and Individual Differences*, *141*, 123–126. https://doi.org/10.1016/j.paid.2018.12.015

Chin, W. W. (1998). Commentary: Issues and Opinion on Structural Equation Modeling. *MIS Quarterly*, *22*(1), vii–xvi. http://www.jstor.org/stable/249674

Chin, W. W., Thatcher, J. B., & Wright, R. T. (2012). Assessing Common Method Bias: Problems with the ULMC Technique. *MIS Quarterly*, *36*(3), 1003–1019. https://doi.org/10.2307/41703491

Choudhary, P. K., Routray, S., Upadhyay, P., & Pani, A. K. (2022). Adoption of enterprise mobile systems–An alternative theoretical perspective. *International Journal of Information Management*, *67*, 102539. https://doi.org/10.1016/j.ijinfomgt.2022.102539

Churchill Jr, G. A. (1979). A paradigm for developing better measures of marketing constructs. *Journal of Marketing Research*, *16*(1), 64–73. https://doi.org/10.1177/002224377901600110

Cohen, J. (1992). Statistical power analysis. *Current Directions in Psychological Science*, *1*(3), 98–101. https://doi.org/10.1111/1467-8721.ep10768783

Compeau, D., Correia, J., & Bennett Thatcher, J. (2022). When Constructs Become Obsolete: A Systematic Approach to Evaluating and Updating Constructs for Information Systems Research. *MIS Quarterly*, *46*(2), 679–711. https://doi.org/10.25300/MISQ/2022/15516

Compeau, D. R., & Higgins, C. A. (1995). Computer Self-Efficacy: Development of a Measure and Initial Test. *MIS Quarterly*, *19*(2), 189–211. https://doi.org/10.2307/249688

Craig, K., Thatcher, J. B., & Grover, V. (2019). The IT Identity Threat: A Conceptual Definition and Operational Measure. *Journal of Management Information Systems*, *36*(1), 259–288. https://doi.org/10.1080/07421222.2018.1550561

Crossler, R. E., & Bélanger, F. (2019). Why Would I Use Location-Protective Settings on My Smartphone? Motivating Protective Behaviors and the Existence of the Privacy Knowledge–Belief Gap. *Information Systems Research*, *30*(3), 995–1006. https://doi.org/10.1287/isre.2019.0846

D'Arcy, J., & Lowry, P. B. (2019). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, *29*(1), 43–69. https://doi.org/10.1111/isj.12173

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, *13*(3), 319–340. https://doi.org/10.2307/249008

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management Science*, *35*(8), 982–1003. https://doi.org/10.1287/mnsc.35.8.982

Deng, G., & Fei, S. (2023). Exploring the factors influencing online civic engagement in a smart city: The mediating roles of ICT self-efficacy and commitment to community. *Computers in Human Behavior*, *143*, 107682. https://doi.org/10.1016/j.chb.2023.107682

Dhillon, G., Abdul Talib, Y. Y., & Picoto, W. N. (2020). The Mediating Role of Psychological Empowerment in Information Security Compliance Intentions. *Journal of the Association for Information Systems*, *21*(1), 5. https://doi.org/10.17705/1jais.00595

Dhillon, G., & Chowdhuri, R. (2013). Individual values for protecting identity in social networks. *International Conference on Information Systems (ICIS 2013): Reshaping Society Through Information Systems Design*, *3*, 2177–2192. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=18dbe95c34ce00ed017e1b5689c6291add214589

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems*, *8*(7), 23. https://doi.org/10.17705/1jais.00133

Eagly, A. H., & Chaiken, S. (1998). *Attitude structure and function*. In D. T. Gilbert, S. T. Fiske, & G. Lindzey (Eds.), The Handbook of Social Psychology (pp. 269–322). New York, NY, USA: McGraw-Hill. https://psycnet.apa.org/record/1998-07091-007

Edwards, J., Miles, M. P., D'Alessandro, S., & Frost, M. (2022). Linking B2B sales performance to entrepreneurial self-efficacy, entrepreneurial selling actions. *Journal of Business Research*, *142*, 585–593. https://doi.org/10.1016/j.jbusres.2021.12.074

Ferrari, J. R. (1992). Psychometric validation of two procrastination inventories for adults: Arousal and avoidance measures. *Journal of Psychopathology and Behavioral Assessment*, *14*(2), 97–110. https://doi.org/10.1007/BF00965170

Fishbein, M., & Ajzen, I. (1980). *Understanding attitudes and predicting social behavior*. Englewood-Cliffs, NJ, USA: Prentice-Hall.

Fisher Jr, E. B., & Rost, K. (1986). Smoking cessation: a practical guide for the physician. *Clinics in Chest Medicine*, *7*(4), 551–565. https://europepmc.org/article/med/3539471

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. https://doi.org/10.1177/002224378201900406

Fornell, C., & Larcker, D. F. (1981). Structural equation models with unobservable variables and measurement error: Algebra and statistics. *Journal of Marketing Research*, *18*(3), 382–388. https://doi.org/10.2307/3150980

FTC. (2020). *Consumer Sentinel Network*. Federal Trade Commission, Data Book 2019. https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2019/consumer_sentinel_network_data_book_2019.pdf

Gao, W., Liu, Z., Guo, Q., & Li, X. (2018). The dark side of ubiquitous connectivity in smartphone-based SNS: An integrated model from information perspective. *Computers in Human Behavior*, *84*, 185–193. https://doi.org/10.1016/j.chb.2018.02.023

Gong, X., Zhang, K. Z. K., Chen, C., Cheung, C. M. K., & Lee, M. K. O. (2020). What drives trust transfer from web to mobile payment services? The dual effects of perceived entitativity. *Information & Management*, *57*(7), 103250. https://doi.org/10.1016/j.im.2019.103250

Goo, J., Kishore, R., Rao, H. R., & Nam, K. (2009). The role of service level agreements in relational management of information technology outsourcing: an empirical study. *MIS Quarterly*, *33*(1), 119–145. https://doi.org/10.2307/20650281

Graham, S., & Weiner, B. (1996). *Theories and Principles of Motivation*. In D. C. Berliner, & R. Calfee (Eds.), Handbook of Educational Psychology (pp. 63-84). New York, NY, USA: Macmillan. https://www.scirp.org/(S(351jmbntvnsjt1aadkposzje))/reference/ReferencesPapers.aspx?ReferenceID=1209774

Guillon, V., Dosnon, O., Esteve, M.-D., & Gosling, P. (2004). Self-efficacy and behavioral intention: A mediational analysis of the effects of commitment on career counseling. *European Journal of Psychology of Education*, *19*(3), 315–332. https://doi.org/10.1007/BF03173226

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2012). Partial least squares: the better approach to structural equation modeling? *Long Range Planning*, *45*(5–6), 312–319. https://doi.org/10.1016/j.lrp.2012.09.011

Hair, J. F., Sarstedt, M., Ringle, C. M., & Mena, J. A. (2012). An assessment of the use of partial least squares structural equation modeling in marketing research. *Journal of the Academy of Marketing Science*, *40*(3), 414–433. https://doi.org/10.1007/s11747-011-0261-6

Hair Jr, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., Danks, N. P., & Ray, S. (2021). *Partial least squares structural equation modeling (PLS-SEM) using R: A workbook*. Cham, Switzerland: Springer Nature. https://doi.org/10.1007/978-3-030-80519-7

Hair Jr, J. F., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. G. (2014). Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. *European Business Review*, *26*(2), 106–121. https://doi.org/10.1108/EBR-10-2013-0128

Hair Jr, J., Hair Jr, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2021). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Thousand Oaks, CA, USA: Sage Publications. https://doi.org/10.1007/978-3-030-80519-7

Hampel, N., Sassenberg, K., Scholl, A., & Ditrich, L. (2023). Enactive mastery experience improves attitudes towards digital technology via self-efficacy–a pre-registered quasi-experiment. *Behaviour & Information Technology*, 1–14. https://doi.org/10.1080/0144929X.2022.2162436

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*(1), 115–135. https://doi.org/10.1007/s11747-014-0403-8

Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2009). The use of partial least squares path modeling in international marketing. In A. M. Rugman (Ed.), *New challenges to international marketing* (pp. 14-33). Bingley, UK: Emerald Group Publishing Ltd. https://doi.org/10.1108/s1474-7979(2009)0000020014

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R. (2014). Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service. *Information Systems Journal*, *24*(1), 61–84. https://doi.org/10.1111/j.1365-2575.2012.00420.x

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. https://doi.org/10.1057/ejis.2009.6

Huang, G., & Ren, Y. (2020). Linking technological functions of fitness mobile apps with continuance usage among Chinese users: Moderating role of exercise self-efficacy. *Computers in Human Behavior*, *103*, 151–160. https://doi.org/10.1016/j.chb.2019.09.013

Jaeger, L. (2018). Information security awareness: literature review and integrative framework. In *Proceedings of the 51st Hawaii International Conference on System Sciences.* The USA. https://doi.org/10.24251/hicss.2018.593

Jaeger, L., & Eckhardt, A. (2021). Eyes wide open: The role of situational information security awareness for security-related behaviour. *Information Systems Journal*, *31*(3), 429–472. https://doi.org/10.1111/isj.12317

Johnson, R. E., Rosen, C. C., & Djurdjevic, E. (2011). Assessing the impact of common method variance on higher order multidimensional constructs. *Journal of Applied Psychology*, *96*(4), 744–761. https://doi.org/10.1037/a0021504

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*(3), 549–566. https://doi.org/10.2307/25750691

Johnston, A. C., Warkentin, M., McBride, M., & Carter, L. (2016). Dispositional and situational factors: influences on information security policy violations. *European Journal of Information Systems*, *25*(3), 231–251. https://doi.org/10.1057/ejis.2015.15

Johnston, A., Di Gangi, P. M., Bélanger, F., Crossler, R. E., Siponen, M., Warkentin, M., & Singh, T. (2023). Seeking rhetorical validity in fear appeal research: An application of rhetorical theory. *Computers & Security*, *125*, 103020. https://doi.org/10.1016/j.cose.2022.103020

Ke, W., Liu, H., Wei, K. K., Gu, J., & Chen, H. (2009). How do mediated and non-mediated power affect electronic supply chain management system adoption? The mediating effects of trust and institutional pressures. *Decision Support Systems*, *46*(4), 839–851. https://doi.org/10.1016/j.dss.2008.11.008

Keith, M. J., Babb, J. S., Lowry, P. B., Furner, C. P., & Abdullat, A. (2015). The role of mobile-computing self-efficacy in consumer information disclosure. *Information Systems Journal*, *25*(6), 637–667. https://doi.org/10.1111/isj.12082

Khan, H., & Das, A. (2016). Security behaviors of smartphone users. *Information Management & Computer Security*, *24*, 116. https://doi.org/10.1108/ICS-04-2015-0018

Khan, N. F., Ikram, N., Murtaza, H., & Javed, M. (2023). Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's Model. *Computers & Security, 125*, 103049. https://doi.org/10.1016/j.cose.2022.103049

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security, 106*, 102267. https://doi.org/10.1016/j.cose.2021.102267

Kim, H.-W., & Kankanhalli, A. (2009). Investigating user resistance to information systems implementation: A status quo bias perspective. *MIS Quarterly, 33*(3), 567–582. https://doi.org/10.2307/20650309

Kirst-Ashman, K. K. (2016). *Empowerment Series: Introduction to Social Work & Social Welfare: Critical Thinking Perspectives*. (5th ed.). Boston, MA, USA: Cengage learning.

Kraiger, K., Ford, J. K., & Salas, E. (1993). Application of cognitive, skill-based, and affective theories of learning outcomes to new methods of training evaluation. *Journal of Applied Psychology, 78*(2), 311 –328. https://doi.org/10.1037/0021-9010.78.2.311

Lee, G., & Xia, W. (2010). Toward agile: an integrated analysis of quantitative and qualitative field data on software development agility. *MIS Quarterly, 34*(1), 87–114. https://doi.org/10.2307/20721416

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems, 18*(2), 177–187. https://doi.org/10.1057/ejis.2009.11

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, 33(1), 71–90. https://doi.org/10.2307/20650279

Liang, H., & Xue, Y. L. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems, 11*(7), 394–413. https://doi.org/10.17705/1jais.00232

Lin, W., Xu, M., He, J., & Zhang, W. (2023). Privacy, security, and resilience in mobile healthcare applications. *Enterprise Information Systems, 17*(3). https://doi.org/10.1080/17517575.2021.1939896

Lindell, M. K., & Whitney, D. J. (2001). Accounting for common method variance in cross-sectional research designs. *Journal of Applied Psychology, 86*(1), 114–121. https://doi.org/10.1037/0021-9010.86.1.114

Liu, J., Skoric, M. M., & Li, C. (2023). Disentangling the relation among trust, efficacy and privacy management: a moderated mediation analysis of public support for government surveillance during the COVID-19 pandemic. *Behaviour & Information Technology*, 1–20. https://doi.org/10.1080/0144929x.2023.2178830

Loh, X.-M., Lee, V.-H., Hew, J.-J., Tan, G. W.-H., & Ooi, K.-B. (2023). The future is now but is it here to stay? Employees' perspective on working from home. *Journal of Business Research*, 167, 114190. https://doi.org/10.1016/j.jbusres.2023.114190

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*(5), 469–479. https://doi.org/10.1016/0022-1031(83)90023-9

Malodia, S., Mishra, M., Fait, M., Papa, A., & Dezi, L. (2023). To digit or to head? Designing digital transformation journey of SMEs among digital self-efficacy and professional leadership. *Journal of Business Research*, 157, 113547.

https://doi.org/10.1016/j.jbusres.2022.113547

Manke, S., & Winkler, I. (2013). *The habits of highly successful security awareness programs: A cross-company comparison*. Securementem, Retrieved April 12, 2016, from https://www.securementem.com/wp-content/uploads/2013/07/Habits_white_paper.pdf

Markelj, B., & Bernik, I. (2015). Safe use of mobile devices arises from knowing the threats. *Journal of Information Security and Applications*, *20*, 84–89. https://doi.org/10.1016/j.jisa.2014.11.001

Martens, M., de Wolf, R., & de Marez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams, and cybercrime in general. *Computers in Human Behavior*, *92*, 139–150. https://doi.org/10.1016/j.chb.2018.11.002

Matook, S., Maggie Wang, Y., Koeppel, N., & Guerin, S. (2023). Metacognitive skills in low-code app development: Work-integrated learning in information systems development. *Journal of Information Technology*, 02683962231170238. https://doi.org/10.1177/02683962231170238

McCall George, J., & Simmons, J. L. (1978). *Identities and interactions: An examination of human associations in everyday life*. New York, NY, USA: Free Press.

Menard, P., Bott, G. J., & Crossler, R. E. (2017). User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems*, *34*(4), 1203–1230. https://doi.org/10.1080/07421222.2017.1394083

Menard, P., Warkentin, M., & Lowry, P. B. (2018). The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination. *Computers & Security*, *75*, 147–166. https://doi.org/10.1016/j.cose.2018.01.020

Mombeuil, C. (2023). Consumers' Willingness to Use Mobile Payments in Micro Business Transactions: Differences in Demographic Factors. *Information Systems Frontiers*, 1–14. https://doi.org/10.1007/s10796-023-10421-6

Mullins, J., & Sabherwal, R. (2022). Just Enough Information? The Contingent Curvilinear Effect of Information Volume on Decision Performance in IS-Enabled Teams. *MIS Quarterly*, *46*(4), 2197–2228. https://doi.org/10.25300/misq/2022/17290

Ogbanufe, O., & Gerhart, N. (2020). The mediating influence of smartwatch identity on deep use and innovative individual performance. *Information Systems Journal*, *30*(6), 977–1009. https://doi.org/10.1111/isj.12288

Ogbanufe, O. M., & Baham, C. (2023). Using Multi-Factor Authentication for Online Account Security: Examining the Influence of Anticipated Regret. *Information Systems Frontiers*, *25*(2), 897–916. https://doi.org/10.1007/s10796-022-10278-1

Ogbanufe, O., & Pavur, R. (2022). Going through the emotions of regret and fear: Revisiting protection motivation for identity theft protection. *International Journal of Information Management*, *62*, 102432. https://doi.org/10.1016/j.ijinfomgt.2021.102432

O'Leary-Kelly, A. M., Martocchio, J. J., & Frink, D. D. (1994). A review of the influence of group goals on group performance. *Academy of Management Journal*, *37*(5), 1285–1301. https://doi.org/10.5465/256673

O'Sullivan, T. L., Corneil, W., Kuziemsky, C. E., & Toal-Sullivan, D. (2015). Use of the structured interview matrix to enhance community resilience through collaboration and inclusive engagement. *Systems Research and Behavioral Science*, *32*(6), 616–628. https://doi.org/10.1002/sres.2250

O'Sullivan, T., Tracey, S., & Corneil, W. (2022). *Structured Interview Matrix (SIM) Facilitators' Guide*. https://ruor.uottawa.ca/bitstream/10393/44813/1/SIM%20Facilitator%27s%20Guide_O%27Sullivan%20et%20al_%202022.pdf

Pavlou, & Fygenson. (2006). Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior. *MIS Quarterly*, *30*(1), 115. https://doi.org/10.2307/25148720

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *88*(5), 879–903. https://doi.org/10.1037/0021-9010.88.5.879

Podsakoff, P. M., & Organ, D. W. (1986). Self-Reports in Organizational Research: Problems and Prospects. *Journal of Management*, *12*(4), 531–544. https://doi.org/10.1177/014920638601200408

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, *32*(4), 179–214. https://doi.org/10.1080/07421222.2015.1138374

Reychav, I., Beeri, R., Balapour, A., Raban, D. R., Sabherwal, R., & Azuri, J. (2019). How reliable are self-assessments using mobile technology in healthcare? The effects of technology identity and self-efficacy. *Computers in Human Behavior*, *91*, 52–61. https://doi.org/10.1016/j.chb.2018.09.024

Rheea, H.-S., Kimb, C., & Ryuc, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, *28*(8), 816–826. https://doi.org/10.1016/j.cose.2009.05.008

Ringle, C. M., Sarstedt, M., & Straub, D. W. (2012). Editor's Comments: A Critical Look at the Use of PLS-SEM in" MIS Quarterly". *MIS Quarterly*, *36*(1), iii–xiv. https://doi.org/10.2307/41410402

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. R. Cacioppo, & R.E. & Petty

(Eds.), *Social Psychology: A Sourcebook*, pp. 153-176. New York, NY, USA: Guilford. https://search.gesis.org/publication/zis-Rogers1983Cognitive

Sanyal, P., Menon, N., & Siponen, M. (2021). An Empirical Examination of the Economics of Mobile Application Security. *MIS Quarterly, 45*(4), 2235–2260. https://doi.org/10.25300/misq/2021/15315

Schunk, D. H., & Pajares, F. (2009). *Self-efficacy theory*. In K. R. Wenzel & A. Wigfield (Eds.), Handbook of motivation at school (pp. 35–53). Milton Park, UK: Routledge/Taylor & Francis Group.
https://repository.stkipjb.ac.id/index.php/lecturer/article/download/2935/2473#page=48

Silic, 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. https://doi.org/10.1080/07421222.2019.1705512

Soh, F., Smith, K., & Dhillon, G. (2022). The Relationship between Social Capital and Social Media Addiction: The Role of Privacy Self-Efficacy. *Australasian Journal of Information Systems*, 26. https://doi.org/10.3127/ajis.v26i0.3367

Souppaya, M., & Scarfone, K. (2013). *Guidelines for Managing the Security of Mobile Devices in the Enterprise*. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-124r1

Stets, J. E., & Cast, A. D. (2007). Resources and identity verification from an identity theory perspective. *Sociological Perspectives*, *50*(4), 517–543.
https://doi.org/10.1525/sop.2007.50.4.517

Stone, D. N. (1994). Overconfidence in initial self-efficacy judgments: Effects on decision processes and performance. *Organizational Behavior and Human Decision Processes*, *59*(3), 452–474. https://doi.org/10.1006/obhd.1994.1069

Straub, D., & Gefen, D. (2004). Validation Guidelines for IS Positivist Research. *Communications of the Association for Information Systems*, 13. https://doi.org/10.17705/1cais.01324

Straub, D. W. (1989). Validating Instruments in MIS Research. *MIS Quarterly, 13*(2), 147. https://doi.org/10.2307/248922

Stryker, S., & Serpe, R. T. (1994). Identity Salience and Psychological Centrality: Equivalent, Overlapping, or Complementary Concepts? *Social Psychology Quarterly*, 57(1), 16–35. https://doi.org/10.2307/2786972

Tang, X., & Wei, S. (2022). How do ambidextrous leadership and self-efficacy influence employees' enterprise system use: an empirical study of customer relationship management system context. *Information Technology & People*, *35*(4), 1443–1465. https://doi.org/10.1108/itp-07-2020-0479

Taylor, S., & Todd, P. A. (1995). Understanding Information Technology Usage: A Test of Competing Models. *Information Systems Research*, 6(2), 144–176. https://doi.org/10.1287/isre.6.2.144

Thangavelu, M., Krishnaswamy, V., & Sharma, M. (2021). Impact of comprehensive information security awareness and cognitive characteristics on security incident management–an empirical study. *Computers & Security*, *109*, 102401. https://doi.org/10.1016/j.cose.2021.102401

Thompson, N., McGill, T. J., & Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security*, *70*, 376–391. https://doi.org/https://doi.org/10.1016/j.cose.2017.07.003

Tubbs, M. (1994). Commitment and the role of ability in motivation: Comment on Wright, O'Leary-Kelly, Cortina, Klein, and Hollenbeck (1994). *Journal of Applied Psychology*, *79*(6), 804–811. https://doi.org/10.1037/0021-9010.79.6.804

Tuckman, B. W. (1991). The Development and Concurrent Validity of the Procrastination Scale. *Educational and Psychological Measurement*, *51*(2), 473–480. https://doi.org/10.1177/0013164491512022

Vancouver, J. B., Thompson, C. M., & Williams, A. A. (2001). The changing signs in the relationships among self-efficacy, personal goals, and performance. *Journal of Applied Psychology*, *86*(4), 605–620. https://doi.org/10.1037/0021-9010.86.4.605

Vedadi, A., & Warkentin, M. (2020). Can Secure Behaviors Be Contagious? A Two-Stage Investigation of the Influence of Herd Behavior on Security Decisions. *Journal of the Association for Information Systems*, *21*(2), 3. https://doi.org/10.17705/1jais.00607

Venkatesh, V., Aloysius, J. A., Hoehle, H., & Burton, S. (2017). Design and evaluation of auto-ID enabled shopping assistance artifacts in customers' mobile phones. *MIS Quarterly*, *41*(1), 83–114. https://doi.org/10.25300/misq/2017/41.1.05

Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the Qualitative-Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems. *MIS Quarterly*, *37*(1), 21–54. https://doi.org/10.25300/misq/2013/37.1.02

Verkijika, S. F. (2018). Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. *Computers & Security*, *77*, 860–870. https://doi.org/10.1016/j.cose.2018.03.008

Verkijika, S. F. (2019). "If you know what to do, will you take action to avoid mobile phishing attacks": Self-efficacy, anticipated regret, and gender. *Computers in Human Behavior*, *101*, 286–296. https://doi.org/10.1016/j.chb.2019.07.034

Wang, J., Li, Y., & Rao, H. R. (2016). Overconfidence in Phishing Email Detection. *Journal of the Association for Information Systems*, *17*(11), 759–783. https://doi.org/10.17705/1jais.00442

Wang, X., Li, Y., Khasraghi, H. J., & Trumbach, C. (2023). The mediating role of security anxiety in internet threat avoidance behavior. *Computers & Security*, 134, 103429. https://doi.org/10.1016/j.cose.2023.103429

Warkentin, M., Johnston, A. C., & Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems*, *20*(3), 267–284. https://doi.org/10.1057/ejis.2010.72

Li, W., Leung, A., & Yue, W. (2023). Where is IT in Information Security? The Interrelationship among IT Investment, Security Awareness, and Data Breaches. *MIS Quarterly*, *47*(1), 317–342. https://doi.org/10.25300/misq/2022/15713

Wigfield, A., & Eccles, J. S. (2000). Expectancy–Value Theory of Achievement Motivation. *Contemporary Educational Psychology*, *25*(1), 68–81. https://doi.org/10.1006/ceps.1999.1015

Willison, R., & Warkentin, M. (2013). Beyond Deterrence: An Expanded View of Employee Computer Abuse. *MIS Quarterly*, *37*(1), 1–20. https://doi.org/10.25300/misq/2013/37.1.01

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communication Monographs*, *59*(4), 329–349. https://doi.org/10.1080/03637759209376276

WITTE, K. (1996). Predicting Risk Behaviors: Development and Validation of a Diagnostic Scale. *Journal of Health Communication*, *1*(4), 317–342. https://doi.org/10.1080/108107396127988

Wu, D., Moody, G. D., Zhang, J., & Lowry, P. B. (2020). Effects of the design of mobile security notifications and mobile app usability on users' security perceptions and continued use intention. *Information & Management*, *57*(5), 103235. https://doi.org/10.1016/j.im.2019.103235

Xiao, Y., & Spanjol, J. (2021). Yes, but not now! Why some users procrastinate in adopting digital product updates. *Journal of Business Research*, *135*, 685–696. https://doi.org/10.1016/j.jbusres.2021.06.066

Xu, Z., & Guo, K. (2019). It ain't my business: A coping perspective on employee effortful security behavior. *Journal of Enterprise Information Management*, *32*(5), 824–842. https://doi.org/10.1108/jeim-10-2018-0229

Yao, M.-L., Chuang, M.-C., & Hsu, C.-C. (2018). The Kano model analysis of features for mobile security applications. *Computers & Security*, *78*, 336–346. https://doi.org/10.1016/j.cose.2018.07.008

Yazdanmehr, A., Li, Y., & Wang, J. (2022). Does stress reduce violation intention? Insights from eustress and distress processes on employee reaction to information security policies. *European Journal of Information Systems*, 32(6), 1033–1051. https://doi.org/10.1080/0960085x.2022.2099767

Yoo, C. W., Goo, J., & Rao, H. R. (2020). Is Cybersecurity a Team Sport? A Multilevel Examination of Workgroup Information Security Effectiveness. *MIS Quarterly*, *44*(2), 907–931. https://doi.org/10.25300/misq/2020/15477

Zahedi, F., Abbasi, A., & Chen, Y. (2015). Fake-Website Detection Tools: Identifying Elements that Promote Individuals' Use and Enhance Their Performance. *Journal of the Association for Information Systems*, 16(6), 448–484. https://doi.org/10.17705/1jais.00399

Zambrano, F. R. R., & Rafael, G. D. R. (2018). Bring your own device: a survey of threats and security management models. *International Journal of Electronic Business*, *14*(2), 146–170. https://doi.org/10.1504/ijeb.2018.094862

Zhou, Q., Li, B., Scheibenzuber, C., & Li, H. (2023). Fake news land? Exploring the impact of social media affordances on user behavioral responses: A mixed-methods research. *Computers in Human Behavior*, *148*, 107889. https://doi.org/10.1016/j.chb.2023.107889

Appendix

Table A1. The self-efficacy conceptualization in the information systems literature

Author	Theory	Self-efficacy Antecedents	Self-efficacy type	Dependent variable	Findings
Yazdanmehr et al. (2023)	TMSC; SET	Security Related Stress (SRS)	ISP-related self-efficacy (ISPSE)	Inward Emotion-Focused Coping (IEFC); Outward Emotion-Focused Coping (OEFC); Problem Focused Coping (PFC)	ISPSE Mod: SRS → IEFC. ISPSE Mod: SRS → OEFC. ISPSE Mod: SRS → PFC.
Liu et al. (2023)	SET	Perceived Cost (PC); Perceived Benefits (PB); Perceived Threat (PT)	Privacy Self-efficacy (PSE); Political Efficacy (PE)	Privacy Trust (PT); Public Support for Government Surveillance (PSGS)	PSE Med: PC;PB;PT → PSGS PE → PT
Matook et al. (2023)	SET	-	Self-efficacy (SE)	Metacognitive Skills (MS)	SE → MS
Loh et al. (2023)	PMT; TTS	-	Self-efficacy (SE)	Work Productivity (WP); Technostress (TS)	SE → WP SE → TS
Wang et al. (2023)	TTAT	-	Security Self-efficacy (SSE); Response-Self-efficacy (RSE)	Avoidance of Internet Threats (AIT)	SSE → AIT RSE → AIT
Zhou et al. (2023)	FIT	Perceived Autonomy (PA)	Skepticism Self-efficacy (SSE)	Fact Authentication (FA); Counter Arguing (CA); Instant Sharing (IS)	PA → SSE SSE → FA SSE → CA
Hampel et al. (2023)	SCT; SET	Intervention Type (IT); Vicarious Experience (VE); Enactive Mastery (EM)	Robot-specific Self-efficacy (RSSE)	Technology Enthusiasm (TE)	IT; VE; EM → RSSE RSSE → TE RSSE Med: IT; VE; EM → TE
Deng & Fei (2023)	SET; SLT	Information Content; Responsiveness Environment Quality	ICT Self-efficacy (ICTSE)	Online Sevic Behaviour (OSB)	ICTSE → OSB
Malodia et al. (2023)	SET	-	Digital Self-efficacy (DSE) for SME	Digital Transformation (DT)	DSE → DT

Yazdanmehr et al. (2022)	TMSC; HSM	Positive Responses (PR); Negative Responses (NR)	Information Security Policies Self-efficacy (ISPSE)	Playful Problem Solving (PPS); Wishful Thinking (WT)	ISPSE Mod: PR →PPS ISPSE Mod: NR →WT
Tang & Wei (2022)	AT	Ambidextrous Leadership	Performance Self-efficacy (PSE); Creative Self-efficacy (CSE)	Exploitative Use (EU); Explorative Use (EU)	PSE → EU CSE → EU
Edwards et al. (2022)	SET	-	Entrepreneurial self-efficacy (ESE)	Creative Selling (CS); Sales Innovation (SI)	ESE → CS ESE → SI
Soh et al. (2022)	SCT; SET	Social Capital Bridging (SCBr.); Social Capital Bonding (SCBo.)	Privacy Self-efficacy (PSE)	Social Media Addiction (SMA)	PSE Mod: SCBr. → SMA PSE Mod: SCBo. → SMA
Mullins & Sabherwal (2022)	IPT; ST	Information Value (IV)	Computer Self-efficacy (CSE)	Decision Performance (DP)	CSE Mod: IV → APM
Ogbanufe & Pavur (2022)	PMT	-	Perceived Efficacy (PE)	Adaptive Protection Motivation (APM); Maladaptive Message Rejection (MMR)	PE → APM PE → MMR
Jaeger & Eckhardt (2021)	PMT	Situational IS Awareness	Perceived Coping Efficacy (PCE)	Protection Motivation (PM)	PCE → PM
Silic & Lowry (2020)	HMSAM	Learning	Security Self-efficacy	Behavioral intention (BI) to follow security policies	SSE → BI to follow security policies
Yoo et al. (2020)	SCT; DT; CT; TPB; IT; PMT	Security knowledge coordination	Individual efficacy (IE); Workgroup collective efficacy (WSE)	Workgroup information security effectiveness (WISE) Effectiveness	IE → WISE Effectiveness WSE → WISE Effectiveness
Huang & Ren (2020)	SCT; SET	Perceived Usefulness (PU)	Exercise Self-efficacy (ESE)	Continuance Use Intention (CUI) of fitness mobile apps	ESE Mod: PU → CI
Balapour et al. (2019)	ITIT, SET; TAM	Related IT Experience (ITE)	Self-Efficacy (SE)	Intention To Use Mobile Health Apps (IUMHA)	ITE → SE ITSEE → IUMHA
Reychav et al. (2019)	SET	Mobile Technology Identity (MTI)	Self-Efficacy (SE)	Self-Report Reliability (SRR)	SE → SRR SE Mod: MTI → SRR

Verkijika (2019)	TTAT	-	Anti-Phishing Self-efficacy (APSE)	Avoidance Motivation (AM); Avoidance Behavior (AB)	APSE → AM APSE → AB
Belanger & Crossler (2019)	TPB	-	Mobile privacy protection self-efficacy (MPPSE)	Mobile privacy protection (MPP) Intention / Behaviour	MPPSE → MPPI/MPPB
D'Arcy & Lowry (2019)	RCT, TPB	-	Compliance Self-efficacy (CSE)	Compliance behavior	CSE → Compliance behavior
Crossler & Bélanger (2019)	SET; IMB Model	Personal motivation, social motivation	Privacy Self-efficacy (PSE)	Individuals' usage of smartphone privacy settings	PSE → Privacy setting usage
Wang et al. (2016)	SCT		Phishing Detection Self-efficacy (PDSE)	Overconfidence Marginal Effect (OME)	PDSE → OME
Johnston et al. (2016)	PMT; GDT. Big Five personality traits	-	Self-efficacy (SE)	Intention to violate IS Security policies (IVISP)	SE→ IVISP
Posey et al. 2015)	PMT	-	Self-efficacy (SE)	Protection motivation (PM)	SE → PM
Zahedi et al. (2015)	PMT	Detector accuracy, Detector speed	Coping Self-efficacy (CSE)	Reliance on the Detector (ROD)	CSE → ROD
Keith et al. (2015)	SCT	-	Mobile-computing Self-efficacy (MCSE)	Trusting belief (TB), Disclosure	MCSE → TB MCSE → Disclosure
Herath et al. (2014)	TAM; TTAT	-	Email screening self-efficacy (ESSE)	Coping Motivation\Behavior (CMB)	ESSE → CMB
Willison & Warkentin (2013)	ST, PMD; TPB	Information systems (IS) controls	Deterrence efficacy (DEF)	IS Policy Violation Intention (ISPVI)	DE → ISPVI

Warkentin et al. (2011)	SLT;
	SET
		situational support; verbal persuasion; vicarious experience	privacy policy compliance Self-efficacy (PPCSE)	Privacy Compliance Learning Behavioral Intention (PCLBI)	PPCSE → PCLBI

Liang & Xue (2010)	TTAT	-	Self-efficacy (SE)	Avoidance Motivation (AM)	SE → AM
Bulgurcu et al. 2010)	TPB, PMT, RCT, DT	-	Self-efficacy to comply (SETC)	Intention to Comply (ITC)	SETC → ITC
Johnston & Warkentin, (2010)	PMT, FAM	Perceived threat & Perceived vulnerability	Self-efficacy (SE)	Behavioral Intentions (BI)	SE → BI
Herath and Rao (2009)	GDT, PMT, TPB, DTPB, OC.	-	Response efficacy (RE)	Security Policy Attitude (SPA)	RE→ SPA

Lee & Larsen (2009)	TPB; TAM; IDT, PMT	-	Self-efficacy (SE)	Intention to Adopt Malware (ITAM) by SME	SE → ITAM by SME
Liang & Xue (2009)	TTAT	-	Self-efficacy (SE)	Perceived Avoidability (PA)	SE → PA
Rheea et al., (2009)	TPB	Computer experience; Security breach incidents; General controllability	Self-efficacy in information security (SEIS)	Information Security Practice Behavior (ISPB)	SEIS→ ISPB
Dinev & Hu (2007)	TPB	-	Self-efficacy (SE)	perceived behavioral control (PBC); Behavioral intention (BI)	SE → PBC SE → BI

Note. TTS: Transactional Theory of stress; FIT: Feelings-as-information theory; TMSC: The Transactional Model of Stress and Coping; HSM: Holistic Stress Model; AT: Ambidexterity Theory IPT: Information Processing Theory; ST: Schema Theory TPB: theory of planned behavior; TTAT: technology threat avoidance theory; TAM: technology acceptance model; IDT: Innovation Diffusion Theory; PMT: Protection motivation theory; GDT: General Deterrence Theory; SCT: Social cognitive theory; DTPB: Decomposed Theory of Planned Behavior; OC: Organizational Commitment; FAM: fear appeal model; RCT: rational choice theory; DT: Deterrence theory; SLT: Social learning theory; SET: social exchange theory; SET: Self-efficacy Theory; PMD: Protection motivation deterrence; IMB: Information Motivation Behavioral Skills Model; CT: Communication theory; IT: Institutional theory; HMSAM: hedonic-motivation system adoption model; ITIT: IT Identity Theory.

Table A2. The gap analysis of mobile identity protection in information systems literature

Protective Motivation Literature			**Adapted Theories**	**Protection Context**			**SE**		**TA**		**PA**		**Protection Environment**			
Authors	Objective	Findings		Information Protection	Privacy Protection	Identity Protection	Direct impact	Moderation	Threat Severity	Threat Vulnerability	Direct impact	Mediation	Mobile	Computer	Network	IT
Ogbanufe & Baham (2023)	Understanding the impact of regret and online security threats response on individuals' usage of Multi-Factor Authentication (MFA)	The emotion of regret heightens threat appraisals and consequently motivates protection and use of MFA	PMT	✓					✓	✓				✓		

Ogbanufe & Pavur (2022)	Explore the impact of regret and fear on individuals' protection motivation toward the threat of identity theft.	While fear impacts individuals only on low threats, regret influences protective behavior in low and high threats of identity theft attacks.	PMT	✓		Gap1	✓	Gap2	✓	✓		Gap3		✓		
Ameen et al. (2021)	Understanding of Employees' information-security behavior	Cybersecurity policies and cultural differences predict different threats specific to smartphone use.	PMT; GDT; TRA	✓			✓		✓	✓			✓			
Vedadi & Warkentin (2020)	Investigated how providing popular information can trigger individuals' behavior and can subsequently influence security behaviors	Users develop a higher protection motivation when they become aware of the widespread use of a certain security technology	EDT	✓			✓		✓	✓	✓			✓	✓	
Bose and Leung (2019)	Exploring the Effects of Adopting Identity Theft Countermeasures on Firm Value	Adopting Identity Theft Countermeasures increases the short and long-term market of adopting firms.	CUT	✓										✓	✓	✓
Verkijika (2019)	Investigated the impact of Self-efficacy, anticipated regret, and gender on Avoidance motivation	Anti-phishing self-efficacy, regret, and gender influence mobile phishing avoidance behavior.	TTAT	✓			✓				✓		✓			

Bélanger & Crossler (2019)	Understanding protective behavior in mobile devices	Mobile privacy protection self-efficacy affects the intention toward mobile information protection.	TPB	✓	✓		✓				✓		✓			
Crossler & Bélanger (2019)	Examining the Privacy Knowledge–Belief Gap and the protective behavior in a mobile context.	Individual privacy skills influence their motivational behavior toward mobile privacy-protective behavior.	IMBS	✓	✓		✓						✓			
Martens, de Wolf, & de Marez (2019)	Investigate motivations to protect oneself against scams, malware, and cybercrime.	Findings suggest significant differences when protecting oneself against 'technical' cybercrimes (malware) compared to more 'social' cybercrimes (scams)	PMT	✓			✓		✓	✓	✓					
Gao et al. (2018)	Explore the dark side of ubiquitous connectivity enabled by smartphone-based SNS.	Ubiquitous connectivity increases SNS users' discontinuous usage intention by raising privacy concerns and protection motivation.	PMT; IPT	✓	✓								✓		✓	

Craig, Thatcher, & Grover (2019)	Developing IT Identity Threat as a new construct to understand employees; resistance behavior to IT use	IT identity Protection behavior may develop resistance response to identity threat sources, such as intergroup conflict, verification prevented, and meaning change.	IDT													✓
Verkijika (2018)	Understanding the anticipated regret of not adhering to a security behavior in smartphones.	Anticipated regret mediating the relationship between mobile security intention and behavior	PMT	✓			✓		✓	✓			✓			
Menard, Warkentin, & Lowry (2018)	Evaluate individual cultural values to motivate employees to perform secure behaviors.	An Individual's orientation toward collectivism has an impact on the intention not to perform secure behaviors.	PMT	✓					✓	✓						✓
Thompson, McGill, & Wang (2017)	Understand the security behavior of mobile users at home	Both self-efficacy and perceived threats have a positive impact on users' security behavior.	PMT	✓			✓		✓	✓			✓	✓		

Note. SE: Self-efficacy; TA: Threat Appraisal; PA: Protection Awareness; TPB: Theory of planned behavior; PMT: Protection motivation theory; USP: Unified security practices; ABM: Awareness boundary model; SET: Self-efficacy theory; IMBS: information–motivation–behavioral skills model.; Grey boxes indicate a gap in the literature. CUT: Cue Utilization Theory; EDT: Expectation-disconfirmation theory; TTAT: Technology Threat Avoidance Theory (TTAT); CCM: Cognition Change Model; IDT: Identity Theory. IPT: Information Processing Theory; GDT: General Deterrence Theory; TRA: Theory of Reasoned Action

Acknowledgments: The authors would like to thank Fundação para a Ciência e a Tecnologia (FCT) regarding the program UIDB/04152/2020-Centro de Investigação em Gestão de Informação—MagIC (NOVA IMS).

doi: https://doi.org/10.3127/ajis.v28.4397