Antecedents of Customer Awareness in Banking Security: A Protection Motivation Theory-Based Systematic Review

Naseer, H.[1], Wijayanayake, J.[2], Jayasinghe, S.A.[3]
[1,2]Department of Industrial Management, Faculty of Science, University of Kelaniya, Sri Lanka.
[3]Department of Business and Law, Southampton Solent University, United Kingdom.
[1]hajaranaseer90@gmail.com, [2]janaka@kln.ac.lk, [3]shan.jayasinghe@solent.ac.uk

Abstract

This study examines the factors influencing customer awareness in personal banking security, with particular emphasis on the Sri Lankan context, where rising cyber-fraud incidents highlight the need for stronger customer awareness. While prior research has focused on technology adoption and security behavior, evidence on the antecedents of customer awareness remains fragmented. A PRISMA-guided systematic literature review of thirty-eight empirical studies indexed in Scopus was conducted using Protection Motivation Theory (PMT) as the primary analytical framework. The review synthesizes findings related to threat appraisal, coping appraisal, and additional factors influencing awareness in digital banking security. The results show that self-efficacy and response efficacy are the most consistent drivers of awareness, while perceived severity and vulnerability show mixed effects. Social influence, fear, and trust further shape awareness beyond PMT's core constructs. The findings are contextualized to Sri Lanka, offering insights to strengthen local banking security awareness strategies.

Keywords: *Banking security, Customer awareness, Cybersecurity behavior, Digital banking, Protection Motivation theory*

Received: 11th December 2025 / **Accepted:** 28th December 2025

Correspondence: shan.jayasinghe@solent.ac.uk

ORCID of authors: Naseer, H.- https://orcid.org/0009-0000-4981-8354
Wijayanayaka, J.- https://orcid.org/0000-0002-9523-5384
Jayasinghe, S.A.-https://orcid.org/0000-0001-8149-2999

DOI: https://doi.org/10.4038/kjm.v14i3.7922

Introduction

Digital banking has become a common part of everyday life, allowing people to make payments, check balances, and manage their finances quickly and easily. As these services continue to grow, customers are also exposed to various cyber risks such as phishing, fake messages, identity theft, and online fraud (Vafaei-Zadeh et al., 2025; Johri & Kumar, 2023). These incidents are now common in many countries, and Sri Lanka is also facing this problem. News reports and customer complaints indicate that individuals are frequently targeted through social engineering scams and fraudulent banking links.

In the Sri Lankan context, prior studies show that customer-related factors play a significant role in digital banking usage and security. For example, Aboobucker and Bao (2018) found that trust, perceived risk, and website-related factors strongly influence Sri Lankan customers' engagement with internet banking. Similarly, studies on mobile and online banking adoption in Sri Lanka report that security concerns, perceived risk, and lack of confidence in digital platforms remain key barriers to effective use (Madusanka & Kumari, 2021). Research focusing on customer perceptions further highlights differences in digital literacy and risk awareness, suggesting uneven levels of understanding of online banking threats (Mano et al., 2020). These findings indicate that customers may continue using digital banking services without fully understanding potential security risks.

Even though banks keep improving their security systems, customers remain an important point of vulnerability. Many users do not fully understand online risks, do not know how to identify suspicious activity, or trust messages that appear to come from the bank. This shows that customer awareness which means knowing the threats, safe practices, and warning signs is a key part of protecting personal banking activities (Johri & Kumar, 2023).

Customer awareness levels vary across countries and depend on factors such as education, digital literacy, and technological experience. In Sri Lanka, these differences are particularly visible, making it difficult to directly apply findings from other regions without careful examination. While several empirical studies have examined adoption, trust, and perceived risk in Sri Lankan e-banking, there is no consolidated understanding of the factors that shape customer awareness specifically.

Although Sri Lankan studies have explored digital banking adoption and customer perceptions, they primarily rely on technology acceptance and usage-oriented frameworks. There is limited evidence of Protection Motivation Theory (PMT) being explicitly applied to examine customer awareness in personal banking security within the Sri Lankan context. In contrast, PMT has been widely used in international cybersecurity and online banking research to explain how individuals perceive security threats and evaluate their ability to respond through protective actions. This highlights a gap between global theoretical developments and local empirical evidence related to customer awareness.

To address this gap, the present study conducts a systematic literature review to synthesize existing empirical research on customer awareness in personal banking security. The review is anchored in Protection Motivation Theory, as PMT provides a well-established framework for explaining how individuals perceive

threats and evaluate their ability to cope with them. These processes align closely with the concept of awareness, which depends not only on recognizing risks but also on believing that protective actions are effective and achievable.

Accordingly, the objective of this review is to identify and synthesize the key antecedents that influence customer awareness in personal banking security, with relevance to the Sri Lankan context. By organizing fragmented findings from prior studies, this review aims to provide clearer theoretical insight and support future empirical research and awareness initiatives tailored to Sri Lankan digital banking users.

Literature Review

Research on digital banking security has grown rapidly alongside the widespread adoption of online and mobile banking services. Much of the existing literature focuses on understanding how customers adopt digital banking technologies and how factors such as trust, perceived risk, and system usability influence usage behavior. In the Sri Lankan context, several studies have examined customer adoption of internet and mobile banking, highlighting the role of trust, perceived security, and risk perceptions in shaping customer behavior (Aboobucker & Bao, 2018; Madusanka & Kumari, 2021). While these studies provide valuable insights, they mainly address usage and adoption rather than customer awareness of security threats.

International studies show a similar pattern, with many relying on adoption-oriented frameworks such as the Technology Acceptance Model (TAM) and the Theory of Planned Behavior (TPB). Although these models are effective in explaining technology acceptance, they place limited emphasis on how customers perceive security threats or evaluate their ability to respond to them. As a result, they offer only partial explanations for security-related awareness.

To overcome these limitations, cybersecurity researchers have increasingly adopted Protection Motivation Theory (PMT). Originally developed in the health domain, PMT has been widely adapted to information security contexts. The theory explains behavior through two key processes: threat appraisal, which reflects perceived severity and vulnerability, and coping appraisal, which reflects beliefs about the effectiveness of protective actions and one's ability to perform them (Verkijika, 2018; Jansen & Van Schaik, 2019).

PMT has been widely applied in cybersecurity research to examine secure online behavior, policy compliance, and protective actions in both individual and organizational settings (Alashoor et al., 2017; Jian Mou et al., 2022). More recently, PMT has also been used in online banking studies to examine cybersecurity awareness. For example, Vafaei-Zadeh et al. (2025) demonstrated that customer awareness is closely linked to how individuals evaluate security threats and their confidence in responding to them.

Despite the growing international use of PMT, its application to customer awareness in the Sri Lankan banking context remains limited. Existing local studies focus primarily on adoption, trust, and perceived risk, without explicitly examining awareness through a threat-and-coping perspective. Moreover, findings across PMT-based studies are scattered and often focus on broader outcomes such as protection motivation or security intention rather than awareness itself.

Therefore, a systematic literature review is necessary to consolidate existing empirical evidence and identify the PMT-based factors and any other factors that influence customer awareness in personal banking security. Such a synthesis is particularly important for the Sri Lankan context, where awareness levels, digital literacy, and exposure to cyber threats may differ from other regions.

Methodology

A systematic literature review was conducted following the PRISMA 2020 guidelines to ensure methodological transparency, reproducibility, and minimization of selection bias. PRISMA offers a clear and structured process for identifying, screening, and selecting studies, which helps maintain consistency and clarity throughout the review (Page et al., 2021). This framework was particularly important for this study because multiple stages of screening and theoretical filtering were required (Chathuranga et al., 2023; De Silva et al., 2025; Dias et al., 2025; Dilhara et al., 2024; Fathima et al., 2024; Galappaththi et al., 2024; Hensman et al., 2024; Jayasinghe et al., 2023; Ranasinghe et al., 2024; Wijesinghe et al., 2024) to refine PMT-based studies relevant to customer awareness in personal banking security.

Review Question

The review was driven by a primary research question formulated to align with the overall aim of identifying the key factors that shape customer awareness in personal banking security. After examining existing gaps in PMT-based cybersecurity literature, the following question was developed to guide the search and synthesis process: “What are the potential antecedents that drive customer awareness from the perspective of Protection Motivation Theory (PMT)?”

This question informed the selection of studies and the organization of the thematic findings.

Search Strategy

Scopus was selected as the primary database for this systematic review due to its broad disciplinary coverage and strong indexing of high-impact journals in information systems, cybersecurity, behavioral science, and financial technologies. Prior studies have highlighted Scopus as a reliable source for systematic literature reviews because of its comprehensive metadata, citation tracking, and advanced filtering capabilities (Singh et al., 2021).

This review adopted a theory-driven search strategy, with Protection Motivation Theory (PMT) serving as the central organizing framework. Accordingly, the primary search string applied was: TITLE-ABS-KEY (“protection motivation theory”)

This strategy ensured that all selected studies were grounded in Protection Motivation Theory and examined security-related behavior. This made it possible to identify and compare awareness-related factors using a common theoretical basis.

Additional factors influencing customer awareness, such as emotional, social, and contextual variables, were identified during the screening and synthesis stages based on their repeated appearance across PMT-based studies. This approach maintained theoretical consistency while allowing the review to capture a broad range of influences on customer awareness.

In addition to the Scopus search, a supplementary search using Google Scholar was conducted to identify Sri Lanka specific studies related to digital banking, security concerns, and customer awareness. These studies were used solely to contextualize the Sri Lankan background of the review and were not included in the final set of reviewed articles.

Screening Process

The screening process was carried out entirely using the Scopus database. The initial search using the term "Protection Motivation Theory" in the title, abstract, or keywords returned 2,888 records. Applying a filter to include only journal articles reduced the set to 2,318 studies. A further refinement retaining only studies that listed "Protection Motivation Theory" as an exact keyword produced 996 records. To focus on financial and security-related contexts, additional filter "banking" was applied, resulting in 107 studies.

Abstract screening was then performed to assess topical relevance and methodological suitability, narrowing the list to 74 studies. After full-text review, which evaluated alignment with PMT constructs, relevance to customer security behavior, and overall empirical suitability, a final set of 38 studies was selected for synthesis. At this stage, studies focusing on health-sector security, general PMT applications, or technology adoption and blockchain without behavioral relevance were excluded. The complete screening process and exclusion decisions at each stage are illustrated in the PRISMA flow diagram (Figure I).

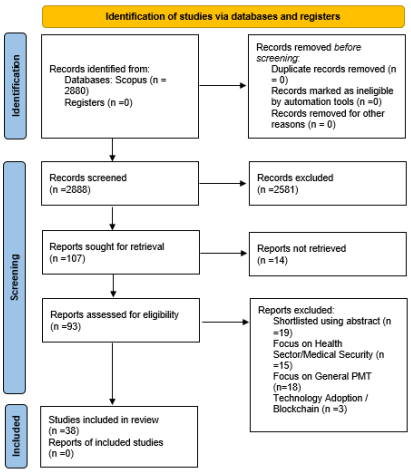

Figure 01: PRISMA flow diagram showing the identification, screening, eligibility assessment, and inclusion of studies in the systematic review.

Inclusion and Exclusion Criteria

The review included studies published between January 2014 and May 2025. Relevant journal articles were identified through the Scopus database, and papers were first screened by reviewing their abstracts. The selection focused on studies that examined Customer Awareness in Banking Security or General Privacy/Security Behavior that could apply to financial services.

Studies were excluded if they focused on health or medical security, presented general PMT research without a security behavior context, or examined technology adoption or blockchain without behavioral relevance. These criteria ensured that the final set of studies was directly related to awareness and security behavior in personal banking.

Quality Assessment

The quality of each study was assessed to ensure that it was suitable for inclusion in the review. The assessment considered

whether the study had clear objectives, used an appropriate sample, measured PMT constructs in a transparent way, and applied suitable analytical methods. Studies also needed to be relevant to cybersecurity, digital banking, or awareness-related behavior. Only studies that met these basic criteria were included in the final analysis.

Data Extraction and Synthesis

Data were extracted using a structured matrix, which is a table used to record key details from each study in a consistent format. The matrix captured the authors, publication year, study context, theoretical model, PMT constructs examined, analytical methods, and key findings. A thematic synthesis approach was used, meaning that findings from all included studies were grouped into common themes based on similar concepts. Constructs were grouped under PMT's threat appraisal and coping appraisal components, along with extended factors such as social influence, fear, trust.

Results

This section presents a structured synthesis of findings from the studies included in the review. The synthesis was guided by Protection Motivation Theory (PMT), which served as the primary analytical framework for organizing and interpreting results. PMT's core components threat appraisal and coping appraisal were used as the main organizing categories, while additional factors repeatedly reported across studies were examined as extended variables.

The results are organized into six subsections: (1) an overview of the included studies, (2) threat appraisal constructs, (3) coping appraisal constructs, (4) extended variables influencing awareness, (5) other theoretical models referenced in the literature, and (6) justification of the final antecedents selected for awareness modelling.

Overview of Included Studies

The reviewed studies covered a range of contexts, including online banking, mobile banking, e-payment services, cybersecurity behavior, and general digital security practices. Most studies employed quantitative approaches such as Partial Least Squares Structural Equation Modeling (PLS-SEM) or covariance-based structural equation modeling (CB-SEM), while some used qualitative or mixed-methods (Hamzah, 2024; Vrhovec and Mihelič, 2021; Alrawhani et al, 2025).

PMT was the dominant theoretical framework across the reviewed literature, although many studies extended the model by integrating additional psychological or contextual variables. Sample populations varied widely and included university students, general technology users, banking customers, and organizational employees. This diversity strengthened the synthesis by allowing patterns in awareness-related behavior to be examined across different user groups and security contexts.

Threat Appraisal Constructs

Threat appraisal reflects how individuals evaluate the seriousness of a security threat and their personal susceptibility to that threat. In the reviewed studies, this appraisal was operationalized through perceived severity and perceived vulnerability (Skalkos et al., 2021).

Several studies reported that higher levels of perceived severity and vulnerability were associated with increased attentiveness to cyber risks and higher awareness levels (Giwah, 2019). Users who believed that cyber incidents could

have serious consequences and that they were personally at risk were more likely to remain cautious and alert.

However, findings related to threat appraisal were not consistent across all contexts. Some studies reported weak or non-significant effects, particularly in environments where cyber incidents were frequent or widely normalized (Vafaei-Zadeh et al., 2025). This suggests that repeated exposure to cyber threats may reduce sensitivity to risk cues. Overall, the synthesis indicates that threat appraisal alone is insufficient to sustain customer awareness, highlighting the need for complementary coping-related factors.

Coping Appraisal Constructs

Coping appraisal captures individuals' evaluations of their ability to respond effectively to security threats. In PMT-based studies, this appraisal includes self-efficacy, response efficacy, and response cost (Mou et al., 2022).

Across the reviewed literature, self-efficacy emerged as the most consistently significant predictor of customer awareness. Users who felt confident in their ability to recognize threats and apply protective measures demonstrated higher vigilance and sustained awareness (Mou et al., 2022; Verkijika, 2018).

Response efficacy also showed strong and consistent positive effects. When users believed that recommended security measures such as strong passwords, two-factor authentication, and regular account monitoring were effective, they were more likely to remain attentive to security risks (Vafaei-Zadeh et al., 2025).

In contrast, findings related to response cost were mixed. Several studies identified perceived inconvenience, time, or effort as barriers that reduced awareness and protective behavior, while others found response cost to be less influential compared to self-efficacy and response efficacy (Verkijika, 2018). Overall, the synthesis indicates that coping appraisal, particularly efficacy-related beliefs, plays a more decisive role in shaping awareness than threat appraisal alone.

Extended Variables

Beyond the core PMT constructs, several studies identified additional factors that influenced customer awareness. These extended variables included social influence, fear, and trust, which captured emotional, social, and contextual dimensions of security behavior.

Social influence including peer behavior, family expectations, and cultural norms was particularly influential in collectivist settings, where awareness is shaped through shared experiences and group behavior (Vafaei-Zadeh et al., 2025; Sulaiman et al., 2022).

Fear functioned as a conditional factor. When accompanied by strong coping beliefs, fear increased attentiveness and learning. However, when coping ability was low, fear led to avoidance or denial rather than increased awareness (Vafaei-Zadeh et al., 2025).

Trust in digital banking systems exhibited a dual effect. While trust increased confidence in institutional security, excessive trust reduced personal vigilance, as users assumed that security was primarily the bank's responsibility (Vafaei-Zadeh et al., 2025). Several studies emphasized that over-reliance on institutional protection can unintentionally lower customer awareness.

Other Theoretical Models in the Reviewed Studies

Although PMT was the primary framework in the reviewed studies, several papers referenced concepts from other behavioral theories, including the Technology Acceptance Model (TAM), Theory of Planned Behavior (TPB), Extended Parallel Process Model (EPPM), and the APCO model (Shahbaznezhad et al., 2021; Alashoor et al., 2017; Lowry et al., 2023).

These theories were not used to directly examine customer awareness but appeared in background discussions or as supplementary perspectives. TAM and TPB contributed adoption-related constructs such as perceived usefulness and subjective norms (Ameen et al., 2020), while EPPM supported findings related to fear and efficacy interactions. The APCO model highlighted trust and privacy concerns.

Their presence indicates that cybersecurity behavior is influenced by multiple psychological dimensions. However, in this review, these theories serve only as contextual references, while the synthesis remains focused on PMT and awareness-related antecedents.

Selection of Final Antecedents

Based on the synthesis, self-efficacy and response efficacy emerged as the strongest and most consistent antecedents of customer awareness. Perceived severity and perceived vulnerability contributed meaningfully but showed contextual variability. Social influence, fear, and trust added important emotional and social dimensions that enhanced explanatory depth.

Although response cost appeared in several PMT-based studies, its influence on customer awareness was inconsistent and comparatively weaker than efficacy-related constructs. Moreover, response cost was more frequently associated with behavioral intention or compliance outcomes rather than awareness itself. Therefore, while response cost is reported in the synthesis for completeness, it was excluded from the final conceptual framework to maintain focus on the most robust and awareness relevant antecedents.

Table I summarizes the final antecedents influencing customer awareness, categorized according to PMT and extended factors, along with the dominant direction of their effects reported across the reviewed studies.

Table 01: Synthesis of Key Antecedents and Their Impact on Awareness

Antecedent	Impact on Awareness	Key Supporting Studies
Perceived Severity	Positive	(Ou et al.,2022) (Skalkos et al. ,2021) (Smit et al, 2021)
Perceived Vulnerability	Positive	(Mou et al.,2022)
Self-Efficacy	Strong Positive	(Lowry et al. ,2023) (Verkijika, 2018) (Tsai et al.,2016)

		(Skalkos et al.,2021) (Smit et al.,2021)
Response Efficacy	Strong Positive	(Lowry et al.,2023) (Verkijika, 2018) (Tsai et al.,2016) (Smit et al.,2021)
Fear	Conditional Positive	(Ou et al.,2022) (Vafaei-Zadeh et al., 2025)
Social Influence	Positive	(Sulaiman et al, 2022)
Trust	Context Dependent	(Vafaei-Zadeh et al. ,2025)

Discussion

The purpose of this systematic literature review was to synthesize existing empirical evidence on the factors that shape customer awareness in personal banking security. By organizing findings using Protection Motivation Theory (PMT) as the primary analytical lens, the review identifies consistent patterns, contextual variations, and gaps in the literature. The results demonstrate that customer awareness is shaped by a combination of cognitive evaluations, emotional responses, and social influences, rather than by threat perception alone.

Interpretation of Key Findings

A clear pattern emerging from the reviewed studies is the dominant role of coping appraisal, particularly self-efficacy and response efficacy, in shaping customer awareness. Across diverse contexts, users who felt confident in their ability to recognize threats and believed that protective actions were effective consistently demonstrated higher levels of awareness and vigilance (Mou et al., 2022; Verkijika, 2018). This suggests that awareness is sustained not merely by knowing that threats exist, but by believing that one can meaningfully respond to them.

In contrast, threat appraisal constructs perceived severity and perceived vulnerability showed mixed effects. While some studies reported positive associations with awareness, others found weak or non-significant relationships, particularly in environments where cyber incidents are frequent or widely normalized (Skalkos et al., 2021; Vafaei-Zadeh et al., 2025). This inconsistency indicates that repeated exposure to cyber risks may lead to desensitization, reducing the motivational impact of threat perception alone. Consequently, threat appraisal appears insufficient to sustain awareness unless supported by strong coping beliefs.

The synthesis also highlights the importance of extended variables. Social influence emerged as a significant factor, especially in collectivist settings where family, peers, and community norms shape individual behavior (Sulaiman et al., 2022). Fear functioned as a conditional driver: when users possessed adequate coping ability, fear increased attentiveness and learning; when coping ability was low, fear led to avoidance or denial (Smit et al., 2021). Trust in banking systems showed a dual effect while institutional

trust encouraged system use, excessive trust reduced personal vigilance by shifting perceived responsibility for security entirely to banks (Vafaei-Zadeh et al., 2025).

A recurring finding across studies is that many customers assume that banks will manage security risks on their behalf. Although this perception strengthens institutional trust, it can unintentionally weaken individual awareness and responsibility. This pattern suggests that awareness should be understood as a shared responsibility between banks and customers, rather than a purely institutional function.

Theoretical Implications

The findings reinforce the suitability of Protection Motivation Theory as a strong theoretical foundation for explaining customer awareness in personal banking security. In particular, the consistent influence of coping appraisal constructs supports PMT's emphasis on efficacy-based evaluations as key drivers of protective cognition and behavior (Mou et al., 2022).

However, the review also demonstrates that PMT alone does not fully capture the complexity of awareness formation. Emotional and social factors such as fear, trust, and social influence played important roles in several studies, indicating that awareness is shaped by broader psychological and contextual dynamics beyond threat and coping evaluations. This suggests that PMT-based models benefit from selective extension rather than strict application. In particular, the review highlights customer awareness as a distinct cognitive outcome that warrants separate theoretical treatment, rather than being implicitly embedded within protection motivation or behavioral intention.

The presence of complementary theories such as TAM, TPB, EPPM, and the APCO model in the reviewed literature further highlights the multidimensional nature of cybersecurity awareness (Ameen et al., 2020; Vrhovec et al., 2023). While these theories were not directly applied in this review, they introduce constructs related to usability, intention, emotional regulation, and privacy concerns that may enrich future awareness models. Overall, the findings suggest that integrating PMT with carefully selected constructs from related frameworks can provide a more comprehensive explanation of customer awareness in digital banking environments.

Practical Implications

The findings of this systematic review offer several practical implications for banking institutions, regulators, and organizations responsible for designing customer awareness initiatives in digital banking environments.

First, the strong and consistent influence of self-efficacy highlights the need for awareness programs to move beyond information provision toward capability-building. Rather than focusing only on warning customers about threats, banks should emphasize how customers can identify risks and what specific actions they can take to protect themselves. Simple, step-by-step guidance on recognizing phishing attempts, verifying official communication, and responding to suspicious activity can strengthen customers' confidence and sustain awareness over time (Mou et al., 2022; Verkijika, 2018).

The importance of response efficacy suggests that customers must clearly understand the effectiveness of recommended security measures. Banks should explain why practices such as two-

factor authentication, strong passwords, and regular account monitoring matter, using clear and non-technical language. When customers believe that these actions genuinely reduce risk, they are more likely to remain attentive and engaged with security-related information (Vafaei-Zadeh et al., 2025). Awareness initiatives should therefore link protective actions directly to tangible security outcomes.

The mixed and context-dependent role of threat appraisal indicates that fear-based messaging alone is insufficient and may even be counterproductive. Repeated exposure to cyber incidents can lead to normalization and reduced sensitivity to threats. As a result, banks and regulators should avoid excessive alarmist messaging and instead balance risk communication with empowerment-oriented messages that reinforce coping ability. This aligns with evidence showing that fear enhances awareness only when users feel capable of responding effectively (Smit et al., 2021).

The role of social influence highlights the value of leveraging social and community-based channels in awareness efforts. In collectivist contexts, such as many developing economies, customers' awareness is shaped by family members, peers, and shared norms (Sulaiman et al., 2022). Banks may therefore benefit from community outreach programs, peer-learning initiatives, and shared digital safety campaigns that encourage discussion and collective responsibility for secure banking behavior.

The dual effect of trust has important implications for how banks communicate security. While institutional trust supports adoption and continued use of digital banking services, excessive reliance on institutional protection can reduce personal vigilance. Banks should clearly communicate that security is a shared responsibility, combining strong institutional safeguards with active customer participation. Messaging that reinforces customer responsibility without undermining trust can help maintain awareness while preserving confidence in the banking system (Vafaei-Zadeh et al., 2025).

Overall, these findings suggest that effective customer awareness initiatives should focus on empowerment rather than fear, capability rather than compliance, and shared responsibility rather than institutional dependence. By aligning awareness strategies with the key drivers identified in PMT-based research, banks and policymakers can design more sustainable and context-sensitive approaches to improving customer awareness in personal banking security.

Conclusion

This systematic literature review examined the factors that shape customer awareness in personal banking security by synthesizing evidence from thirty-eight empirical studies, using Protection Motivation Theory (PMT) as the primary analytical framework. The review demonstrates that customer awareness is a multidimensional construct shaped not only by perceptions of threat, but more strongly by individuals' beliefs about their ability to respond effectively to security risks, as well as by emotional and social influences embedded within digital banking environments.

Across the reviewed literature, coping appraisal constructs particularly self-efficacy and response efficacy emerged as the most consistent and influential antecedents of customer awareness. Customers who believed they could recognize threats and who trusted the effectiveness of protective actions showed

higher and more sustained levels of awareness. In contrast, threat appraisal constructs, namely perceived severity and perceived vulnerability, exhibited mixed and context-dependent effects. In environments where cyber incidents are frequent and increasingly normalized, threat perception alone appeared insufficient to maintain awareness, reinforcing the importance of empowerment-oriented approaches over fear-based risk communication.

The review further highlights the role of extended factors such as social influence, fear, and trust. Social influence was especially salient in collectivist contexts, where awareness is shaped through shared norms and peer behavior. Fear functioned as a conditional factor that enhanced awareness only when supported by strong coping beliefs, while trust in banking systems showed dual effects supporting continued usage but potentially reducing personal vigilance when customers rely excessively on institutional protection. Together, these findings emphasize that customer awareness should be understood as a shared responsibility between banks and customers, rather than as an outcome driven solely by institutional safeguards.

From a theoretical perspective, the findings confirm the suitability of PMT as a robust foundation for examining customer awareness in personal banking security, particularly due to its strong explanatory power in relation to efficacy-based evaluations. At the same time, the review demonstrates that selectively extending PMT with empirically relevant emotional and social constructs enhances its explanatory depth. Importantly, this study positions customer awareness as a distinct cognitive outcome, rather than treating it implicitly as part of protection motivation or behavioral intention, thereby offering clearer conceptual grounding for future research.

Practically, the review underscores the need for awareness initiatives that prioritize capability-building, clear communication of the effectiveness of protective measures, and balanced messaging that avoids excessive reliance on fear. Banks and policymakers should design awareness strategies that strengthen customer confidence, leverage social and community-based influence, and clearly communicate shared responsibility for security. Such approaches are particularly relevant for contexts like Sri Lanka, where levels of digital literacy, exposure to cyber threats, and reliance on institutional protection may differ from those in more mature digital banking markets.

While this review provides a comprehensive synthesis of PMT-based evidence, it also opens avenues for future research. Empirical studies that apply PMT within the Sri Lankan banking context remain limited, highlighting the need for context-specific investigations using robust theoretical models. Future research may also explore integrated frameworks that combine PMT with selected constructs from complementary behavioral theories to further enrich understanding of customer awareness in digital banking security.

Overall, this study offers a structured and evidence-based foundation for advancing both theory and practice in customer awareness research. By clarifying key antecedents and contextual influences, the review supports the development of more effective awareness models, targeted interventions, and future empirical research within the evolving digital banking landscape.

References

Abbasi, A., Chen, Y., & Zahedi, F. (2015). Fake-website detection tools: Identifying elements that promote individuals' Use and enhance their performance. *Journal of the Association for Information Systems*, *16*(6), 448–484. https://doi.org/10.17705/1jais.00399

Aboobucker, I., & Bao, Y. (2018). What obstruct customer acceptance of internet banking? Security and privacy, risk, trust and website usability and the role of moderators. *The Journal of High Technology Management Research*, *29*(1), 109–123. https://doi.org/10.1016/j.hitech.2018.04.010

Alashoor, T., Han, S., & Joseph, R. C. (2017). Familiarity with big data, privacy concerns, and self-disclosure accuracy in social networking websites: An APCO Model. *Communications of the Association for Information Systems*, *41*, 62–96. https://doi.org/10.17705/1CAIS.04104

Alrawhani, E. M., Romli, A., & Al-Sharafi, M. A. (2025). Evaluating the role of protection motivation theory in information security policy compliance: Insights from the banking sector using PLS-SEM approach. *Journal of Open Innovation: Technology, Market, and Complexity*, *11*(1), 100463. https://doi.org/10.1016/j.joitmc.2024.100463

Alrawhani, E. M., Romli, A. B., Al-Sharafi, M. A., & Alkawsi, G. (2025). Integrating information security culture and protection motivation to enhance Compliance with Information Security Policies in Banking: Evidence from PLS-SEM and fsQCA. *International Journal of Human–Computer Interaction*, 1–22. https://doi.org/10.1080/10447318.2025.2464900

Alsharida, R. A., Al-rimy, B. A. S., Al-Emran, M., Al-Sharafi, M. A., & Zainal, A. (2025). An Integrated SEM-ANN approach to evaluating cybersecurity behaviors in the Metaverse. *International Journal of Human–Computer Interaction*, 1–20. https://doi.org/10.1080/10447318.2025.2484650

Ameen, N., Tarhini, A., Hussain Shah, M., & Madichie, N. O. (2020). Employees' behavioural intention to smartphone security: A gender-based, cross-national study. *Computers in Human Behavior*, *104*, 106184. https://doi.org/10.1016/j.chb.2019.106184

Çetintaş, E., & Daştan, İ. (2022). Examination of privacy and security perceptions of social media and online shopping users: A comparison between Turkey and the USA. *International Journal of Information Security and Privacy*, *16*(1), 1–19. https://doi.org/10.4018/IJISP.300321

Chathuranga, S., Jayasinghe, S., Antucheviciene, J., Wickramarachchi, R., Udayanga, N., & Weerakkody, W. A. S. (2023). Practices driving the adoption of agile project management methodologies in the design stage of building construction projects. *Buildings*, *13*(4), 1-19. https://doi.org/10.3390/buildings13041079

Chen, H., & Yuan, Y. (2023). The impact of ignorance and bias on information security protection motivation: A case of e-waste handling. *Internet Research*, *33*(6), 2244–2275. https://doi.org/10.1108/INTR-04-2022-0238

De Silva, N., Wijayanayake, J., & Jayasinghe, S. (2025, 19-20 February). Critical factors influencing the maturity of business analytics of software and apparel industries in Sri Lanka.

5th International Conference on Advanced Research in Computing, Belihuloya, Sri Lanka. https://doi.org/10.1109/ICARC64760.2025.10963021

Dias, I., Wickramarachchi, R., & Jayasinghe, S. (2025, 3 April). Key success factors for adoption of CI/CD with agile project management - Systematic literature review. International Research Conference on Smart Computing and Systems Engineering, Colombo, Sri Lanka.https://doi.org.10.1109/SCSE65633.2025.11031019

Dilhara, T., Jayasinghe, S., & Fernando, I. (2024, 4 April). Factors influencing the adoption of agile project management methodologies by engineering teams in the telecommunications industry. International Research Conference on Smart Computing and Systems Engineering, Kelaniya, Sri Lanka. https://doi.org/10.1109/SCSE61872.2024.10550785

Fathima, F., Jayasinghe, S., Prasadika, J., & Wijerathna, S. (2024, 4 April). Drivers of actual usage of building information modelling tools by civil engineering professionals in construction industry of Sri Lanka. International Research Conference on Smart Computing and Systems Engineering, Kelaniya, Sri Lanka. https://doi.org/10.1109/SCSE61872.2024.10550677

Galappaththi, D., Jayasinghe, S., & Peiris, P. (2024, 4 April). Antecedents of customer purchase intention of furniture from online stores with the assistance of augmented reality applications. International Research Conference on Smart Computing and Systems Engineering, Kelaniya, Sri Lanka. https://doi.org/10.1109/SCSE61872.2024.10550849

Gerdin, M., Grönlund, Å., & Kolkowska, E. (2025). Conceptual inconsistencies in variable definitions and measurement items within ISP non-/compliance research: A systematic literature review. *Computers & Security*, *152*, 104365. https://doi.org/10.1016/j.cose.2025.104365

Giwah, A. D. (2019). *Empirical Assessment of Mobile Device Users' Information Security Behavior towards Data Breach: Leveraging Protection Motivation Theory*. DOI-10.1108/JIC-03-2019-0063

Grimes, M., & Marquardson, J. (2019). Quality matters: Evoking subjective norms and coping appraisals by system design to increase security intentions. *Decision Support Systems*, *119*, 23–34. https://doi.org/10.1016/j.dss.2019.02.010

Hamzah, M. I. (2024). Fear of COVID-19 disease and QR-based mobile payment adoption: A protection motivation perspective. *Journal of Financial Services Marketing*, *29*(3), 946–963. https://doi.org/10.1057/s41264-023-00246-4

Hensman, S., Jayasinghe, S., & Fernando, I. (2024, 4 April). Antecedents of driving customer purchase intention via AI based customer engagement strategies in the post pandemic era. International Research Conference on Smart Computing and Systems Engineering, Kelaniya, Sri Lanka. https://doi.org/10.1109/SCSE61872.2024.10550604

Jansen, J., & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology*, *10*(1), 79-91. https://doi.org/10.5281/ZENODO.58523

Jansen, J., & Van Schaik, P. (2018a). Persuading end users to act cautiously online: A fear appeals study on phishing. *Information & Computer Security*, *26*(3), 264–276. https://doi.org/10.1108/ICS-03-2018-0038

Jansen, J., & Van Schaik, P. (2018b). Testing a model of precautionary online behaviour: The case of online banking. *Computers in Human Behavior*, *87*, 371–383. https://doi.org/10.1016/j.chb.2018.05.010

Jansen, J., & Van Schaik, P. (2019). The design and evaluation of a theory-based intervention to promote security behaviour against phishing. *International Journal of Human-Computer Studies*, *123*, 40–55. https://doi.org/10.1016/j.ijhcs.2018.10.004

Jayasinghe, S., Suraweera, T., & Samarasinghe, D. (2023). Job seeker value proposition conceptualised from the perspective of the job choice theory. *Sri Lanka Journal of Social Sciences*, *45*(2). https://doi.org/10.4038/sljss.v45i2.8341

Jenkins, J. L., Grimes, M., Proudfoot, J. G., & Lowry, P. B. (2014). Improving password cybersecurity through inexpensive and minimally invasive means: Detecting and deterring password reuse through keystroke-dynamics monitoring and just-in-time fear appeals. *Information Technology for Development*, *20*(2), 196–213. https://doi.org/10.1080/02681102.2013.814040

Johri, A., & Kumar, S. (2023). Exploring customer awareness towards their cyber security in the Kingdom of Saudi Arabia: A study in the era of banking digital transformation. *Human Behavior and Emerging Technologies*, 2103442. https://doi.org/10.1155/2023/2103442

Kim, D., & Bae, J. K. (2020). The effects of protection motivation and perceived innovation characteristics on innovation resistance and innovation acceptance in internet primary bank services. *Global Business Finance Review*, *25*(1), 1–12. https://doi.org/10.17549/gbfr.2020.25.1.1

Lowry, P. B., Moody, G. D., Parameswaran, S., & Brown, N. J. (2023). Examining the differential effectiveness of fear appeals in information security management using two-stage meta-analysis. *Journal of Management Information Systems*, *40*(4), 1099–1138. https://doi.org/10.1080/07421222.2023.2267318

Madusanka, K. A. E., & Kumari, D. A. T. (2021). Antecedents of customer adoption on digital banking with special reference to non-banking financial institutes in Sri Lanka. *South Asian Journal of Finance*, *1*(1), 61–79. https://doi.org/10.4038/sajf.v1i1.28

Mano, W., Anuja, L., Prashanthy, K., Subarami, S., Rubika, S., & G. T. H. D, L. (2020). a study on customer perception towards e-banking: With special reference to urban and rural districts in Sri Lanka. *International Journal of Academic Research in Business and Social Sciences*, *10*(10), 682-698. https://doi.org/10.6007/IJARBSS/v10-i10/7766

Mou, J., Cohen, J., Bhattacherjee, A., & Kim, J. (2022). A test of protection motivation theory in the information security literature: A meta-analytic structural equation modeling approach in search advertising. *Journal of the Association for Information Systems*, *23*(1), 196–236. https://doi.org/10.17705/1jais.00723

Nehme, A., Li, M. (Leah), & Warkentin, M. (2024). Adaptive and maladaptive factors behind password manager use: A hope-extended protection motivation perspective. *Computers & Security*, *144*, 103941. https://doi.org/10.1016/j.cose.2024.103941

Ng, K. C., Zhang, X., Thong, J. Y. L., & Tam, K. Y. (2021). Protecting against threats to information security: An attitudinal ambivalence perspective. *Journal of Management Information Systems*, *38*(3), 732–764. https://doi.org/10.1080/07421222.2021.1962601

Ong, A. K. S., Prasetyo, Y. T., Tapiceria, R. P. K. M., Nadlifatin, R., & Gumasing, Ma. J. J. (2024). Factors affecting the intention to use COVID-19 contact tracing application "StaySafe PH": Integrating protection motivation theory, UTAUT2, and system usability theory. *PLOS ONE*, *19*(8), e0306701. https://doi.org/10.1371/journal.pone.0306701

Ou, C. X., Zhang, X., Angelopoulos, S., Davison, R. M., & Janse, N. (2022). Security breaches and organization response strategy: Exploring consumers' threat and coping appraisals. *International Journal of Information Management*, *65*, 102498. https://doi.org/10.1016/j.ijinfomgt.2022.102498

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, n71. https://doi.org/10.1136/bmj.n71

Rahi, S., Alghizzawi, M., & Ngah, A. H. (2024). Understanding consumer behavior toward adoption of e-wallet with the moderating role of pandemic risk: An integrative perspective. *Kybernetes*, *53*(11), 4818–4839. https://doi.org/10.1108/K-10-2022-1431

Rahman, K. R. S., Faruq, O., Rahman, Md. T., Sumon, Md. R., Rahman, Md. A., Parvez, A. S. M., Nath, N. C., & Sohel, T. A. (2024). Adoption of identity theft protection services in social media: A PMT investigation. *Sustainable Engineering and Innovation*, *6*(1), 87–102. https://doi.org/10.37868/sei.v6i1.id248

Ranasinghe, V., Jayasinghe, S., & Peiris, P. (2024, 21-24 February). Determinants of intention to use project management information system by agile project teams in the information technology industry in Sri Lanka: an extension of the classic technology acceptance model. 4th International Conference on Advanced Research in Computing, Belihuloya, Sri Lanka. https://doi.org/10.1109/ICARC61713.2024.10499786

Seini, A. B., Adam, I. O., & Alhassan, M. D. (2025). Examining the effect of security behaviour on the continuance use of mobile money services in Ghana: A protection motivation perspective. *Information Technology for Development*, 1–18. https://doi.org/10.1080/02681102.2025.2483695

Shahbaznezhad, H., Kolini, F., & Rashidirad, M. (2021). Employees' Behavior in Phishing Attacks: What Individual, Organizational, and Technological Factors Matter? *Journal of Computer Information Systems*, *61*(6), 539–550. https://doi.org/10.1080/08874417.2020.1812134

Singh, V. K., Singh, P., Karmakar, M., Leta, J., & Mayr, P. (2021). The journal coverage of Web of Science, Scopus and Dimensions: A comparative analysis. *Scientometrics*, *126*(6), 5113–5142. https://doi.org/10.1007/s11192-021-03948-5

Skalkos, A., Stylios, I., Karyda, M., & Kokolakis, S. (2021). Users' privacy attitudes towards the use of behavioral biometrics continuous authentication (BBCA) technologies: A protection motivation theory approach. *Journal of Cybersecurity and Privacy*, *1*(4), 743–766. https://doi.org/10.3390/jcp1040036

Smit, T., Van Haastrecht, M., & Spruit, M. (2021). The effect of countermeasure readability on security intentions. *Journal of Cybersecurity and Privacy*, *1*(4), 675–703. https://doi.org/10.3390/jcp1040034

Sulaiman, N. S., Fauzi, M. A., Hussain, S., & Wider, W. (2022). cybersecurity behavior among government employees: The role of protection motivation theory and responsibility in mitigating cyberattacks. *Information*, *13*(9), 413. https://doi.org/10.3390/info13090413

Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*, 138–150. https://doi.org/10.1016/j.cose.2016.02.009

Vafaei-Zadeh, A., Nikbin, D., Teoh, K. Y., & Hanifah, H. (2025). Cybersecurity awareness and fear of cyberattacks among online banking users in Malaysia. *International Journal of Bank Marketing*, *43*(3), 476–505. https://doi.org/10.1108/IJBM-03-2024-0138

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

Vrhovec, S., Bernik, I., & Markelj, B. (2023). Explaining information seeking intentions: Insights from a Slovenian social engineering awareness campaign. *Computers & Security*, *125*, 103038. https://doi.org/10.1016/j.cose.2022.103038

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

Wang, Z., & Liu, Y. (2014). Identifying key factors affecting information disclosure intention in online shopping. *International Journal of Smart Home*, *8*(4), 47–58. https://doi.org/10.14257/ijsh.2014.8.4.05

Wijesinghe, E. P. S. D., Jayasinghe, S., Prasadika, A. P. K. J., & Wijerathna, S. K. (2024, 4 April). A systematic review on the determinants of customer relationship quality in agile projects in the IT industry: A social exchange theory perspective. International Research Conference on Smart Computing and Systems Engineering, Kelaniya, Sri Lanka. https://doi.org/10.1109/SCSE61872.2024.10550794