Received 14 November 2024
Revised 3 June 2025
13 March 2026
Accepted 10 May 2026

Identifying factors influencing the employee's intention with self-protective behaviors against phishing attacks

Seyedeh OMSalameh Pourhashemi
Islamic Azad University Central Tehran Branch, Tehran, Iran
Bilal Naqvi
Department of Software Engineering, Lappeenrannan-Lahden Teknillinen Yliopisto, Lappeenranta, Finland, and
Mehdi Azizi Mehmandoost
ICT Research Institute, Tehran, Iran

Abstract

Purpose – Phishing is a form of social engineering attack that poses an increasingly significant risk in today's digital era. The challenges and implications associated with phishing affect both end users and organizations. However, organizations face particularly serious consequences, as a single employee's error can compromise the security and privacy of the entire organization.

Design/methodology/approach – This research examines the factors influencing employees' intentions to adopt self-protective behaviors against phishing attacks using protection motivation theory (PMT). The study sample comprised 200 employees working in higher education institutions (HEIs).

Findings – Perceived vulnerability, perceived risk, perceived barriers, response efficacy and self-efficacy influence behavioral intention. The findings also identify significant positive associations between conceptual knowledge and self-efficacy, procedural knowledge and self-efficacy and perceived vulnerability and information security awareness.

Originality/value – This study contributes to the state of the art by extending PMT by integrating conceptual and procedural knowledge to explain employees' self-protective behaviors against phishing attacks. It also provides empirical evidence from the higher education sector, a context that has received limited attention in prior phishing research.

Keywords Anti-phishing, Employees' intention, Phishing, Protection motivation theory

Paper type Research article

1. Introduction

Information and communication technology (ICT) continues to advance rapidly and has become an integral part of daily life. While ICT helps people do their work quickly, simply, and effectively, it has also enabled mechanisms that, if exploited, can hamper all the benefits ICT has on offer (Desolda *et al*., 2023). Phishing is one such mechanism that attackers employ to gather sensitive information from victims; this includes, for instance, authentication credentials, encryption keys, among others (Chiew *et al*., 2018). A phishing attack is a form of social engineering attack, and its vectors include email, messaging services, and social media platforms, etc. Phishing attacks can have significant repercussions, including financial loss, identity theft, and reputational damage. In addition, attackers also use phishing emails to trick victims into installing spyware, impersonating websites, etc. (Harrison *et al*., 2015). The

Information Technology & People
Vol. 39 No. 8, 2026
pp. 50-79
Emerald Publishing Limited
e-ISSN: 1758-5813
p-ISSN: 0959-3845
DOI 10.1108/ITP-11-2024-1429

consequences of phishing attacks are not limited to individuals; organizations and companies are also affected. For instance, an organization could suffer serious consequences if an employee clicks on a link in a phishing email. The situation is further complicated by the fact that employees possess varying levels of cybersecurity awareness and skills (De Bona and Paci, 2020).

Furthermore, phishing is a highly context-specific attack mechanism that also relies on the victim's ability to distinguish between legitimate and phishing content. Several attributes of human behavior, such as degree of knowledge, attitudes, and behaviors, influence their phishing detection and prevention abilities. In addition, in case of a successful phishing attack, it is the people rather than technology who are blamed as the weakest link in the security chain. Therefore, the knowledge and awareness of phishing attacks, their vectors, and several mechanisms being employed to execute them are of prime importance (Mohammad *et al*., 2022; Nachin *et al*., 2019). Susceptibility to phishing varies among individuals according to their awareness levels. Moreover, there is a consensus that boosting cybersecurity awareness helps mitigate phishing attacks targeted towards an organization (Krawczyk-Sokołowska and Caputa, 2023; Mohammad *et al*., 2022; Nachin *et al*., 2019).

Having mentioned the importance of training and awareness activities in shaping employees' anti-phishing abilities, it is relevant to consider that all such efforts are still susceptible to employees' non-compliant behaviors and careless attitudes. It is therefore vital to identify factors influencing the employees' intentions to comply with self-protective behaviors against phishing attacks. This will also enable the development of more focused anti-phishing training and awareness activities. Therefore, with a rationale to identify such factors, the primary research question for this study was formulated: *What factors influence employees' intentions to engage in self-protective behaviors against phishing attacks?* In line with the research question, a study featuring ($n = 200$) employees working at Iranian higher education institutions (HEIs) was conducted. The justification for considering HEIs in this research lies in their increased exposure to phishing threats, mainly due to their access to sensitive information and university systems. Moreover, the context of HEIs has received limited attention in prior phishing research.

Furthermore, an important consideration before investigating the research question was the selection of an appropriate theoretical framework (Kanth *et al*., 2013). Therefore, this study adopts the Protection Motivation Theory (PMT) proposed by Rogers (1975). Based on the PMT, this study presents an empirically validated structural model that examines employees' intentions to adopt self-protective behaviors in response to phishing attacks. The study not only contributes to the body of knowledge but also provides practical insights for cybersecurity awareness within organizations to limit phishing attacks and improve employees' anti-phishing capabilities.

The remainder of the paper is organized as follows. Section 2 presents the background and related work. Section 3 presents the hypotheses and outlines the research model. Section 4 presents the details of the research method adopted for this study. Section 5 presents the analysis and findings. Section 6 encompasses the discussion and limitations of the study, and Section 7 concludes the paper.

2. Background and related work

2.1 Background

Phishing is a form of social engineering aimed at deceiving individuals into revealing information against their interests (Abbate, 2020). The attacker (phisher) typically sends emails or messages that mimic legitimate communications from reputable companies or websites. These deceptive messages often contain hyperlinks that direct victims to counterfeit websites that closely resemble legitimate ones. Once there, victims are prompted to enter sensitive information such as credit card numbers or passwords. The malicious actors behind these schemes then exploit this information to pilfer money or assume the victim's identity.

Phishing attacks manifest primarily through fraudulent emails (Naqvi *et al.*, 2023), spoofed websites (Chiew *et al*., 2018), phone calls (Gupta *et al*., 2018), and text messages (Alani and Tawfik, 2022), impersonating trustworthy entities such as banks, social media platforms, or government agencies. In some instances, these attacks result in the installation of hazardous malware (Hong, 2012). Essentially, a phishing attack combines social engineering with technical tactics to persuade users into unwittingly providing sensitive information, which the attacker can then exploit for financial gain (Kirda and Kruegel, 2006).

Furthermore, a generic phishing attack typically unfolds in four stages (Parekh *et al*., 2018),: (1) website creation: the attacker crafts and establishes a fake website, meticulously designed to resemble an authentic one, (2) targeted communication: the attacker then sends a URL link to the victim, masquerading as a legitimate organization, user, or association, (3) temptation and visit: the unsuspecting victim is tempted to visit the injected fake website, and (4) data surrender: tragically, the targeted victim clicks on the deceptive link and unintentionally provides valuable personal data. By leveraging this individual information, the attacker engages in impersonation activities.

Moreover, Basit *et al*. (2021) highlight that a surge in phishing attacks in recent years has affected Internet users, governments, and service-providing organizations alike. A significant challenge arises when the pretext of a phishing email aligns seamlessly with a user's work context, making detection more difficult (Steves *et al*., 2020). Additionally, Naqvi *et al.* (2023) reveal that while technical safeguards such as spam filters and email authentication mechanisms reduce the number of malicious phishing attempts, users still experience a lot of phishing emails. Consequently, the research has increasingly focused on understanding behavioral factors that influence users' responses to phishing attempts.

2.2 Related work

The prior research aimed at understanding behavioral factors in the context of phishing attacks has examined mainly two user categories: end-users and employees. Studies on end-users investigate how individuals perceive and respond to phishing attacks, highlighting the role of cognition, attention, and risk perception in phishing susceptibility (e.g. Downs *et al*., 2006; Sheng *et al*., 2010; Vishwanath *et al*., 2011). Moreover, the end-user category represents a diverse range of users with different backgrounds, abilities, education, and other factors influencing their behaviors when confronted with phishing attacks. The second category of users considered extensively in prior literature is the organizational employees. This is important because employees represent one of the primary targets of phishing attacks in organizational environments. Broadly, the research conducted in organizational contexts explores how work-related factors, organizational policies, and security awareness influence phishing susceptibility (Parsons *et al*., 2015; Canfield *et al*., 2016; Wash, 2020). Since the focus of the current work is on factors influencing employees' intentions with self-protective behaviors against phishing attacks, we will discuss the related work concerning employees as primary users within organizational environments. A brief classification of related work on employees can be made into (1) studies examining employees' phishing behavior, (2) studies examining employees' cybersecurity behavior in general, and (3) studies examining employee security policy compliance. We discuss each of these categories in turn.

Among the studies examining employees' phishing behavior, Shahbaznezhad *et al*. (2021) discuss the factors that influence employees in clicking phishing emails from a broader socio-technical perspective. The authors use a socio-technical model by combining behavioral theories such as Protection Motivation Theory (PMT) and habit theory for investigating individual factors, Theory of Planned Behavior (TPB) for investigating organizational factors, and Deterrence Theory for investigating technological factors. The findings indicate that habit and protective countermeasures impact clicking phishing emails. Moreover, the authors argue that the results of the study can be used to design phishing simulation exercises. In addition, Buckley *et al*. (2023) examine the relationship between sociodemographic factors,

information processing factors, and risky and secure email behaviors. The findings indicate that the likelihood of clicking a phishing link was lower in the case of employees who trusted their intuition and paid more attention to the sender's email address.

Furthermore, Tian *et al*. (2023) apply self-determination theory to study the susceptibility of phishing attacks across industries. The authors consider finance and non-finance organizations for the study. The findings reveal that there is a varying susceptibility to phishing techniques across industries. Moreover, Frank *et al*. (2022) employ contextual theory to examine contextual factors that influence employees' phishing susceptibility. The authors develop and validate a multi-dimensional model including social, task, and physical components to explain why employees are likely to fall for phishing emails. The authors identify that context plays a crucial role in developing a thorough understanding of phishing susceptibility. More recently, Pratama *et al*. (2025) explore factors influencing the behavioral intention of (state-owned enterprise) employees towards phishing emails. The authors apply protection motivation theory to examine how threat awareness, security knowledge, perceived vulnerability, perceived severity, response efficacy, and self-efficacy influence employees' intention to avoid clicking phishing links. The findings indicate that self-efficacy, perceived vulnerability, and perceived severity significantly influence employees' security intention, while threat awareness and security knowledge indirectly shape these perceptions. The results highlight the need for enterprises to enhance employee perceptions of severity, self-efficacy, and security behavior intention through focused intervention and practical training.

In addition, from the perspective of the effectiveness of anti-phishing training, Sumner *et al*. (2022) examine factors that impact the effectiveness of anti-phishing training and study the correlation between personality traits and phishing susceptibility. The findings revealed that anti-phishing training positively impacts participants' knowledge about phishing attacks, their behavior, and their ability to identify phishing attacks. Moreover, the findings also reveal that the differences in education impact the efficacy of training across people with varying education levels.

From the perspective of studies examining employees' cybersecurity behavior in general, Sulaiman *et al*. (2022) examine the cybersecurity behavior of governmental employees by applying the protection motivation theory. The findings identify that perceived severity, vulnerability, response efficacy, and self-efficacy significantly influence employee cybersecurity behavior.

Furthermore, from the perspective of studies examining employee security policy compliance, Akib *et al*. (2025) conducted a study featuring employees from the banking sector. The research focuses on how policy provision, security training, and awareness activities influence employees' security compliance behavior. The authors apply the theory of planned behavior and protection motivation theory to develop an integrated framework for testing. The findings reveal that policy provision and security training and awareness activities significantly impact cybersecurity awareness, thereby influencing compliance attitude and intention to drive protective behavior. In addition, Lee *et al*. (2023a) examine the impact of employees' psychological contract breach on cybersecurity policy compliance. The study considers both intrinsic and extrinsic factors using the theory of planned behavior and general deterrence theory. The findings reveal that employee motivation and organizational fairness impact cybersecurity compliance intentions. Moreover, from the perspective of insider threats, Safa *et al*. (2019) present a conceptual framework to mitigate insider attacks using deterrence and prevention approaches. The findings reveal that the severity and certainty of sanctions significantly influence employees' attitudes and prevent them from engaging in security misconduct.

Having discussed the related works, this study aims to examine the *factors that influence employees' intention to engage in self-protective behaviors against phishing attacks*. It is relevant to note that a recent study by Pratama *et al*. (2025) examined employees' behavioral intentions to avoid clicking phishing email links within a protection motivation framework. While their study provides valuable insights into phishing-related decision-making, it focuses

primarily on a specific organizational context, a specific phishing vector (email), and a limited set of behavioral factors. However, the current study aims to provide a broader understanding of the factors influencing employees' intentions to engage in self-protective behaviors against phishing attacks.

Furthermore, academic employees were selected as participants for this study, as they are particularly vulnerable to phishing attacks due to the openness, accessibility, and collaborative nature of academic environments. Academic institutions, such as universities, store large amounts of sensitive information, including personal data, academic grades, and research records, which makes them an attractive target for attackers. In addition, with the constantly changing staff and students, there are more gaps in anti-phishing preparedness as compared to other sectors.

Moreover, based on the literature review, it was found that this topic has received less attention in technologically developing countries like Iran. In addition, the variables considered in this study have not been widely examined simultaneously, particularly within organizational contexts. To the best of the authors' knowledge, the PMT-based model developed during this study has not been tested previously alongside the variables included in the proposed conceptual model. A summary of the related works discussed in this section is presented in Table 1.

3. Research model and hypothesis

3.1 Protective motivation theory (PMT)

Rogers (1975) developed PMT to describe the mental activity humans participate in to control their conduct in the face of danger to their health and the safety of others. The hypothesis is grounded in the observation that people conduct risk assessments to evaluate current health and safety conditions and engage in related coping strategies. Their decision to take precautions is influenced by this assessment process, which may lead to adaptive or maladaptive behavior. In the context of cybersecurity, PMT has been extensively used over the years, and in this aspect, the theory appears to hold up well (Abumalloh *et al*., 2021; Alsharida *et al*., 2023; De Kimpe *et al*., 2022; Menard *et al*., 2018). The theory holds that people engage in self-protective behaviors if they perceive a threat as substantial. Threat assessments appear to have a direct and favorable influence on information technology (IT) professionals' online behavior in online environments (Safa *et al*., 2015). The effectiveness of addressing these threats can be assessed using PMT, in addition to individual threat assessments (Rogers, 1975, 1983).

Furthermore, it is this aspect of PMT that enables an understanding of how individuals respond to perceived threats and adopt protective behaviors across various domains, which makes PMT relevant for this study's context. PMT suggests that individuals' motivation to stay protected is determined by two appraisal processes: their desire to take precautions is influenced by how they perceive the threat ("threat appraisal") and how they evaluate their options for coping with it ("coping appraisal"). The threat appraisal considers both the perceived likelihood of affecting them (perceived vulnerability), the perceived severity and probable repercussions of the threat. In addition, coping appraisal considers three factors: (1) self-efficacy, which refers to an individual's confidence in their ability to deal with a threat, (2) response efficacy, which refers to the benefit of this response is expected to be concerning the threat, and (3) response cost, which refers to the individuals estimate of how much it will cost in terms of money, time, or effort to respond to the threat (Kemp, 2023). In the context of phishing attacks, employees evaluate the potential risks associated with phishing attacks (e.g. loss of data, damage to reputation, monetary loss) and assess their ability to detect and avoid such threats. In addition, factors such as response efficacy, self-efficacy, and perceived barriers influence employees' coping appraisal, thereby shaping their motivation to adopt self-protective behaviors. Therefore, PMT provides a suitable theoretical framework for

Table 1. Summary of the related work

	Ref.	Context	Investigated topics and factors
1	Shahbaznezhad *et al*. (2021)	Employees' Behavior in Phishing Attacks	This study examines three categories of factors, i.e. individual, organizational, and technological, which influence users' intentions when encountering phishing emails. *Theory:* Protection Motivation Theory/Theory of planned behavior/ Deterrence theory
2	Buckley *et al*. (2023)	Employee phishing email behaviors	This study investigates the interplay among sociodemographic factors, cybersecurity training, phishing email typology, information processing, and both risky and secure email-response behaviors. *Theory: Not Specified*
3	Tian *et al*. (2023)	Phishing susceptibility across industries	This research examines how industry-specific characteristics affect susceptibility to phishing influence techniques. *Theory:* Self-Determination Theory
4	Frank *et al*. (2022)	Employees' phishing susceptibility	The study investigates a multidimensional model that incorporates three contextual components: social, task, and physical. This model explains why an employee may be susceptible to phishing attempts or, conversely, why they might resist them. *Theory:* Contextual theory
5	Pratama *et al*. (2025)	Employee phishing email behaviors	The study investigates the factors influencing employees' intentions to refrain from clicking links in phishing emails. The findings reveal that self-efficacy, perceived vulnerability, and perceived severity significantly influence employees' behavioral intentions. *Theory:* Protection Motivation Theory
6	Sumner *et al*. (2022)	Effectiveness of Anti-Phishing Training	This study investigates the influence of various factors on the effectiveness of anti-phishing training. It also explores the correlation between personality traits and an individual's susceptibility to phishing attempts. *Theory:* Technology threat avoidance theory
7	Sulaiman *et al*. (2022)	Cybersecurity behavior among governmental employees	This study examines the factors influencing the cybersecurity behavior of governmental employees. It addresses an often-ignored topic: how government employees handle cybersecurity risks. The findings reveal that high motivation, high severity, response efficacy, and self-efficacy are critical in exercising cybersecurity behavior. *Theory*: Protection Motivation Theory
8	Akib *et al*. (2025)	Cybersecurity compliance among banking employees	This study examines the role of policy provision and security training and awareness activities in the cybersecurity compliance behavior of banking employees. *Theory:* Protection Motivation Theory and Theory of Planned Behavior
9	Lee *et al*. (2023a)	Cybersecurity policy compliance among employees	The study examines both intrinsic and extrinsic factors that affect employees' psychological contract breach and cybersecurity compliance. *Theory:* Theory of Planned Behavior and General Deterrence Theory

(*continued*)

Table 1. Continued

	Ref.	Context	Investigated topics and factors
10	Safa *et al*. (2019)	Employee Misconduct	This study concerns the insider threats to organizations in the context of cybersecurity. A novel framework is presented to mitigate insider threats by integrating multiple factors. *Theory:* Deterrence Theory, Situational Crime Prevention Theory, Theory of Planned Behaviour

explaining how employees develop intentions to adopt self-protective behaviors when facing phishing attacks.

The research model is grounded in PMT and is presented in Figure 1. The model uses PMT coupled with the dimensions of conceptual and procedural knowledge to predict employees' intention to adhere to self-protective measures against phishing attacks. In the research model, perceived threat severity, perceived vulnerability, and perceived risk represent *threat appraisal constructs*, while perceived barriers, response efficacy, and self-efficacy represent *coping appraisal constructs* influencing employees' behavioral intentions. The study is based on the premise that both procedural and conceptual knowledge improve users' ability to counter phishing attacks. McCormick (1997) reveal that one's knowledge can be influenced by learning procedural and conceptual knowledge associated with it. Plant (1994) argue that conceptual knowledge is close to the idea of *"know that"*, and procedural knowledge, *"know-how"*, in which both ideas are imperative to educate one to resist phishing attacks. Furthermore, Plants' work identifies that conceptual knowledge permits an individual to explain why, and hence the difference between knowing how and knowing why. It is relevant to note that all direct hypotheses (H1-H9) are depicted in the research model; indirect hypotheses (H10-H11) are tested statistically and are not visually represented for clarity. All hypotheses are presented in the subsequent sub-sections with relevant details.

3.2 Perceived threat severity

People and businesses are increasingly urged to educate themselves and to become aware of techniques to reduce their susceptibility to phishing (Torten *et al*., 2018). Nevertheless, research demonstrates that both behavioral intention and perceived threat are positively correlated (Vrhovec and Mihelič, 2021). The study by Rainear and Christensen (2017) found that perceived severity is one of the strongest predictors of intention, providing additional evidence for the association between perceived severity and intention. In this study, perceived severity refers to employees' evaluation of the seriousness of phishing attacks and their potential negative consequences. Consequently, the hypothesis (H1) is proposed:

H1. Immersive technology capabilities have a significantly positive impact on perceived usefulness.

3.3 Perceived vulnerability

A person's perception of their perceived vulnerability is how likely they believe they are to face dangerous circumstances, such as becoming a victim of cybercrime (Ifinedo, 2012). According to Vance *et al*. (2012), perceived vulnerability is the risk that a person would be the victim of an unanticipated incident (such as a data breach incident). Perceived vulnerability is the employee's estimation of how vulnerable their company is to phishing attacks if no precautions are taken to stop them (Piquero *et al*., 2005). In this study, perceived vulnerability refers to employees' assessments of their susceptibility to phishing threats in the absence of

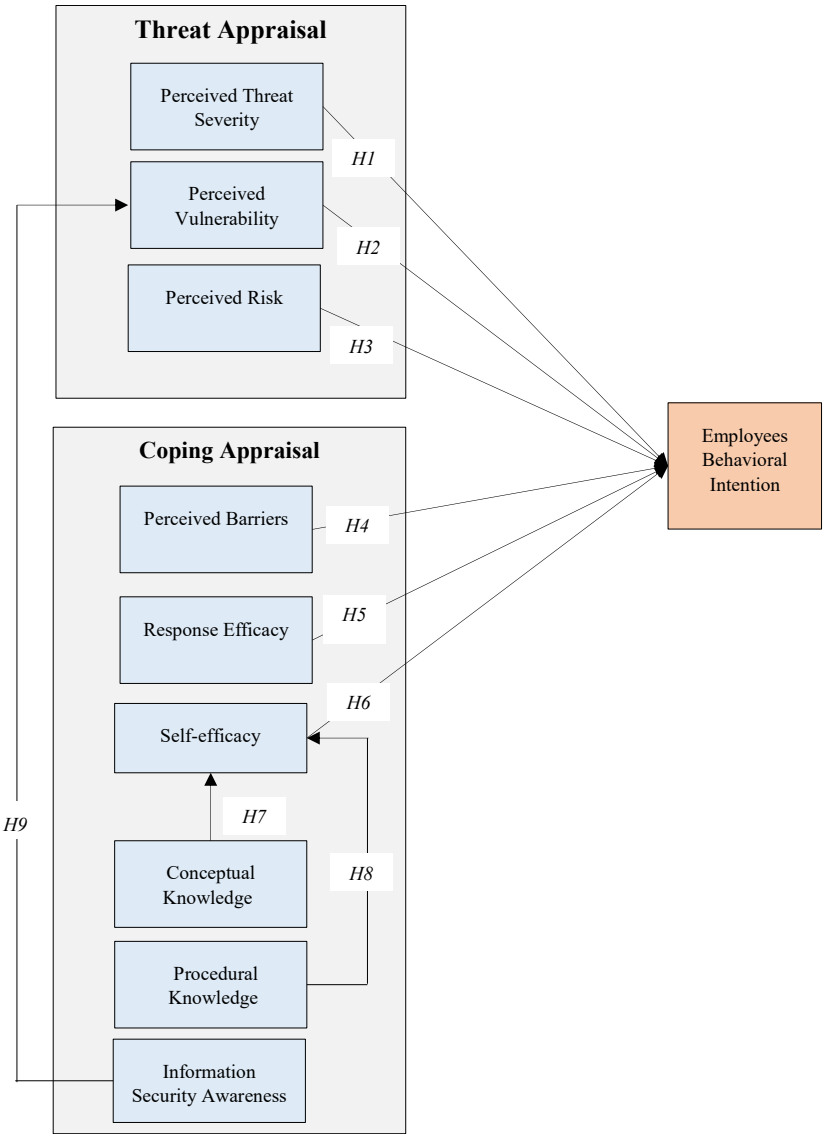

Figure 1. Research model

protective measures. In addition, according to numerous research studies (Beu *et al*., 2023; Vance *et al*., 2012; Wright *et al*., 2014), people who perceive vulnerability as being high exhibit a stronger intention to observe mitigation advice. Perceived vulnerability also significantly affects coping responses.

Furthermore, an employee who is more familiar with the information systems in the company will be more equipped to take precautions when there is a suspected risk. Existing studies have shown that employees are more likely to adopt cybersecurity policies when they believe they are vulnerable to cyberattacks (Siponen *et al*., 2014). Therefore, the following hypothesis (H2) is proposed:

H2. The perceived vulnerability has a significantly positive impact on employees' intentions and their protective measures against phishing attacks.

3.4 Perceived risk

Perceived risk is a person's perception of uncertainty regarding the safety of engaging in a particular action (Mun *et al*., 2013). Every person has a unique perception of the risk associated with the behavior they engage in. According to Zimbardo (2007), individuals have distinct levels of familiarity with issues; some consider a problem more pertinent to them than others do, and vice versa. The level of participation in this behavior varies with the emotions a person associates with a situation and with the potential financial loss if an attack occurs (Orgill *et al*., 2004). Pyszczynski *et al*. (1997) argue that when people feel threatened, their behavior depends on how many risks they can tolerate. The severity of an attack and the amount of loss they believe will result from a risk determine this alteration, a psychological response. The inclination to behave adversely is constantly impacted by perceived risk (Mun *et al*., 2013; Ridinger *et al*., 2016). When people perceive a greater risk of cyberattacks, they pay more attention to potential harm. Therefore, people are required to pay greater attention when the program has not completely removed the threat, such as in phishing emails, thereby increasing perceived risk. Therefore, the following hypothesis (H3) is proposed:

H3. Perceived risk has a significantly negative impact on employees' intentions and their protective measures against phishing attacks.

3.5 Perceived barriers

The concept of perceived barriers was introduced in cybersecurity literature by Claar and Johnson (2012). Moreover, Yoon *et al*. (2012) employed the response costs construct, which refers to the perceived effort, time, or resources required to engage in protective behavior. Both studies suggest that protective behavior tends to decrease as barriers and response costs increase. Perceived barriers reflect a person's concern about the challenges they would encounter in acquiring the new behavior. According to Lee *et al*. (2008), it is directly correlated with preventive security behaviors. According to Djatsa (2019), consumers' online security habits are influenced by perceived restrictions. Therefore, perceived barriers in this study refer to obstacles that a person perceives will prevent them from taking action to prevent phishing attempts. Considering the above, the following hypothesis (H4) is proposed:

H4. Perceived barriers have a significantly positive impact on employees' intentions and their protective measures against phishing attacks.

3.6 Response efficacy

In Protection Motivation Theory (PMT), coping appraisal includes response efficacy and self-efficacy (Vrhovec and Mihelič, 2021). Response efficacy refers to an individual's belief that a recommended protective action will effectively mitigate or prevent a threat. Scarpa and Thiene (2011) define response efficacy as the belief that adopting a particular adaptive response can help protect individuals from potential threats. In the context of phishing attacks, response efficacy reflects employees' beliefs that adopting recommended security practices can effectively reduce the risk of phishing attacks. Prior research suggests that intention to adopt a behavior is positively impacted by response efficacy (Bayl-Smith *et al*., 2022; Verkoeyen and Nepal, 2019). Response efficacy in this study refers to an employee's belief that self-protective measures can effectively reduce the risk of falling victim to phishing attacks. Hence, the following hypothesis (H5) is proposed:

H5. Response effectiveness has a significantly positive impact on employees' intentions and their protective measures against phishing attacks.

3.7 Self-efficacy

The concept of self-efficacy relates to an individual's belief in their ability to handle possible (threat) scenarios, assuming they are aware of their abilities and characteristics (Bandura, 1982). In the context of phishing attacks, self-efficacy refers to an individual's confidence in their ability to spot a phishing attempt. According to Torten *et al.* (2018), user adoption of appropriate security behaviors is significantly influenced by self-efficacy. An individual is more likely to have positive thoughts (i.e. an attitude) towards an action if they believe they are capable of performing it (Herath and Rao, 2009). Self-efficacy may be related to attitude towards conduct (Pang *et al.*, 2021; Zhang *et al.*, 2020). Concerning personal information security practices, self-efficacy has been shown to have an illustrative impact on both technological usage and cybersecurity behavior (Rhee *et al.*, 2009). Therefore, the following hypothesis (H6) is proposed:

H6. Self-efficacy has a significantly positive impact on employees' intentions and their protective measures against phishing attacks.

3.8 Conceptual knowledge

Conceptual knowledge consists of the understanding and ideas that enable an individual to think about and interpret concepts (i.e. "know that") in a technological setting (Plant, 1994). Without employees' active participation, it is hard for organizations to safeguard their assets (Ahmed *et al.*, 2014). Employees must, in essence, know what to do and how to do it; as a result, they must have the necessary knowledge and skills (know-how) to contribute to cybersecurity hygiene. Although awareness campaigns and training are unquestionably important and helpful, they often prove to be insufficient (Alahmari *et al.*, 2022). In existing research, the relationship between self-efficacy and knowledge has been examined (Hsu *et al.*, 2007; Hu, 2010). For instance, users are more likely to take appropriate precautions to avoid phishing when they are informed of the associated risks. Thus, the following hypothesis (H7) is proposed:

H7. Conceptual knowledge has a positive influence on self-efficacy.

3.9 Procedural knowledge

Procedural knowledge (knowing how) involves the execution of tasks, processes, and procedures. Arachchilage and Love (2014) identify that risks associated with phishing are reduced when both conceptual and procedural expertise are utilized. The authors further examined how conceptual and procedural knowledge affect users' confidence in their ability to deal with phishing threats. The research demonstrates that the combination of conceptual and procedural knowledge positively impacts users' confidence. Furthermore, Liang and Xue (2009) identify that both procedural knowledge and conceptual knowledge have an impact on self-efficacy. Thus, the following hypothesis (H8) was formulated:

H8. Procedural knowledge has a positive influence on self-efficacy.

3.10 Information security awareness

A crucial component in the development of beliefs, attitudes, and intentions toward policy compliance is information security awareness. It can be interpreted as general knowledge about information security and an understanding of organizational security rules (Bulgurcu *et al.*, 2010). Individuals who are generally aware of security risks may nevertheless click on

unknown links or attachments in certain situations (Moody *et al*., 2017). One or more information security responses may be undertaken in response to information security awareness (Yoon *et al*., 2012). In addition, Hughes (2016) note that improving corporate security attitudes can be achieved by increasing employee understanding of information security policies and enforcing them. The following hypothesis (H9) is proposed:

H9. Information security awareness has a positive influence on perceived vulnerability.

3.11 Mediating role of self-efficacy

Self-efficacy refers to an individual's perception of what they can accomplish with their abilities (Zainal *et al*., 2022) and is linked to knowledge (Arachchilage and Love, 2014). Employees confident in their experience and ability to provide valuable knowledge are more likely to exhibit both a stronger intention to share knowledge and more frequent knowledge-sharing behaviors. Moreover, employees with more knowledge or expertise are confident and have a better intention to share knowledge, either voluntarily or when requested to share (Wipawayangkool and Teng, 2019). Conversely, if an employee is not confident about the information, they will have many concerns about providing or sharing wrong or inaccurate information (Razmerita *et al*., 2016). For example, when users are more confident in taking the necessary precautions to avoid phishing attempts (self-efficacy), they are aware and knowledgeable of the risks involved, resulting in the avoidance of phishing attacks (Arachchilage and Love, 2014). A high level of ability to acquire anti-phishing knowledge (self-efficacy) may reduce the risk of phishing victimization (Martens *et al*., 2019).

Arachchilage and Hameed (2017) identify the need to cultivate threat perception among users to motivate them to avoid phishing attacks. Self-efficacy is associated with better threat perception, i.e. the more knowledgeable employees are about phishing threats, the higher their threat perception. Moreover, Hsu *et al*. (2007) and Hu (2010) identify a co-relationship between self-efficacy and knowledge. For example, a user is more confident to take action against a phishing attack if they know how to avoid phishing threats (Arachchilage and Love, 2014). Self-efficacy plays a pivotal mediating role between knowledge and behavioral intention in phishing contexts (Baral and Arachchilage, 2019; Lee *et al*., 2023b). It influences whether employees feel confident enough to apply their procedural and conceptual knowledge to mitigate phishing attacks. Both types of knowledge are foundational for employees to build a robust defense against phishing. Procedural knowledge equips employees with practical skills, while conceptual knowledge fosters a deeper understanding of the threat landscape, enabling more informed decision-making.

The mediating role of self-efficacy in the relationship between procedural and conceptual knowledge and employees' intention to counter phishing attacks is crucial. Procedural and conceptual knowledge jointly enhance self-efficacy, which, in turn, shapes employees' attitudes and intentions toward mitigating phishing attacks. Effective cybersecurity strategies must therefore integrate knowledge enhancement with efforts to build and sustain self-efficacy, ensuring employees are both capable and confident in defending against phishing threats. Existing research shows that higher levels of both procedural and conceptual knowledge contribute positively to enhancing self-efficacy (Baral and Arachchilage, 2019). When employees understand not only how to detect phishing attempts but also why these attacks occur and what their potential consequences are, their confidence in managing these threats increases. This heightened self-efficacy then motivates protective behaviors, such as scrutinizing suspicious messages, refraining from sharing sensitive information, and reporting phishing attempts.

Therefore, self-efficacy mediation occurs because procedural knowledge alone may not directly translate into intention unless employees believe they can effectively apply that knowledge. Self-efficacy boosts this belief, thereby increasing motivation and intention to act. This is supported by findings that self-efficacy influences motivation and work performance,

often through enhancing intrinsic motivation or perceived workplace support (Çetin and Aşkun, 2019; Na-Nan and Sanamthong, 2020). Therefore, the following hypotheses (H10, H11) are proposed:

H10. Self-efficacy mediates the relationship between Conceptual knowledge and Employees' intention.

H11. Self-efficacy mediates the relationship between Procedural Knowledge and Employees' intention.

4. Research method

This study adopted a quantitative research approach to examine the factors influencing employees' intentions to engage in self-protective behaviors against phishing attacks. The constructs used in this study were measured using previously validated scales adapted from prior studies in cybersecurity and phishing literature. Adapting established measurement instruments helps ensure the reliability and validity of the constructs. Specifically, the items measuring perceived threat severity (PS1-PS3) and perceived vulnerability (PV1-PV3) were adapted from Zahedi *et al.* (2015). In addition, the constructs for measuring perceived risk (PR1-PR4) and perceived barriers (PB1-PB4) were adapted from Anwar *et al.* (2017) and Ng *et al.* (2009). Response efficacy items (RE1-RE3) were adapted from Boss *et al.* (2015). However, self-efficacy, conceptual, and procedural knowledge constructs (SE1-S4, CK1-CK3, PK1-PK3, respectively) were adapted from Arachchilage and Love (2014). Information security awareness was measured using items (ISA1-ISA3) adapted from Zhan *et al.* (2019), and employees' intention to adopt self-protective behaviors was measured using items (IB1-IB3) adapted from Anwar *et al.* (2017). The constructs and variables used in the study are presented in Table 2.

All constructs were measured using a five-point Likert scale, with 1 denoting "strongly disagree" and 5 denoting "strongly agree." The complete questionnaire was reviewed by a panel of four subject experts to ensure content validity and alignment with the research problem. The questionnaire was then uploaded to Google Forms for data collection. The respondents in the study included employees working at universities in Iran. In addition, the reliability and construct validity of the scales were further assessed in this study using statistical measures including Cronbach's alpha, composite reliability (CR), and average variance extracted (AVE).

Moreover, a convenience sampling technique was used for sampling. Non-probability convenience sampling is one of the most common sampling techniques used in social sciences and behavioral intention-related studies (Singh *et al.*, 2024; Sun *et al.*, 2016; Yeng *et al.*, 2022). It is also an efficient way of collecting information in a limited time (Bougie and Sekaran, 2019). During the data collection phase, the respondents were made aware of ethical concerns followed in the study and were assured that their personal details and details of their responses would not be disclosed at any stage of this study. It is relevant to state that G*Power 3.3 software was used for sample size calculation. The power test parameter was set to 0.8 (Cohen, 2013), and the effect size was set to 0.15 (Faul *et al.*, 2007). The test dictated a minimum of 157 cases for the sample size; however, in the current study, 200 respondents completed the survey questionnaire.

To test the proposed research model and hypotheses, the study employed Partial Least Squares Structural Equation Modeling (PLS-SEM). This method is appropriate for examining complex relationships among latent constructs and is widely used in behavioral and information systems research. The analysis followed a two-step approach in line with Hair *et al.* (2021). First, the measurement model was evaluated to assess the reliability and validity of the constructs. Second, the structural model was assessed to examine the relationships among constructs and test the proposed hypotheses. More details about the analysis are discussed in the following section.

Table 2. Research constructs and items

Latent variable	Items
Perceived threat severity (Zahedi *et al*., 2015)	
PS1	Considering the severity of damage caused by a phishing attack, I perceive it to be (very low/very high)
PS2	The potential damage from a phishing attack is (very low/very high)
PS3	My possible loss due to a phishing attack is (very low/very high)
Perceived vulnerability (Zahedi *et al*., 2015)	
PV1	In my opinion, the probability of encountering a phishing attack is (very low/very high)
PV2	The likelihood that I will experience a phishing attack is (very low/very high)
PV3	I believe the chances of encountering a phishing attack are (very low/very high)
Perceived risk (Anwar *et al*., 2017; Ng *et al*., 2009)	
PR1	I am aware that my organization's data and resources may be compromised if I don't pay adequate attention to phishing attack tricks
PR2	I am not convinced that an information security breach can occur at my workplace through clicking email links
PR3	I check the links in my email or SMS to ensure they are not harmful before clicking
PR4	I avoid opening email attachments from unknown senders
Perceived barriers (Anwar *et al*., 2017; Ng *et al*., 2009)	
PB1	Checking the security of an email with an attachment is inconvenient for me
PB2	I don't have enough time to check for phishing clues in an email
PB3	I lack the knowledge to identify phishing clues in an email
PB4	I haven't received adequate training to recognize phishing-related clues
Response efficacy (Boss *et al*., 2015)	
RE1	I believe that adopting security software and practices effectively protects against phishing attacks
RE2	Adopting security software and practices is effective in countering phishing attempts
RE3	By adopting security software and practices, a computer is more likely to be protected from phishing attacks
Self-efficacy (Arachchilage and Love, 2014)	
SE1	I am confident that I can successfully gain anti-phishing knowledge even if I have never learned it before
SE2	I believe I can gain anti-phishing knowledge with the available resources for reference
SE3	I am confident that I can successfully acquire anti-phishing knowledge independently
SE4	I am confident that I can successfully gain anti-phishing knowledge with ample time
Conceptual knowledge (Arachchilage and Love, 2014)	
CK1	I have the intention to obtain anti-phishing knowledge to protect against phishing attacks
CK2	I predict that I will acquire anti-phishing knowledge to safeguard against phishing attacks
CK3	I feel that I do not desire to acquire anti-phishing knowledge to avoid phishing attacks
Procedural knowledge (Arachchilage and Love, 2014)	
PK1	I possess an overall awareness of potential security threats and their negative consequences
PK2	I frequently update my anti-phishing knowledge to defend against suspected 'phishing' URLs
PK3	Updating anti-phishing knowledge is essential to counter phishing attacks
Information security awareness (Zhan *et al*., 2019; Bulgurcu *et al*., 2010)	
ISA1	I possess an overall awareness of potential security threats and their negative consequences
ISA2	I have sufficient knowledge about the effects of potential security problems
ISA3	I understand the concerns regarding the risks posed by information security
Employees' intention (Anwar *et al*., 2017)	
IB1	I maintain my computer's anti-virus software up to date
IB2	I observe unusual computer behaviors/responses (e.g. pop-up windows in the computer, etc.)
IB3	I don't open email attachments from unknown senders

5. Data analysis and findings

As part of the analysis, the reliability and validity of the constructs were evaluated (measurement model) using criteria such as outer loadings, Cronbach's alpha, composite reliability, and average variance extracted. Moreover, the structural model was analyzed to test the hypothesis and evaluate the relations among constructs in the research model. The results of these assessments are presented in respective sub-sections. In addition, the demographic details of the study participants are presented in Table 3.

5.1 Measurement model assessment

Measurement model assessment results are presented in Table 4. The indicator reliability was assessed by examining the outer loadings of each indicator on its respective construct. All outer loading values exceeded the threshold of 0.70, indicating that the indicators adequately represent underlying constructs. The convergent validity was evaluated using the Average Variance Extracted (AVE). The AVE values for all latent variables were more than 0.50, indicating that the constructs explain more than half of the variance of their indicator. The high outer loadings of the indicators further support the convergent validity of the constructs. The internal consistency reliability was evaluated using Cronbach's alpha and Composite Reliability (CR). As shown in Table 4, all variables had values more than the recommended threshold of 0.70. These results indicate satisfactory internal consistency reliability for all constructs. Finally, multicollinearity among indicators was assessed using the Variance Inflation Factor (VIF). All VIF values were below the threshold of 5.0, indicating no multicollinearity concerns in the measurement model.

Table 3. Respondent characteristics

	Total ($N = 200$)	
	N	Percentage (%)
Gender		
- Male	104	52
- Female	96	48
Age		
- Under 25	18	9
- 25–34 years old	59	29.5
- 35–44 years old	108	54
- 45 years old and above	15	7.5
Level of education		
- Bachelor	48	24
- Master	137	68.5
- Ph.D.	15	7.5
Work experience		
- Less than 5 years	8	4
- 5–10 years	76	38
- 11–15 years	104	52
- 16 years or more	12	6
Average hours spent per week on the internet		
- 6–10 h	31	15.5
- 11–15 h	145	72.5
- More than 16 h	24	12

Table 4. Reliability and validity measures

Indicators	Construct	Convergent validity Outer loading (>0.70)	AVE (>0.50)	Internal consistency reliability Cronbach's alpha (>0.70)	Composite reliability (>0.70)	Collinearity statistics VIF (<5.0)
PS1	Perceived threat severity (PS)	0.865	0.730	0.815	0.890	2.062
PS2		0.876				2.062
PS3		0.822				1.555
PV1	Perceived vulnerability (PV)	0.836	0.721	0.823	0.886	3.653
PV2		0.854				1.349
PV3		0.857				3.805
PR1	Perceived risk (PR)	0.838	0.708	0.863	0.907	1.923
PR2		0.827				1.946
PR3		0.839				2.042
PR4		0.861				2.237
PB1	Perceived barriers (PB)	0.744	0.639	0.810	0.876	1.546
PB2		0.749				1.561
PB3		0.837				2.971
PB4		0.861				3.147
RE1	Response efficacy (RE)	0.766	0.667	0.750	0.857	1.334
RE2		0.823				1.664
RE3		0.859				1.692
SE1	Self-efficacy (SE)	0.854	0.781	0.907	0.934	2.168
SE2		0.904				3.285
SE3		0.895				3.078
SE4		0.881				2.930
CK1	Conceptual knowledge (CK)	0.794	0.644	0.722	0.844	1.503
CK2		0.870				1.640
CK3		0.738				1.296
PK1	Procedural knowledge (PK)	0.856	0.785	0.863	0.916	1.976
PK2		0.894				2.362
PK3		0.908				2.460
ISA1	Information security awareness (ISA)	0.884	0.759	0.844	0.904	2.797
ISA2		0.873				2.752
ISA3		0.856				1.584
IB1	Behavioral intention (IB)	0.765	0.704	0.788	0.877	1.428
IB2		0.898				2.202
IB3		0.850				1.913

Furthermore, discriminant validity for the constructs was first assessed using the Fornell-Larcker criterion (Fornell and Larcker, 1981). According to Hair *et al.* (2019), this criterion requires that the square root of the Average Variance Extracted (AVE) for each construct be greater than its correlations with other constructs. The results from the Fornell-Larcker criterion analysis are presented in Table 5. The results indicate that this condition was satisfied for all constructs, thereby confirming discriminant validity.

Moreover, discriminant validity was evaluated using the Heterotrait-Monotrait ratio (HTMT) (Henseler *et al.*, 2015). The HTMT values should be below the threshold of 0.9 to indicate adequate discriminant validity (Hair *et al.*, 2019). As shown in Table 6, all HTMT values ranged from 0.351 to 0.804 and were below the threshold value. Therefore, the results confirm that discriminant validity was established among the constructs.

To further assess discriminant validity, cross-loadings were examined. The results are presented in Table 7, which indicates that all items load higher on their respective constructs than on other constructs, confirming discriminant validity (Hair *et al.*, 2019).

Table 5. Fornell-Larcker criterion analysis

	CK	IB	ISA	PB	PR	PS	PV	PK	RE	SE
CK	*0.802*									
IB	0.391	*0.839*								
ISA	0.411	0.549	*0.871*							
PB	0.451	0.580	0.456	*0.799*						
PR	−0.299	−0.555	−0.378	−0.484	*0.841*					
PS	0.317	0.609	0.458	0.597	−0.598	*0.855*				
PV	0.396	0.504	0.612	0.456	−0.334	0.436	*0.849*			
PK	0.594	0.614	0.532	0.675	−0.499	0.511	0.512	*0.886*		
RE	0.275	0.553	0.407	0.424	−0.440	0.513	0.485	0.376	*0.817*	
SE	0.534	0.486	0.461	0.474	−0.433	0.395	0.377	0.646	0.324	*0.884*

Note(s): CK: Conceptual Knowledge; IB: Behavioral Intention; ISA: Information Security Awareness; PB: Perceived Barriers; PR: Perceived Risk; PS: Perceived threat severity; PV: Perceived Vulnerability; PK: Procedural Knowledge; RE: Response Efficacy; SE: Self-efficacy

Table 6. HTMT ratio

	CK	IB	ISA	PB	PR	PS	PV	PK	RE	SE
CK										
IB	0.508									
ISA	0.528	0.677								
PB	0.579	0.724	0.547							
PR	0.376	0.675	0.439	0.575						
PS	0.404	0.755	0.554	0.737	0.713					
PV	0.487	0.575	0.651	0.515	0.351	0.478				
PK	0.746	0.738	0.627	0.804	0.575	0.605	0.564			
RE	0.373	0.721	0.506	0.536	0.535	0.655	0.587	0.465		
SE	0.654	0.566	0.535	0.550	0.483	0.453	0.404	0.722	0.386	

Note(s): CK: Conceptual Knowledge; IB: Behavioral Intention; ISA: Information Security Awareness; PB: Perceived Barriers; PR: Perceived Risk; PS: Perceived threat severity; PV: Perceived Vulnerability; PK: Procedural Knowledge; RE: Response Efficacy; SE: Self-efficacy

5.2 Structural model assessment

Once the measurement model's validity and reliability were established, the structural model was evaluated. The hypotheses were tested using a bootstrapping approach with 1,000 samples in SmartPLS, as proposed by Hair *et al.* (2016). In addition, the coefficient of determination (R^2) was examined to assess the model's explanatory power. The results (see Table 8) show that the R^2 value for behavioral intention (IB) is 0.555, indicating that the six external factors accounted for approximately 55.5% of the variance in IB. In addition, the R^2 values for perceived vulnerability (PV) and self-efficacy (SE) are 0.375 and 0.452, respectively. R^2 values greater than 0.33 indicate strong predictive precision (Chin, 1998); therefore, R^2 values presented in Table 8 demonstrate moderate predictive accuracy and a sizable effect on employees' intentions in this study (Hair *et al.*, 2019). Furthermore, the predictive relevance Q^2 was assessed using the blindfolding procedure in SmartPLS (see Table 8). A Q^2 value greater than zero indicates that the model has predictive relevance. The results reveal Q^2 values of 0.374,0.221, and 0.344 for IB, PV, and SE, respectively. was that all Q^2 values were >0. Cross-validated redundancy was used to assess the route model's capacity to predict endogenous parameters indirectly from their relevant latent variables, leveraging the

Table 7. Loadings and cross-loading of measures

	CK	IB	ISA	PB	PK	PR	PS	PV	RE	SE
CK1	0.794	0.325	0.250	0.368	0.414	−0.216	0.233	0.357	0.291	0.393
CK2	0.870	0.356	0.400	0.434	0.560	−0.290	0.314	0.363	0.257	0.495
CK3	0.738	0.251	0.326	0.270	0.441	−0.204	0.203	0.227	0.107	0.386
IB1	0.210	0.765	0.373	0.399	0.412	−0.500	0.421	0.347	0.507	0.311
IB2	0.391	0.898	0.466	0.531	0.563	−0.475	0.580	0.488	0.460	0.434
IB3	0.368	0.850	0.536	0.523	0.562	−0.427	0.523	0.425	0.433	0.469
ISA1	0.375	0.473	0.884	0.361	0.509	−0.305	0.409	0.488	0.297	0.481
ISA2	0.417	0.548	0.873	0.404	0.510	−0.341	0.428	0.447	0.367	0.459
ISA3	0.302	0.430	0.856	0.420	0.392	−0.339	0.370	0.628	0.390	0.298
PB1	0.248	0.437	0.347	0.744	0.393	−0.290	0.445	0.315	0.266	0.310
PB2	0.354	0.453	0.324	0.749	0.507	−0.347	0.480	0.286	0.301	0.437
PB3	0.436	0.479	0.386	0.837	0.622	−0.447	0.477	0.450	0.382	0.394
PB4	0.395	0.485	0.398	0.861	0.620	−0.452	0.504	0.399	0.398	0.373
PK1	0.515	0.480	0.401	0.609	0.856	−0.384	0.396	0.429	0.319	0.523
PK2	0.563	0.565	0.483	0.585	0.894	−0.454	0.447	0.474	0.286	0.571
PK3	0.504	0.582	0.520	0.603	0.908	−0.482	0.508	0.458	0.390	0.618
PR1	−0.197	−0.499	−0.340	−0.406	−0.421	0.838	−0.524	−0.288	−0.462	−0.431
PR2	−0.256	−0.442	−0.263	−0.377	−0.389	0.827	−0.574	−0.300	−0.383	−0.299
PR3	−0.281	−0.458	−0.339	−0.399	−0.446	0.839	−0.443	−0.286	−0.303	−0.387
PR4	−0.278	−0.464	−0.327	−0.445	−0.422	0.861	−0.473	−0.251	−0.325	−0.333
PS1	0.218	0.490	0.375	0.574	0.430	−0.491	0.865	0.376	0.441	0.318
PS2	0.295	0.539	0.428	0.523	0.460	−0.474	0.876	0.363	0.449	0.372
PS3	0.294	0.530	0.370	0.437	0.419	−0.566	0.822	0.378	0.425	0.320
PV1	0.281	0.315	0.364	0.306	0.324	−0.171	0.249	0.836	0.352	0.263
PV2	0.382	0.539	0.689	0.489	0.543	−0.402	0.507	0.854	0.486	0.391
PV3	0.312	0.347	0.380	0.293	0.357	−0.190	0.252	0.857	0.344	0.254
RE1	0.274	0.434	0.312	0.242	0.324	−0.234	0.406	0.530	0.766	0.253
RE2	0.212	0.414	0.347	0.351	0.278	−0.330	0.403	0.314	0.823	0.230
RE3	0.193	0.499	0.339	0.433	0.318	−0.493	0.445	0.349	0.859	0.303
SE1	0.441	0.501	0.453	0.480	0.636	−0.415	0.404	0.356	0.305	0.854
SE2	0.518	0.410	0.397	0.422	0.569	−0.427	0.372	0.329	0.268	0.904
SE3	0.438	0.375	0.336	0.393	0.505	−0.307	0.276	0.255	0.226	0.895
SE4	0.487	0.415	0.430	0.370	0.556	−0.368	0.328	0.380	0.335	0.881

Table 8. Coefficient of determination (R^2) and predictive relevance (Q^2)

	R^2	Q^2
Behavioral intention (IB)	0.555	0.374
Perceived vulnerability (PV)	0.375	0.221
Self-efficacy (SE)	0.452	0.344

associated structural relations. Hair *et al*. (2021) note that Q^2 values of 0.02, 0.15, and 0.35, respectively, indicate strong predictive relevance for IB and SE and moderate predictive relevance for PV (Hair *et al*., 2021).

As mentioned earlier, bootstrapping was employed to estimate significance of the path relationships in the model by generating standard errors of each hypothesis tested (see Figure 2). This was done in line with the procedure recommended by Hair *et al*. (2019). The testing results of the structural model are presented in Table 9.

As shown in Table 9, the hypotheses H1-H9 were supported for the direct linkages. Employees' intentions to engage in self-protective behaviors against phishing attacks were positively and significantly affected by PS ($\beta = 0.192$, $p < 0.05$) and PV ($\beta = 0.138$, $p < 0.05$); hence, H1 and H2 were supported. H3 was supported, as a negative relationship was observed between PR and IB ($\beta = -0.162$, $p < 0.05$). Employees' intention to engage in self-protective behaviors against phishing attacks is positively and significantly correlated with PB ($\beta = 0.174$, $p < 0.05$), RE ($\beta = 0.196$, $p < 0.05$), and SE ($\beta = 0.142$, $p < 0.05$); hence, H4, H5, and H6 were supported. Additionally, a significant positive relationship was found between CK and SE ($\beta = 0.232$, $p < 0.05$), between PK and SE ($\beta = 0.508$, $p < 0.05$), and between ISA and PV ($\beta = 0.612$, $p < 0.05$); hence, H7, H8, and H9 were supported. Moreover, the results of the mediator study of self-efficacy showed that it does not mediate the relationship between conceptual knowledge and behavioral intention ($\beta = 0.064$, $t = 1.695$, $p > 0.05$); however, it mediates the relationship between procedural knowledge and behavioral intention ($\beta = 0.072$, $t = 1.987$, $p < 0.05$); hence H10 was not supported, however, H11 was supported.

6. Discussion

6.1 Key findings

The purpose of this study was to investigate the factors that affect employees' intentions to engage in self-protective behaviors against phishing attacks using the Protection Motivation Theory (PMT). As discussed earlier, perceived threat intensity affects employees' intentions. These results are in line with earlier research (Menard *et al*., 2018; Rogers, 1975). This finding is also consistent with more recent research on phishing attacks, demonstrating that employees who perceive a higher level of threat severity are more likely to adopt protective behaviors against phishing attacks (Shahbaznezhad *et al*., 2021; Buckley *et al*., 2023). Additionally, behavioral intention and perceived risk are inversely related: perceived risk of an employee's adherence to the anti-phishing security policy increases the likelihood of security risk behavior and reduces phishing attacks. This implies that employees who believe they can avoid phishing scams are more vulnerable.

Furthermore, the findings indicate a positive correlation between behavioral intention and perceived barriers. Perceived barriers are obstacles that can hinder secure behavior when faced with phishing attacks. Eliminating perceived barrier threats will enhance phishing awareness. This finding aligns with previous studies (Safa *et al*., 2019; Sulaiman *et al*., 2022), indicating that organizational and individual barriers can hinder employees' compliance with security practices and phishing mitigation strategies. The results also demonstrate that employees' intentions to adhere to self-protective practices against phishing attacks are influenced by response efficacy and self-efficacy. This means that by giving employees the right

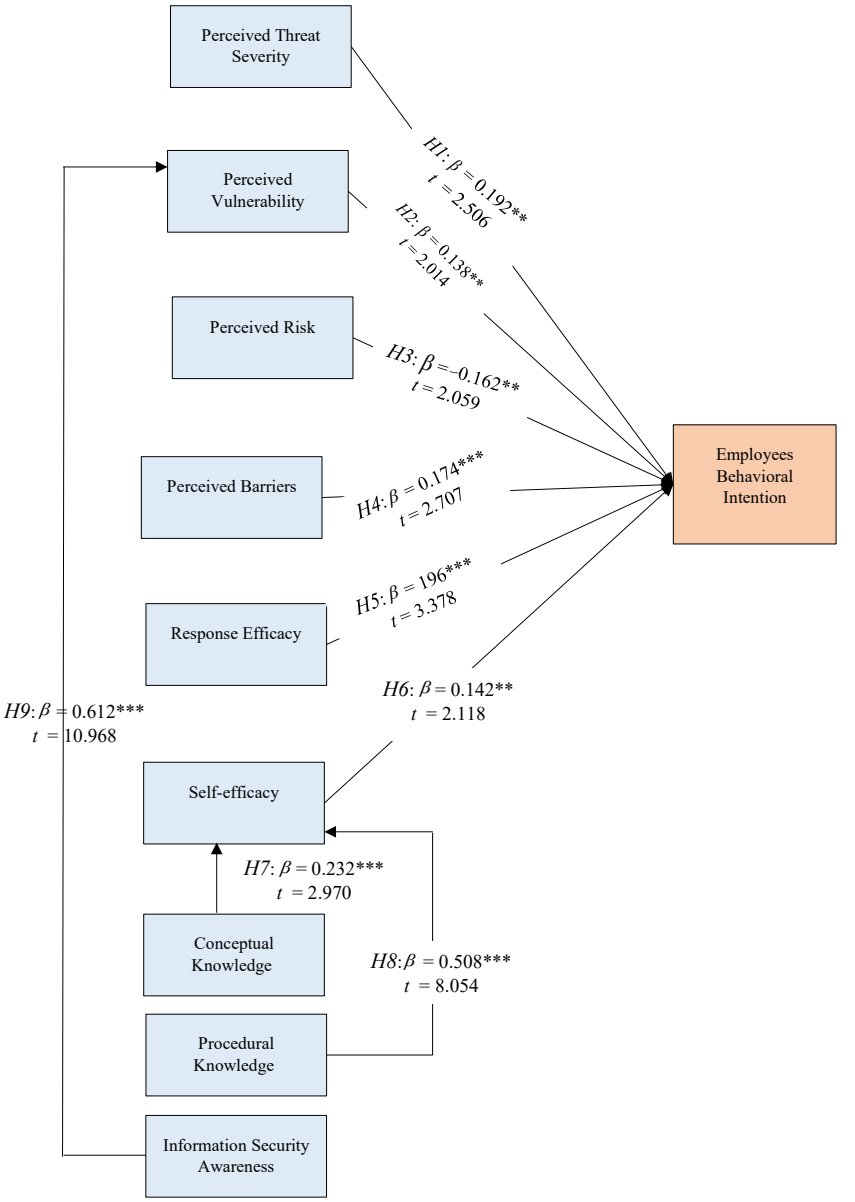

Figure 2. Results of the structural model assessment

information, they would be more aware of how to practice self-protective behaviors. Strong and effective informational messages can improve employees' behavioral intentions when faced with security and environmental hazards, encouraging them to adopt protective behaviors against phishing attempts (Ertan *et al.*, 2020; Herath and Rao, 2009). This is consistent with prior studies (Lee *et al.*, 2023a; Tian *et al.*, 2023), which emphasize the critical role of self-efficacy in cybersecurity behavior.

Table 9. The results of the hypothesis testing

Hypothesis		β	Effect size (f^2)	*t*-value	*p*-values	Evaluation
H1	PS → BI	0.192	0.039	2.506	0.012**	Supported
H2	PV → BI	0.138	0.028	2.014	0.044**	Supported
H3	PR → BI	−0.162	0.034	2.059	0.040**	Supported
H4	PB → BI	0.174	0.037	2.707	0.007***	Supported
H5	RE → BI	0.196	0.055	3.378	0.001***	Supported
H6	SE → BI	0.142	0.032	2.118	0.034**	Supported
H7	CK → SE	0.232	0.064	2.970	0.003***	Supported
H8	PK → SE	0.508	0.305	8.054	0.000***	Supported
H9	ISA → PV	0.612	0.599	10.968	0.003***	Supported
H10	CK → SE → BI	0.033	0.064	1.695	0.090	Not supported
H11	PK → SE → BI	0.072	0.305	1.987	0.047**	Supported

Note(s): Statistical significance **$p < 0.05$, ***$p < 0.01$. PS: Perceived threat Severity; PV: Perceived Vulnerability; PR: Perceived Risk; PB: Perceived Barriers; RE: Response Efficacy; SE: Self-efficacy; CK: Conceptual Knowledge; PK: Procedural Knowledge; ISA: Information Security Awareness; BI: Behavioral Intention

Furthermore, the results show that both conceptual and procedural knowledge affect self-efficacy. Employees with strong conceptual knowledge are better equipped to understand the rationale for their tasks and the broader organizational context. This understanding reduces uncertainty and ambiguity, which are common sources of workplace anxiety and self-doubt. When employees grasp the "why" and "how" behind their work, they are more likely to feel capable of making informed decisions and tackling new challenges, thereby enhancing their self-efficacy. The impact of conceptual knowledge on employees' self-efficacy is profound and multifaceted. By enabling employees to understand complex systems, develop creative solutions, and continuously grow, conceptual knowledge lays the groundwork for high self-efficacy. This finding extends previous research on security knowledge and phishing awareness. Prior studies (Akib *et al*., 2025; Sumner *et al*., 2022) have shown that users' understanding of phishing attacks improves their ability to recognize malicious communications and strengthens their confidence in handling such threats. Organizations that prioritize conceptual learning and foster supportive environments empower their employees to perform at their best, drive innovation, and adapt to an ever-evolving workplace (Daud *et al*., 2025; Zaki *et al*., 2019).

Moreover, as employees repeatedly perform tasks, they develop procedural knowledge and proficiency. This hands-on competence directly boosts their confidence, reinforcing the belief that they can handle similar or even more complex tasks in the future. Therefore, employees with strong procedural knowledge adapt more quickly to changes, such as new technologies or updated protocols. Their ability to transfer learned skills to new situations fosters a resilient sense of self-efficacy. Hence, employees with strong procedural knowledge adapt more quickly to changes, such as new technologies or updated protocols. Conceptual and procedural knowledge impact employees' self-efficacy in combating phishing attacks. This enhanced self-efficacy not only improves individual behavior but also fosters a security-conscious culture within organizations, ultimately reducing the risk and impact of phishing attacks. The self-efficacy component received particular emphasis in the study, as it is correlated with users' knowledge levels. This finding is consistent with earlier studies suggesting that practical knowledge plays a crucial role in enabling employees to apply security practices effectively in real-world situations (Frank *et al*., 2022; Tian *et al*., 2023).

The results also indicate that perceived vulnerability is directly impacted by information security awareness. Information security awareness plays a critical role in determining employees' perceived vulnerability to phishing attacks. Information security awareness

programs aim to educate employees about cyber threats, how to recognize phishing attempts, and the appropriate responses. Research indicates that such awareness significantly influences employees' perceived vulnerability and their subsequent behavior when confronted with phishing emails (Li *et al*., 2019; Shahbaznezhad *et al*., 2021). This suggests that awareness not only raises recognition skills but also shapes employees' confidence and perceived ability to handle phishing threats. While awareness alone does not eliminate risk, it is a vital component in reducing the success of phishing attacks and mitigating their psychological and organizational consequences. Continuous, adaptive training programs, combined with supportive technical and cultural measures, are necessary to strengthen this human firewall and protect organizations against phishing threats. Nevertheless, these results provide evidence of a connection among business information security knowledge, adoption of more secure practices, and perceived reduction in vulnerability. Organizations that prioritize cybersecurity are likely to have employees accountable for cybersecurity, have implemented security controls, and are more likely to know how to avoid phishing scams. Similar conclusions have been reported in previous studies examining organizational cybersecurity awareness programs. For instance, Sulaiman *et al*. (2022) and Shahbaznezhad *et al*. (2021) found that increased information security awareness significantly improves employees' ability to identify phishing attempts and reduces organizational vulnerability to phishing attacks.

In addition, with respect to mediation, the results indicate that self-efficacy did not mediate the relationship between conceptual knowledge and behavioral intention. Therefore, conceptual knowledge is necessary, but not always sufficient, to increase self-efficacy or translate into stronger intentions to mitigate phishing attacks. Even with adequate conceptual knowledge, employees may lack sufficient self-efficacy to act, or self-efficacy may not significantly influence their intention to engage in protective behaviors. This could be because conceptual knowledge alone does not provide the practical skills or procedural knowledge users need to feel capable of taking effective action. The lack of an effect of mediating self-efficacy on the relationship between conceptual knowledge and employees' intention in phishing attacks stems from the complex and sometimes counterintuitive relationships among knowledge, confidence, attitudes, and behavior. Conceptual knowledge alone does not reliably increase self-efficacy, and self-efficacy does not always mediate the impact of knowledge on intention. This finding differs from some prior studies that reported stronger links between knowledge and protective behavioral intentions in cybersecurity contexts (Sumner *et al*., 2022). The difference may be explained by the fact that conceptual understanding alone may not provide the practical skills necessary for employees to respond effectively to phishing attacks.

Finally, the results show that self-efficacy mediates the relationship between procedural knowledge and behavioral intention. It transforms knowledge into actionable intentions by boosting confidence, shaping protective attitudes, and motivating proactive behaviors. Organizations aiming to mitigate phishing risks must prioritize employee self-efficacy and equip employees with the knowledge needed to counter evolving phishing threats effectively. Employees with high self-efficacy feel capable of applying their procedural knowledge effectively. This confidence motivates them to engage in protective behaviors such as scrutinizing emails and resisting phishing attempts. Without this belief, even knowledgeable employees may hesitate or fail to act, reducing the impact of their knowledge on intention (Lee *et al*., 2023b). This finding also supports recent research emphasizing that practical experience and applied security knowledge are essential for translating cybersecurity awareness into protective behaviors in organizational environments (Buckley *et al*., 2023; Frank *et al*., 2022).

6.2 Theoretical implications

This article represents an initial step toward comprehending the effectiveness of self-protective behaviors against phishing attacks, which aim to enhance employees' resilience in the digital era. To gain a deeper understanding of responses to phishing attacks within business

contexts, concerted efforts must be made to improve data collection. The study's specific findings provide actionable insights for information security professionals, policymakers, and other stakeholders combating phishing attacks. These insights can be adapted to enhance employees' cyber resilience against cybercrime, including ransomware attacks (de Bruijn and Janssen, 2017).

This study contributes to understanding self-protective behaviors against phishing attacks by emphasizing the importance of Protection Motivation Theory. Specifically, it broadens the existing limited focus on phishing attacks while highlighting the impact of employees' intention to comply with self-protective measures. The research model delves into various factors associated with PMT, providing valuable insights for mitigating cyber risks.

According to this study's findings, the PMT model was extended to include conceptual knowledge, procedural knowledge, self-efficacy, and information security awareness. Moreover, the mediating role of self-efficacy (not examined in prior studies) was considered to address a key gap in the state of the art.

6.3 Practical implications

The findings of the current study underscore the importance of self-efficacy in the implementation of security behaviors. From the employees' perspective, the results highlight the importance of developing both conceptual and procedural knowledge to effectively recognize and respond to phishing attempts. Employees who understand not only how to identify phishing messages but also why such threats occur are more likely to adopt proactive security behaviors. Therefore, individuals should actively engage in cybersecurity training programs and continuously update their knowledge of emerging phishing techniques. Employees' ability to adhere to security practices, even when unsupervised, is crucial. Consequently, it is advisable to continue the phishing-related awareness, education, and training programs to enhance self-efficacy (Goel and Jain, 2018; Verkijika, 2019). Recognizing that each employee starts with varying levels of technical knowledge, competence, and awareness, those overseeing anti-phishing efforts and informational websites should demonstrate empathy and understanding. This approach will help organizational managers recognize and appreciate the diverse values, beliefs, and traits that employees bring from various groups and across the organization as a whole. Building on this study's findings, managers and supervisors should prioritize both conceptual and procedural knowledge. By doing so, employees can better safeguard themselves and their data by adhering to protective behaviors against phishing attacks. For organizations, the findings emphasize the need to design comprehensive security awareness programs that combine theoretical understanding of cyber threats with practical detection skills. Training initiatives should therefore incorporate interactive exercises, simulated phishing campaigns, and scenario-based learning to strengthen employees' self-efficacy and reduce susceptibility to phishing attacks.

Security professionals can strike a balance by training university employees to handle phishing threats responsibly. Additionally, organizations can implement additional security controls to support employees in adopting security practices, particularly in critical departments. Furthermore, because perceived barrier risk predicts self-reported security behavior risk, addressing perceived barrier risks may improve conscious security behavior. Based on this study, several proactive measures should be implemented by organizational managers and government bodies to mitigate phishing attacks. From a policy perspective, the findings suggest that governmental agencies and regulatory bodies should support the development of national cybersecurity awareness programs and guidelines for employee security training. Policymakers can also encourage organizations, particularly in the higher education sector, to adopt standardized cybersecurity awareness frameworks and provide incentives for implementing continuous phishing awareness training. Within the university community, leaders must implement targeted training, awareness campaigns, and educational

initiatives to counteract this susceptibility trend. Given the open and collaborative nature of academic environments, universities should also integrate cybersecurity awareness into staff development programs and institutional policies. Such initiatives can help reduce vulnerabilities arising from high staff turnover, diverse user populations, and extensive information sharing within academic institutions. Additionally, leveraging intrinsic incentives derived from these findings can enhance awareness of phishing.

Beyond training, it is crucial to enhance employees' awareness to mitigate security risks. Developing social and cultural factors that promote conscious care behavior among employees is vital. Equipping employees with robust knowledge and skills in phishing-related security practices can also reduce perceived barriers to effective security. In addition, innovative training technologies, such as virtual reality, augmented reality, and extended reality, can play a pivotal role in fostering longer-lasting psychological incentives to avoid phishing susceptibility. By embracing these state-of-the-art tools, organizations can empower their workforce to stay vigilant and resilient against phishing threats.

6.4 Limitations

The integrated model was validated as a strong predictor of employees' intention to adhere to self-protective measures against phishing attempts, yielding several interesting findings. However, it is worth noting some limitations of this study. Firstly, data for this study were collected at a single point in time and were based on a cross-sectional design. A longitudinal data-collection method would have been more advantageous, as it would enable more precise analysis and allow researchers to track the evolution of the variables. Additionally, by employing a convenience sample that may not accurately reflect the broader population, this study merely indicates participants' intention to adhere to self-protective practices. Future research could compare similar frameworks or analyze the impact of employees' intentions using samples more representative of the general population.

While the current study primarily focuses on evaluating specific interventions, we recognize the importance of addressing gender imbalances and other relevant demographic factors in future research projects. Although gender was not included as a control variable in this study, accounting for gender balance in subsequent research is essential for a comprehensive investigation.

7. Conclusion

Given the continued rise in phishing attacks over the years, it is evident that technology alone is insufficient to protect against phishing. However, it also requires positive intent and responsible behavior among human users to remain protected online. This paper aimed to identify factors influencing employees' intention to adopt self-protective behaviors against phishing attacks. The paper presented a case study of employees in an academic setting. The findings have implications for other sectors as well, as phishing vectors include mainly email systems and web applications, tools that are standardized and used across several sectors.

The study used PMT to study the relationships between perceived threat severity, perceived vulnerability, perceived risk, perceived barriers, response efficacy, and self-efficacy. The outcomes demonstrate that behavioral intention is impacted by the perceived risk of undesirable outcomes. The outcomes also showed a favorable relationship between conceptual knowledge, procedural knowledge, and self-efficacy. Additionally, the direct effect of information security awareness on perceived vulnerability was found. Overall, the results showed that behavioral intention to engage in self-protective activities against phishing attempts is driven by social pressures and one's beliefs. By increasing users' understanding of phishing attacks through widespread awareness efforts, security policymakers could use the study's findings to further encourage self-protective practices. By highlighting the importance of cultivating an information security culture within a business and its subgroups, this study

makes a valuable contribution to the field of information security research. Organizations should ensure their cybersecurity strategies account for these concerns.

References

Abbate, P. (2020), *Internet Crime Report 2020*, Federal Bureau of Investigation, Internet Crime Complaint Center, available at: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (accessed 15 July 2021).

Abumalloh, R.A., Asadi, S., Nilashi, M., Minaei-Bidgoli, B., Nayer, F.K., Samad, S., Mohd, S. and Ibrahim, O. (2021), "The impact of coronavirus pandemic (COVID-19) on education: the role of virtual and remote laboratories in education", *Technology in Society*, Vol. 67, 101728, doi: 10.1016/j.techsoc.2021.101728.

Ahmed, G., Ragsdell, G. and Olphert, W. (2014), "Knowledge sharing and information security: a paradox?", pp. 1083-1090.

Akib, A.A.P.M., Candiwan, C. and Ramadhani, D.P. (2025), "Cybersecurity compliance and others that affect on employee protective behavior: case study bank X in Indonesia", *International Journal of Safety and Security Engineering*, Vol. 15 No. 6, pp. 1229-1241, doi: 10.18280/ijsse.150613.

Alahmari, S., Renaud, K. and Omoronyia, I. (2022), "Moving beyond cyber security awareness and training to engendering security knowledge sharing", *Information Systems and E-Business Management*, Vol. 21 No. 1, pp. 123-158, doi: 10.1007/s10257-022-00575-2.

Alani, M.M. and Tawfik, H. (2022), "PhishNot: a cloud-based machine-learning approach to phishing URL detection", *Computer Networks*, Vol. 218, 109407, doi: 10.1016/j.comnet.2022.109407.

Alsharida, R.A., Al-rimy, B.A.S., Al-Emran, M. and Zainal, A. (2023), "A systematic review of multi perspectives on human cybersecurity behavior", *Technology in Society*, Vol. 73, 102258, doi: 10.1016/j.techsoc.2023.102258.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L. and Xu, L. (2017), "Gender difference and employees' cybersecurity behaviors", *Computers in Human Behavior*, Vol. 69, pp. 437-443, doi: 10.1016/j.chb.2016.12.040.

Arachchilage, N.A.G. and Hameed, M.A. (2017), "Integrating self-efficacy into a gamified approach to thwart phishing attacks", arXiv preprint arXiv:1706.07748.

Arachchilage, N.A.G. and Love, S. (2014), "Security awareness of computer users: a phishing threat avoidance perspective", *Computers in Human Behavior*, Vol. 38, pp. 304-312, doi: 10.1016/j.chb.2014.05.046.

Bandura, A. (1982), "Self-efficacy mechanism in human agency", *American Psychologist*, Vol. 37 No. 2, pp. 122-147, doi: 10.1037/0003-066x.37.2.122.

Baral, G. and Arachchilage, N.A.G. (2019), "Building confidence not to be phished through a gamified approach: conceptualising users' self-efficacy in phishing threat avoidance behaviour", *2019 Cybersecurity and Cyberforensics Conference (CCC)*.

Basit, A., Zafar, M., Liu, X., Javed, A.R., Jalil, Z. and Kifayat, K. (2021), "A comprehensive survey of AI-enabled phishing attacks detection techniques", *Telecommunication Systems*, Vol. 76 No. 1, pp. 139-154, doi: 10.1007/s11235-020-00733-2.

Bayl-Smith, P., Taib, R., Yu, K. and Wiggins, M. (2022), "Response to a phishing attack: persuasion and protection motivation in an organizational context", *Information and Computer Security*, Vol. 30 No. 1, pp. 63-78, doi: 10.1108/ics-02-2021-0021.

Beu, N., Jayatilaka, A., Zahedi, M., Babar, A., Hartley, L., Lewinsmith, W. and Baetu, I. (2023), "Falling for phishing attempts: an investigation of individual differences that are associated with behavior in a naturalistic phishing simulation", *Computers and Security*, Vol. 131, 103313, doi: 10.1016/j.cose.2023.103313.

Boss, S.R., Galletta, D.F., Lowry, P.B., Moody, G.D. and 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*, Vol. 39 No. 4, pp. 837-864, doi: 10.25300/misq/2015/39.4.5.

Bougie, R. and Sekaran, U. (2019), *Research Methods for Business: A Skill Building Approach*, John Wiley & Sons, Hoboken, New Jersey.

Buckley, J., Lottridge, D., Murphy, J. and Corballis, P. (2023), "Indicators of employee phishing email behaviours: intuition, elaboration, attention, and email typology", *International Journal of Human-Computer Studies*, Vol. 172, 102996, doi: 10.1016/j.ijhcs.2023.102996.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", *MIS Quarterly*, Vol. 34 No. 3, pp. 523-548, doi: 10.2307/25750690.

Canfield, C.I., Fischhoff, B. and Davis, A. (2016), "Quantifying phishing susceptibility for detection and behavior decisions", *Human Factors*, Vol. 58 No. 8, pp. 1158-1172, doi: 10.1177/0018720816665025.

Çetin, F. and Aşkun, D. (2019), "The effect of occupational self-efficacy on work performance through intrinsic work motivation", *Management Research Review*, Vol. 41 No. 2, pp. 186-201, doi: 10.1108/MRR-03-2017-0062.

Chiew, K.L., Yong, K.S.C. and Tan, C.L. (2018), "A survey of phishing attacks: their types, vectors, and technical approaches", *Expert Systems with Applications*, Vol. 106, pp. 1-20, doi: 10.1016/j.eswa.2018.03.050.

Chin, W.W. (1998), "The partial least squares approach to structural equation modeling", in *Modern Methods for Business Research*, Vol. 295 No. 2, pp. 295-336.

Claar, C.L. and Johnson, J. (2012), "Analyzing home PC security adoption behavior", *Journal of Computer Information Systems*, Vol. 52 No. 4, pp. 20-29.

Cohen, J. (2013), *Statistical Power Analysis for the Behavioral Sciences*, Lawrence Erlbaum Associates, Hillsdale, NJ.

Daud, A., Marliani, L., Kurniawanto, H. and Purnama, C. (2025), "Analysis of factors that impact self-efficacy in terms of locus control, learning orientation, and work environment characteristics", *Journal of Ecohumanism*, Vol. 4 No. 1, pp. 1380-1393.

De Bona, M. and Paci, F. (2020), "A real-world study on employees' susceptibility to phishing attacks", *Proceedings of the 15th International Conference on Availability, Reliability and Security*, pp. 1-10.

de Bruijn, H. and Janssen, M. (2017), "Building cybersecurity awareness: the need for evidence-based framing strategies", *Government Information Quarterly*, Vol. 34 No. 1, pp. 1-7, doi: 10.1016/j.giq.2017.02.007.

De Kimpe, L., Walrave, M., Verdegem, P. and Ponnet, K. (2022), "What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context", *Behaviour and Information Technology*, Vol. 41 No. 8, pp. 1796-1808, doi: 10.1080/0144929x.2021.1905066.

Desolda, G., Aneke, J., Ardito, C., Lanzilotti, R. and Costabile, M.F. (2023), "Explanations in warning dialogs to help users defend against phishing attacks", *International Journal of Human-Computer Studies*, Vol. 176, 103056, doi: 10.1016/j.ijhcs.2023.103056.

Djatsa, F. (2019), "How perceived benefits and barriers affect millennial professionals' online security behaviors", *Journal of Information Security*, Vol. 10 No. 4, pp. 278-301, doi: 10.4236/jis.2019.104016.

Downs, J.S., Holbrook, M.B. and Cranor, L.F. (2006), "Decision strategies and susceptibility to phishing", *Proceedings of the Second Symposium on Usable Privacy and Security (SOUPS 2006)*, Association for Computing Machinery, New York, NY, pp. 79-90, doi: 10.1145/1143120.1143127.

Ertan, A., Crossland, G., Heath, C., Denny, D. and Jensen, R. (2020), "Cybersecurity behaviour in organisations", arXiv preprint arXiv:2004.11768.

Faul, F., Erdfelder, E., Lang, A.-G. and Buchner, A. (2007), "G* Power 3: a flexible statistical power analysis program for the social, behavioral, and biomedical sciences", *Behavior Research Methods*, Vol. 39 No. 2, pp. 175-191, doi: 10.3758/bf03193146.

Fornell, C. and Larcker, D.F. (1981), "Evaluating structural equation models with unobservable variables and measurement error", *Journal of Marketing Research*, Vol. 18 No. 1, pp. 39-50, doi: 10.1177/002224378101800104.

Frank, M., Jaeger, L. and Ranft, L.M. (2022), "Contextual drivers of employees' phishing susceptibility: insights from a field study", *Decision Support Systems*, Vol. 160, 113818, doi: 10.1016/j.dss.2022.113818.

Goel, D. and Jain, A.K. (2018), "Mobile phishing attacks and defence mechanisms: state of the art and open research challenges", *Computers and Security*, Vol. 73, pp. 519-544, doi: 10.1016/j.cose.2017.12.006.

Gupta, B.B., Arachchilage, N.A. and Psannis, K.E. (2018), "Defending against phishing attacks: taxonomy of methods, current issues and future directions", *Telecommunication Systems*, Vol. 67 No. 2, pp. 247-267, doi: 10.1007/s11235-017-0334-z.

Hair, J., Joe, F., Sarstedt, M., Matthews, L.M. and Ringle, C.M. (2016), "Identifying and treating unobserved heterogeneity with FIMIX-PLS: part I–method", *European Business Review*, Vol. 28 No. 1, pp. 63-76, doi: 10.1108/ebr-09-2015-0094.

Hair, J.F., Risher, J.J., Sarstedt, M. and Ringle, C.M. (2019), "When to use and how to report the results of PLS-SEM", *European Business Review*, Vol. 31 No. 1, pp. 2-24, doi: 10.1108/ebr-11-2018-0203.

Hair, J.F., Hult, G.T.M., Ringle, C.M. and Sarstedt, M. (2021), *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, Sage Publications, Los Angeles.

Harrison, B., Vishwanath, A., Ng, Y.J. and Rao, R. (2015), "Examining the impact of presence on individual phishing victimization", *2015 48th Hawaii International Conference on System Sciences*, IEEE, pp. 3483-3489.

Henseler, J., Ringle, C.M. and Sarstedt, M. (2015), "A new criterion for assessing discriminant validity in variance-based structural equation modeling", *Journal of the Academy of Marketing Science*, Vol. 43 No. 1, pp. 115-135, doi: 10.1007/s11747-014-0403-8.

Herath, T. and Rao, H.R. (2009), "Protection, motivation and deterrence: a framework for security policy compliance in organisations", *European Journal of Information Systems*, Vol. 18 No. 2, pp. 106-125, doi: 10.1057/ejis.2009.6.

Hong, J. (2012), "The state of phishing attacks", *Communications of the ACM*, Vol. 55 No. 1, pp. 74-81, doi: 10.1145/2063176.2063197.

Hsu, M.H., Ju, T.L., Yen, C.H. and Chang, C.M. (2007), "Knowledge sharing behavior in virtual communities: the relationship between trust, self-efficacy, and outcome expectations", *International Journal of Human-Computer Studies*, Vol. 65 No. 2, pp. 153-169, doi: 10.1016/j.ijhcs.2006.09.003.

Hu, W. (2010), "Self-efficacy and individual knowledge sharing", *3rd International Conference on Information Management, Innovation Management and Industrial Engineering*, Vol. 2, IEEE, pp. 401-404, doi: 10.1109/iciii.2010.261.

Hughes, A. (2016), *Student Information Security Behaviors and Attitudes at a Private Liberal Arts University in the Southeastern United States*, Doctoral Dissertation, Northcentral University, Arizona.

Ifinedo, P. (2012), "Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory", *Computers and Security*, Vol. 31 No. 1, pp. 83-95, doi: 10.1016/j.cose.2011.10.007.

Kanth, S.K., Mohapatra, S., Mohanty, D. and Basak, P. (2013), "Parameterizing decision factors on centralization of software testing organization: a practitioner's perspective", *Management Review: An International Journal*, Vol. 8 No. 2, p. 4.

Kemp, S. (2023), "Exploring public cybercrime prevention campaigns and victimization of businesses: a Bayesian model averaging approach", *Computers and Security*, Vol. 127, 103089, doi: 10.1016/j.cose.2022.103089.

Kirda, E. and Kruegel, C. (2006), "Protecting users against phishing attacks", *The Computer Journal*, Vol. 49 No. 5, pp. 554-561, doi: 10.1093/comjnl/bxh169.

Krawczyk-Sokołowska, I. and Caputa, W. (2023), "Awareness of network security and customer value–the company and customer perspective", *Technological Forecasting and Social Change*, Vol. 190, 122430, doi: 10.1016/j.techfore.2023.122430.

Lee, D., Larose, R. and Rifon, N. (2008), "Keeping our network safe: a model of online protection behaviour", *Behaviour and Information Technology*, Vol. 27 No. 5, pp. 445-454, doi: 10.1080/01449290600879344.

Lee, D., Lallie, H.J. and Michaelides, N. (2023a), "The impact of an employee's psychological contract breach on compliance with information security policies: intrinsic and extrinsic motivation", arXiv:2307.02916 [cs.CY].

Lee, Y.Y., Gan, C.L. and Liew, T.W. (2023b), "Thwarting instant messaging phishing attacks: the role of self-efficacy and the mediating effect of attitude towards online sharing of personal information", *International Journal of Environmental Research and Public Health*, Vol. 20 No. 4, p. 3514, doi: 10.3390/ijerph20043514.

Li, L., He, W., Xu, L., Ash, I., Anwar, M. and Yuan, X. (2019), "Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior", *International Journal of Information Management*, Vol. 45, pp. 13-24, doi: 10.1016/j.ijinfomgt.2018.10.017.

Liang, H. and Xue, Y. (2009), "Avoidance of information technology threats: a theoretical perspective", *MIS Quarterly*, Vol. 33 No. 1, pp. 71-90, doi: 10.2307/20650279.

Martens, M., De Wolf, R. and 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*, Vol. 92, pp. 139-150, doi: 10.1016/j.chb.2018.11.002.

McCormick, R. (1997), "Conceptual and procedural knowledge", *International Journal of Technology and Design Education*, Vol. 7, pp. 141-159.

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

Mohammad, T., Hussin, N.A.M. and Husin, M.H. (2022), "Online safety awareness and human factors: an application of the theory of human ecology", *Technology in Society*, Vol. 68, 101823, doi: 10.1016/j.techsoc.2021.101823.

Moody, G.D., Galletta, D.F. and Dunn, B.K. (2017), "Which phish get caught? An exploratory study of individuals' susceptibility to phishing", *European Journal of Information Systems*, Vol. 26 No. 6, pp. 564-584, doi: 10.1057/s41303-017-0058-x.

Mun, Y.Y., Yoon, J.J., Davis, J.M. and Lee, T. (2013), "Untangling the antecedents of initial trust in web-based health information: the roles of argument quality, source expertise, and user perceptions of information quality and risk", *Decision Support Systems*, Vol. 55 No. 1, pp. 284-295.

Na-Nan, K. and Sanamthong, E. (2020), "Self-efficacy and employee job performance", *International Journal of Quality and Reliability Management*, Vol. 37 No. 1, pp. 1-17, doi: 10.1108/IJQRM-01-2019-0013.

Nachin, N., Tangmanee, C. and Piromsopa, K. (2019), "How to increase cybersecurity awareness", *ISACA Journal*, Vol. 2, pp. 45-50.

Naqvi, B., Perova, K., Farooq, A., Makhdoom, I., Oyedeji, I. and Porras, J. (2023), "Mitigation strategies against the phishing attacks: a systematic literature review", *Computers and Security*, Vol. 132, 103387, doi: 10.1016/j.cose.2023.103387.

Ng, B.-Y., Kankanhalli, A. and Xu, Y.C. (2009), "Studying users' computer security behavior: a health belief perspective", *Decision Support Systems*, Vol. 46 No. 4, pp. 815-825, doi: 10.1016/j.dss.2008.11.010.

Orgill, G.L., Romney, G.W., Bailey, M.G. and Orgill, P.M. (2004), "The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems", *Proceedings of the 5th Conference on Information Technology Education*, pp. 177-181.

Pang, S.M., Tan, B.C. and Lau, T.C. (2021), "Antecedents of consumers' purchase intention towards organic food: integration of theory of planned behavior and protection motivation theory", *Sustainability*, Vol. 13 No. 9, p. 5218, doi: 10.3390/su13095218.

Parekh, S., Parikh, D., Kotak, S. and Sankhe, S. (2018), "A new method for detection of phishing websites: URL detection", *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*, pp. 949-952.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2015), "The human aspects of information security questionnaire (HAIS-Q): two further validation studies", *Computers and Security*, Vol. 66, pp. 40-51, doi: 10.1016/j.cose.2017.01.004.

Piquero, N.L., Tibbetts, S.G. and Blankenship, M.B. (2005), "Examining the role of differential association and techniques of neutralization in explaining corporate crime", *Deviant Behavior*, Vol. 26 No. 2, pp. 159-188, doi: 10.1080/01639620590881930.

Plant, M. (1994), "How is science useful to technology", in *Design and Technology in the Secondary Curriculum: A Book of Readings*, The Open University, Milton Keynes, pp. 96-108.

Pratama, O., Aladin, R.A., Lim, B. and Sundjaja, A.M. (2025), "Determinants of security behavior intention in state-owned enterprises: applying protection motivation theory to phishing emails", *International Journal of Safety and Security Engineering*, Vol. 15 No. 3, pp. 443-453, doi: 10.18280/ijsse.150304.

Pyszczynski, T., Greenberg, J. and Solomon, S. (1997), "Why do we need what we need? A terror management perspective on the roots of human social motivation", *Psychological Inquiry*, Vol. 8 No. 1, pp. 1-20, doi: 10.1207/s15327965pli0801_1.

Rainear, A.M. and Christensen, J.L. (2017), "Protection motivation theory as an explanatory framework for proenvironmental behavioral intentions", *Communication Research Reports*, Vol. 34 No. 3, pp. 239-248, doi: 10.1080/08824096.2017.1286472.

Razmerita, L., Kirchner, K. and Nielsen, P. (2016), "What factors influence knowledge sharing in organizations? A social dilemma perspective of social media communication", *Journal of Knowledge Management*, Vol. 20 No. 6, pp. 1225-1246, doi: 10.1108/jkm-03-2016-0112.

Rhee, H.S., Kim, C. and Ryu, Y.U. (2009), "Self-efficacy in information security: its influence on end users' information security practice behavior", *Computers and Security*, Vol. 28 No. 8, pp. 816-826, doi: 10.1016/j.cose.2009.05.008.

Ridinger, G., John, R.S., McBride, M. and Scurich, N. (2016), "Attacker deterrence and perceived risk in a Stackelberg security game", *Risk Analysis*, Vol. 36 No. 8, pp. 1666-1681, doi: 10.1111/risa.12547.

Rogers, R.W. (1975), "A protection motivation theory of fear appeals and attitude change1", *The Journal of Psychology*, Vol. 91 No. 1, pp. 93-114, doi: 10.1080/00223980.1975.9915803.

Rogers, R.W. (1983), "Cognitive and psychological processes in fear appeals and attitude change: a revised theory of protection motivation", in *Social Psychophysiology: A Sourcebook*, pp. 153-176.

Safa, N.S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N.A. and Herawan, T. (2015), "Information security conscious care behaviour formation in organizations", *Computers and Security*, Vol. 53, pp. 65-78, doi: 10.1016/j.cose.2015.05.012.

Safa, N.S., Maple, C., Furnell, S., Azad, M.A., Perera, C., Dabbagh, M. and Sookhak, M. (2019), "Deterrence and prevention-based model to mitigate information security insider threats in organisations", arXiv:1903.12079v1 [cs.CY].

Scarpa, R. and Thiene, M. (2011), "Organic food choices and protection motivation theory: addressing the psychological sources of heterogeneity", *Food Quality and Preference*, Vol. 22 No. 6, pp. 532-541, doi: 10.1016/j.foodqual.2011.03.001.

Shahbaznezhad, H., Kolini, F. and Rashidirad, M. (2021), "Employees' behavior in phishing attacks: what individual, organizational, and technological factors matter?", *Journal of Computer Information Systems*, Vol. 61 No. 6, pp. 539-550, doi: 10.1080/08874417.2020.1812134.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F. and Downs, J. (2010), "Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions", *Proceedings*

of the SIGCHI Conference on Human Factors in Computing Systems (CHI 2010), ACM, pp. 373-382, doi: 10.1145/1753326.1753383.

Singh, S., Subramani, A.K., David, R. and Jan, N.A. (2024), "Workplace ostracism influencing turnover intentions: moderating roles of perceptions of organizational virtuousness and authentic leadership", *Acta Psychologica*, Vol. 243, 104136, doi: 10.1016/j.actpsy.2024.104136.

Siponen, M., Mahmood, M.A. and Pahnila, S. (2014), "Employees' adherence to information security policies: an exploratory field study", *Information and Management*, Vol. 51 No. 2, pp. 217-224, doi: 10.1016/j.im.2013.08.006.

Steves, M., Greene, K. and Theofanos, M. (2020), "Categorizing human phishing difficulty: a phish scale", *Journal of Cybersecurity*, Vol. 6 No. 1, tyaa009, doi: 10.1093/cybsec/tyaa009.

Sulaiman, N.S., Fauzi, M.A., Hussain, S. and Wider, W. (2022), "Cybersecurity behavior among government employees: the role of protection motivation theory and responsibility in mitigating cyberattacks", *Information*, Vol. 13 No. 9, p. 413, doi: 10.3390/info13090413.

Sumner, A., Yuan, X., Anwar, M. and McBride, M. (2022), "Examining factors impacting the effectiveness of anti-phishing training", *Journal of Computer Information Systems*, Vol. 62 No. 5, pp. 975-997, doi: 10.1080/08874417.2021.1955638.

Sun, J.C.-Y., Yu, S.-J., Lin, S.S.J. and Tseng, S.-S. (2016), "The mediating effect of anti-phishing self-efficacy between college students' internet self-efficacy, anti-phishing behavior, and gender difference", *Computers in Human Behavior*, Vol. 59, pp. 249-257, doi: 10.1016/j.chb.2016.02.004.

Tian, C.A., Jensen, M.L. and Durcikova, A. (2023), "Phishing susceptibility across industries: the differential impact of influence techniques", *Computers and Security*, Vol. 135, 103487, doi: 10.1016/j.cose.2023.103487.

Torten, R., Reaiche, C. and Boyle, S. (2018), "The impact of security awareness on information technology professionals' behavior", *Computers and Security*, Vol. 79, pp. 68-79, doi: 10.1016/j.cose.2018.08.007.

Vance, A., Siponen, M. and Pahnila, S. (2012), "Motivating IS security compliance: insights from habit and protection motivation theory", *Information and Management*, Vol. 49 Nos 3-4, pp. 190-198, doi: 10.1016/j.im.2012.04.002.

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*, Vol. 101, pp. 286-296, doi: 10.1016/j.chb.2019.07.034.

Verkoeyen, S. and Nepal, S.K. (2019), "Understanding scuba divers' response to coral bleaching: an application of protection motivation theory", *Journal of Environmental Management*, Vol. 231, pp. 869-877, doi: 10.1016/j.jenvman.2018.10.030.

Vishwanath, A., Herath, T., Chen, R., Wang, J. and Rao, H.R. (2011), "Why do people get phished? Testing individual differences in phishing vulnerability within an integrated information processing model", *Decision Support Systems*, Vol. 51 No. 3, pp. 576-586, doi: 10.1016/j.dss.2011.03.002.

Vrhovec, S. and Mihelič, A. (2021), "Redefining threat appraisals of organizational insiders and exploring the moderating role of fear in cyberattack protection motivation", *Computers and Security*, Vol. 106, 102309, doi: 10.1016/j.cose.2021.102309.

Wash, R. (2020), "How experts detect phishing scam emails", *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI 2020)*, Association for Computing Machinery, pp. 1-12.

Wipawayangkool, K. and Teng, J.T. (2019), "Profiling knowledge workers' knowledge sharing behavior via knowledge internalization", *Knowledge Management Research and Practice*, Vol. 17 No. 1, pp. 70-82, doi: 10.1080/14778238.2018.1557798.

Wright, R.T., Jensen, M.L., Thatcher, J.B., Dinger, M. and Marett, K. (2014), "Research note–influence techniques in phishing attacks: an examination of vulnerability and resistance", *Information Systems Research*, Vol. 25 No. 2, pp. 385-400, doi: 10.1287/isre.2014.0522.

Yeng, P.K., Fauzi, M.A., Yang, B. and Nimbe, P. (2022), "Investigation into phishing risk behaviour among healthcare staff", *Information*, Vol. 13 No. 8, p. 392, doi: 10.3390/info13080392, available at: https://www.mdpi.com/2078-2489/13/8/392

Yoon, C., Hwang, J.-W. and Kim, R. (2012), "Exploring factors that influence students' behaviors in information security", *Journal of Information Systems Education*, Vol. 23 No. 4, pp. 407-416.

Zahedi, F.M., Abbasi, A. and Chen, Y. (2015), "Fake-website detection tools: identifying elements that promote individuals' use and enhance their performance", *Journal of the Association for Information Systems*, Vol. 16 No. 6, pp. 2-484, doi: 10.17705/1jais.00399.

Zainal, N.C., Puad, M.H.M. and Sani, N.F.M. (2022), "Moderating effect of self-efficacy in the relationship between knowledge, attitude, and environment behavior of cybersecurity awareness", *Asian Social Science*, Vol. 18 No. 1, pp. 1-55, doi: 10.5539/ass.v18n1p55.

Zaki, W., Ali, A., Bakar, A. and Sarwar, B. (2019), "Role of self-efficacy in the relationship of training and employee performance", *Paradigms*, Vol. 13 No. 1, pp. 67-73.

Zhan, X., Nah, F.F.-h., Siau, K., Hall, R. and Cheng, M. (2019), "Impact of framing and base size of computer security risk information", *Americas Conference on Information Systems (AMCIS)*, Cancun, Mexico, August 2019.

Zhang, X., Liu, S., Wang, L., Zhang, Y. and Wang, J. (2020), "Mobile health service adoption in China", *Online Information Review*, Vol. 44 No. 1, pp. 1-23, doi: 10.1108/OIR-11-2016-0339.

Zimbardo, P.G. (2007), *The Lucifer Effect: Understanding How Good People Turn Evil*, Blackwell Publishing, New York, NY.

Further reading

Alavi, M. and Leidner, D.E. (2001), "Knowledge management and knowledge management systems: conceptual foundations and research issues", *MIS Quarterly*, Vol. 25 No. 1, pp. 107-136, doi: 10.2307/3250961.

Hosseini-Ghavam-Abad, L., Asghari, F., Bandehagh, A., Najafipour, S. and Bigdeli, S. (2019), "Patient privacy: awareness and attitudes of Iran university of medical sciences medical students", *Medical Journal of the Islamic Republic of Iran*, Vol. 33, p. 12, doi: 10.34171/mjiri.33.12.

Ringle, C.M., Sarstedt, M., Mitchell, R. and Gudergan, S.P. (2020), "Partial least squares structural equation modeling in HRM research", *The International Journal of Human Resource Management*, Vol. 31 No. 12, pp. 1617-1643, doi: 10.1080/09585192.2017.1416655.

Corresponding author
Bilal Naqvi can be contacted at: syed.naqvi@lut.fi