INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN ACCOUNTING, FINANCE AND MANAGEMENT SCIENCES

OPEN ACCESS JOURNAL

Vol 15, Issue 3, (2025) E-ISSN: 2225-8329

Cybersecurity Awareness and Customer Satisfaction in Digital Banking: A Conceptual Framework from the Malaysian Context

Khaled Al-Daraba
Institute of Technology Management and Entrepreneurship, Universiti Teknikal Malaysia Melaka
Email: p082210002@student.utem.edu.my

Sabri Mohamad Sharif
Universiti Teknikal Malaysia Melaka, Fakulti Pengurusan Teknologi dan Teknousahawanan
Corresponding Author Email: sabri@utem.edu.my

DOI Link: http://dx.doi.org/10.6007/IJARAFMS/v15-i3/26309

Published Online: 04 September 2025

Abstract
The rapid evolution of digital technology has transformed global banking by enhancing accessibility and efficiency, yet it has simultaneously heightened exposure to cyber risks, making cybersecurity a critical concern for safeguarding customer trust and institutional resilience. In Malaysia, where the financial ecosystem spans commercial, Islamic, digital, and investment banks, internet banking adoption has grown rapidly, but threats such as phishing, hacking, malware, and ATM skimming have eroded confidence in digital platforms. Although scholars stress that customer awareness is central to building trust and satisfaction, studies reveal inconsistent levels of awareness in Malaysia, with many customers lacking sufficient knowledge of advanced risks and protective practices. This gap underscores the need to analyze not only institutional safeguards but also the customer's role in enhancing cybersecurity. To address this, the study adopts the Information System Success Model (ISSM) to examine how awareness of cyberattacks, phishing, hacking, and data privacy influences customer satisfaction in online banking. The methodology is grounded in a systematic literature review, and the findings emphasize that customer awareness is positively correlated with satisfaction and trust. Importantly, the study contributes a conceptual framework positioning awareness dimension as antecedents of satisfaction, offering a structured foundation for future empirical research and practical strategies in Malaysian digital banking.

Keywords: Cybersecurity, Awareness, Digital, Banking, Customer, Satisfaction

Introduction

The rapid evolution of digital technology has significantly transformed the global financial sector, with banking institutions positioned at the forefront of this transition. Increasing reliance on online platforms and digital tools has reshaped banking practices, enabling customers to enjoy greater convenience, accessibility, and efficiency in managing their financial activities. However, this transformation has also introduced new challenges, particularly in the domain of cybersecurity. Cybersecurity broadly refers to the protection of systems, networks, and data from malicious attacks, unauthorized access, and digital crimes (Von Solms & Van Niekerk, 2013; Singer & Friedman, 2014). Within the banking context, cybersecurity plays a critical role in safeguarding the confidentiality, integrity, and availability of financial data, ensuring both institutional resilience and customer trust. As banks adopt ever more advanced technologies, the urgency of addressing cyber risks intensifies, particularly in countries like Malaysia, where internet banking adoption has grown rapidly.

The origins of cybersecurity can be traced back to the late 1960s with the development of ARPANET, which laid the groundwork for today’s internet (Branch, 2020). Early manifestations of cyber threats, such as the Creeper worm in 1971 and the subsequent creation of the Reaper program to eliminate it, underscored the need for defense mechanisms from the outset (Higgins, 2022). Since then, the sophistication of cyberattacks has escalated dramatically, with hackers devising new methods to exploit vulnerabilities in interconnected systems. Scholars contend that cybersecurity has evolved in tandem with advancements in computing, becoming indispensable in mitigating threats in the digital era (Naager, 2023). The banking sector, being one of the most data-intensive industries, remains a prime target for cybercriminals due to the vast amounts of sensitive personal and financial information it processes daily (Marecki, 2022).

Malaysia offers a particularly relevant context for exploring the nexus between cybersecurity and customer satisfaction. The nation’s financial system, as reported by Bank Negara Malaysia (2020), consists of 55 registered banks, including commercial banks, Islamic banks, digital banks, and investment banks. Commercial banks offer traditional financial services such as loans, deposits, and mortgages. Islamic banks, meanwhile, operate under Shariah principles, offering profit- and risk-sharing arrangements compliant with Islamic law (Salaudeen, 2023; Saravanakumar, 2024). More recently, Malaysia has welcomed digital banks, which operate entirely online to provide efficient, low-cost alternatives to conventional banking (Abbas, 2023). Complementing these institutions, investment banks focus on advisory services, asset management, and complex financial transactions (GDSLINK, 2023). This diversity illustrates Malaysia’s readiness to embrace digital transformation in banking. However, as digital adoption deepens, so too does vulnerability to cyberattacks, elevating cybersecurity to a matter of national concern.

The principal challenge for Malaysian banks lies in balancing the ease of digital convenience with robust security measures. Internet banking has revolutionized customer access, allowing transactions to be performed at any time and place. Yet, the rise of phishing attacks, malware infections, hacking incidents, and ATM skimming has eroded public trust in digital platforms. Phishing, for instance, deceives users into disclosing sensitive information through fraudulent emails or websites, while malware compromises login credentials and monitors activities (Amar Johri, 2023). ATM skimming, which captures card details via hidden devices, remains a pressing concern for customer trust. These vulnerabilities directly affect satisfaction, as customers grow hesitant to use online banking for fear of financial losses or identity theft (Romanosky, 2016). A lack of confidence in digital security can prompt customers to abandon online services in favor of alternative methods or institutions perceived to offer stronger protections.

A growing body of scholarship highlights the pivotal role of customer awareness in shaping trust and satisfaction with banking services. Awareness refers to the extent to which customers understand cyber risks and adopt practices to safeguard themselves (Smith et al., 2020). Customers familiar with phishing techniques are less likely to succumb to scams, while those informed about data privacy issues express greater confidence in their banks' security (Lim et al., 2021). In Malaysia, awareness levels remain inconsistent. Ahmad and Hassan (2019) found that although customers acknowledge the importance of cybersecurity, many lack detailed knowledge of advanced risks and mitigation strategies. This gap widens the disconnect between institutional security policies and customer behavior, leaving exploitable vulnerabilities for cybercriminals. The consequences of inadequate awareness are multifaceted. On a financial level, customers risk losing their savings to fraud. Psychologically, insecurity breeds anxiety and reduces satisfaction, discouraging loyalty. Institutionally, banks face reputational damage, customer attrition, and diminished profitability (Bijnen & Shaiques, 2021). More broadly, weakened trust in digital banking could impede Malaysia's goals for financial inclusion and digital economic growth, as outlined in the Financial Sector Blueprint (Bank Negara Malaysia, 2020). Strengthening awareness is thus more than a defensive tactic it is a strategic necessity for sustaining digital adoption and customer loyalty.

Despite the growing urgency of cybersecurity in the global digital economy, research focusing on customer awareness in Malaysia remains limited. While international studies have examined phishing, hacking, and privacy concerns as determinants of consumer trust and satisfaction (Jackson et al., 2020; Ahmad & Hassan, 2019), local investigations have been relatively scarce. Much of the existing Malaysian research has concentrated on technological safeguards such as encryption and authentication systems or institutional frameworks including regulations and policies. This creates an imbalance, as the human dimension—particularly customer awareness and behavior—has often been overlooked. This research gap is particularly critical as Malaysia accelerates toward digital-first financial models and mobile-driven banking services. With Bank Negara Malaysia promoting the adoption of digital banks and e-wallets, customer trust and awareness have become central to the sustainability of these services. At the same time, cybercriminals increasingly exploit end-users through social engineering and behavioral manipulation, making customers the weakest link in the security chain. Even the most advanced technological solutions cannot fully mitigate risks if users lack awareness or practice unsafe online behaviors. Thus, understanding and strengthening customer awareness in cybersecurity is not only an academic necessity but also a strategic priority for Malaysia's digital economy. Without deeper insights into how Malaysian consumers perceive and respond to cyber risks, policymakers and financial institutions may struggle to implement effective awareness campaigns, leaving a critical vulnerability in the country's transition toward a secure and inclusive digital financial ecosystem. The model emphasizes four key factors awareness of cyberattacks, phishing, hacking, and data privacy and evaluates them using the Information System Success Model (ISSM), originally proposed by DeLone and McLean (2003). The importance of this conceptual model lies in its ability to reframe cybersecurity as both a technical and behavioral issue, showing how awareness can act as a catalyst for enhancing trust and satisfaction. By integrating ISSM with awareness dimensions, the framework not only advances theoretical understanding but also provides a structured foundation for empirical validation in future studies. In doing so, it highlights the interdependence between institutional security measures and informed customer behavior—an essential synergy for safeguarding Malaysia's digital banking ecosystem.

Literature Review

The literature on cybersecurity in banking highlights the growing sophistication of threats in the digital financial environment and emphasizes the decisive role of customer awareness in fostering satisfaction and trust. In the contemporary era, digital adoption is not an option but a necessity, as internet banking, mobile applications, and digital payment systems have become standard in financial services worldwide. While these innovations enhance convenience and efficiency, they also expose institutions and customers to unprecedented vulnerabilities. Scholars argue that cybersecurity in banking must be regarded not only as a technical challenge but also as a behavioral and educational issue, requiring the active involvement of customers alongside institutional defenses (Andress, 2014; Jang-Jaccard & Nepal, 2014). In Malaysia, where the banking landscape spans from established commercial and Islamic banks to newly licensed digital banks, the expansion of digital services has accelerated faster than the growth of public awareness, creating an urgent need to understand how knowledge, trust, and satisfaction interact within this evolving ecosystem (Bank Negara Malaysia, 2020; Fong, 2022).

Cybersecurity in the Banking Sector

Cybersecurity is broadly defined as the practice of securing systems, networks, and data from malicious attempts to disrupt services, steal resources, or compromise privacy (Von Solms & Van Niekerk, 2013). In banking, this responsibility assumes greater significance due to the sensitive financial and personal data handled by institutions on a daily basis. Cyberattacks against banks frequently aim to extract financial gains, disrupt operations, or tarnish institutional credibility (Marecki, 2022). Common risks include malware infections, phishing schemes, ransomware, and denial-of-service attacks, alongside insider threats and advanced persistent threats, where attackers infiltrate systems and remain undetected for extended periods (Rahimi, 2021).

International cases illustrate the gravity of these risks. Distributed denial-of-service (DDoS) attacks have disrupted major banking services in Europe and the United States, while ransomware attacks have paralyzed financial institutions by locking data until payments were made (Bauer, 2015). In Malaysia, Bank Negara Malaysia (2020) identified phishing, card fraud, and ATM skimming as the most pressing security concerns. These breaches not only inflict financial losses but also damage customer confidence in digital services. Customers who perceive their banks as insecure often abandon digital platforms in favor of traditional methods or seek out alternative providers, underscoring that cybersecurity in banking is not merely a technical safeguard but also a critical determinant of institutional trust and customer satisfaction.

Customer Awareness of Cybersecurity

Customer awareness plays a pivotal role in mitigating cyber risks. It refers to the degree to which customers comprehend digital threats and adopt security-conscious behaviors (Smith et al., 2020). Even with advanced institutional protections, users remain vulnerable if they fall prey to phishing schemes, reuse weak passwords, or share sensitive information with fraudulent actors (Amar Johri, 2023). Ahmad and Hassan (2019), studying Malaysian bank customers, revealed that while basic awareness exists, knowledge of advanced threats and protective measures is often lacking. This gap is particularly concerning in light of increasingly sophisticated cyberattacks that exploit human error more than technical flaws.

Awareness is also directly linked to customer satisfaction. Clients who understand cyber risks feel more confident in the protective measures offered by their banks, leading to higher satisfaction and loyalty (Lim et al., 2021). By contrast, individuals with limited awareness are more vulnerable to fraud and more likely to perceive digital banking services as unsafe, undermining satisfaction and trust (Ozatac et al., 2016). Thus, awareness functions as both a preventive defense and a determinant of satisfaction, shaping the perceived quality of digital financial services.

Theoretical Foundation: Information System Success Model (ISSM)

To analyze the relationship between awareness and satisfaction, this study employs the Information System Success Model (ISSM) proposed by DeLone and McLean (2003). The model conceptualizes system success through six interconnected dimensions: system quality, information quality, service quality, use, user satisfaction, and net benefits. It has been widely recognized as a robust framework for evaluating the performance of information systems across diverse sectors (Qureshi, 2022).

In banking cybersecurity, ISSM is highly relevant because it integrates both technical and user perspectives. System quality reflects the reliability and robustness of security mechanisms, while information quality emphasizes the clarity, timeliness, and relevance of security information communicated to customers. Service quality captures the responsiveness and effectiveness of banks in educating and supporting customers in addressing cyber threats. Together, these dimensions shape user satisfaction, which is central to ISSM. Previous studies have applied the model successfully in evaluating healthcare systems (Lalankesh et al., 2020) and financial services (Ramayah et al., 2021), demonstrating its adaptability and confirming its suitability for analyzing cybersecurity in Malaysia's banking industry.

Factors Influencing Customer Satisfaction

Drawing on ISSM and previous literature, four primary factors emerge as determinants of satisfaction with cybersecurity in online banking: awareness of cyberattacks, awareness of phishing, awareness of hacking, and awareness of data privacy. Each factor contributes uniquely to how customers perceive the safety and reliability of digital banking platforms.

Awareness of Cyberattacks

Cyberattacks encompass a wide range of malicious activities targeting digital systems, including malware infections, ransomware, and denial-of-service attempts. Customers knowledgeable about these threats are better able to appreciate the protective measures implemented by their banks, leading to stronger satisfaction (DeLone & McLean, 2003).

Awareness campaigns, such as those emphasizing the dangers of malware, encourage safe practices like installing antivirus software and avoiding unverified websites. Ahmad and Hassan (2019) confirmed that greater awareness of cyberattacks positively correlates with customer trust and satisfaction, as informed customers feel reassured that their financial assets are well protected.
H1: Awareness of cyberattacks has a positive effect on customer satisfaction with cybersecurity in the Malaysian banking industry.

Awareness of Phishing Attacks
Phishing is one of the most common and effective forms of cyber fraud, using deceptive emails, websites, or messages to extract sensitive information. Customers trained to recognize phishing attempts are less likely to fall victim and more likely to maintain confidence in their banks' online services (Smith et al., 2020). Jackson et al. (2020) demonstrated that comprehensive phishing awareness programs significantly boost customer confidence in digital banking. When banks provide resources to help customers identify fraudulent links or SMS messages, they not only reduce fraud but also enhance satisfaction by signaling a commitment to customer safety.
H2: Awareness of phishing attacks has a positive effect on customer satisfaction with cybersecurity in the Malaysian banking industry.

Awareness of Hacking
Hacking refers to unauthorized access to digital systems, often exploiting software vulnerabilities or employing social engineering techniques. Customers aware of hacking risks are more likely to adopt protective behaviors such as creating strong passwords, enabling two-factor authentication, and monitoring their accounts regularly. Ahmad and Hassan (2019) observed that customers with higher awareness of hacking threats expressed greater trust in their banks. Awareness thus empowers customers to act as partners in security, complementing institutional measures. In contrast, limited awareness magnifies vulnerability, leading to dissatisfaction and diminished trust when breaches occur.
H3: Awareness of hacking has a positive effect on customer satisfaction with cybersecurity in the Malaysian banking industry.

Awareness of Data Privacy
Data privacy concerns the handling of personal and financial information by banks, particularly regarding its collection, storage, and use. Customers who understand privacy practices and regulations are more likely to trust their banks with sensitive data. Transparent policies combined with customer awareness enhance satisfaction by assuring clients that their information is secure and not misused (Lim et al., 2021). As Malaysia advances toward digital-first banking, data-driven personalization amplifies the importance of privacy. Studies highlight that customers informed about privacy protections report higher levels of satisfaction and perceive their banks as both competent and ethical (Bijnen & Shaiques, 2021).
H4: Awareness of data privacy has a positive effect on customer satisfaction with cybersecurity in the Malaysian banking industry.

Linking Awareness and ISSM

Building on these insights, ISSM has been widely employed to examine user satisfaction and system usage across multiple sectors, including healthcare and finance. In cybersecurity research, the framework has been extended to encompass dimensions of awareness, positioning them as antecedents of satisfaction rather than mere outcomes of system use. Table 1 summarizes the positive relationships consistently identified between awareness factors and user satisfaction. Previous applications, such as Lalankesh et al. (2020) in health information systems, further reinforce the framework's validity.

Table 1

Types of relations found in ISSM and related studies.

Awareness Type	Related Component	Type of Relationship	Key Findings	Study Reference
Awareness of Cyberattack	User Satisfaction	Positive Correlation	Higher awareness of cyberattacks leads to greater user satisfaction with security measures.	DeLone & McLean (2003)
Awareness of Phishing Attack	User Satisfaction	Positive Correlation	Users aware of phishing attacks feel more secure and satisfied with online banking.	Smith et al. (2020)
Awareness of Hacking	User Satisfaction	Positive Correlation	Awareness of hacking risks correlates with increased user trust and satisfaction.	Ahmad & Hassan (2019)
Awareness of Data Privacy	User Satisfaction	Positive Correlation	Understanding data privacy enhances user confidence and satisfaction with online banking.	Lim et al. (2021)

In line with DeLone and McLean's IS Success Model, the conceptual framework for this study positions awareness of cyberattacks, phishing, hacking, and data privacy as independent variables influencing customer satisfaction with online banking security (Figure 1).

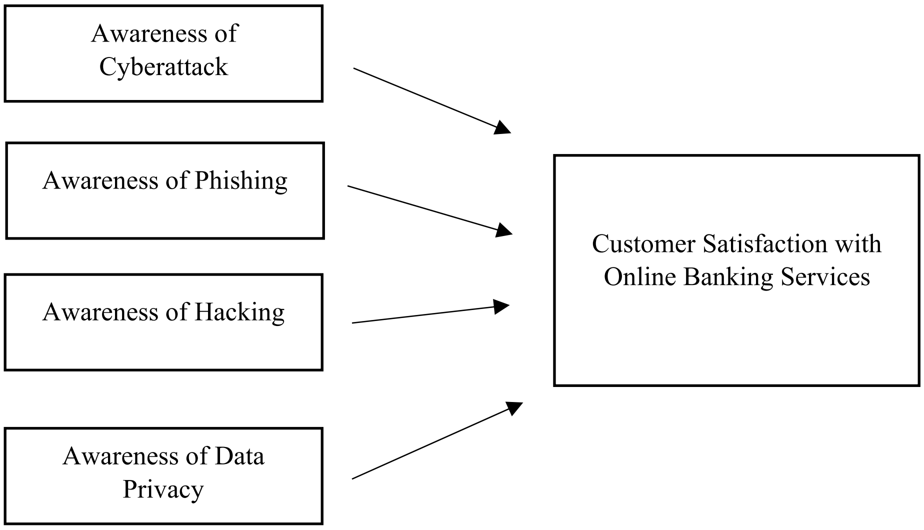
Awareness of Cyberattack
Awareness of Phishing
Awareness of Hacking
Awareness of Data Privacy
Customer Satisfaction with Online Banking Services

Figure 1: Conceptual Framework of Research

Contribution of the Study

This study contributes to both theory and practice in the field of digital banking and cybersecurity. From a theoretical perspective, it extends the Information System Success Model (ISSM) by positioning cybersecurity awareness—covering cyberattacks, phishing, hacking, and data privacy as critical antecedents of customer satisfaction. While ISSM has been widely applied in evaluating system quality and user satisfaction, its integration with awareness dimensions in the Malaysian banking context provides a fresh lens for understanding how behavioral factors interact with technical safeguards. This conceptual framework therefore advances scholarly discourse by bridging gaps between information systems theory, cybersecurity, and customer behavior. From a practical standpoint, the study offers actionable insights for banks, regulators, and policymakers. By emphasizing customer awareness as a strategic pillar, it highlights the need for banks to invest not only in advanced security infrastructure but also in systematic education and training initiatives for customers. Regulators can draw on the framework to design policies and awareness campaigns that promote safer digital banking environments, while practitioners can apply its insights to build trust, improve satisfaction, and strengthen loyalty. In doing so, the study aligns with Malaysia's financial sector goals of enhancing digital adoption, advancing financial inclusion, and safeguarding consumer confidence in an increasingly digital economy.

Conclusion

This study highlights the pivotal role of cybersecurity awareness in shaping customer satisfaction within Malaysia's rapidly evolving digital banking sector. While technological safeguards remain indispensable, findings from the literature review underscore that customer awareness of cyberattacks, phishing, hacking, and data privacy directly influences trust and satisfaction with online banking services. By applying the Information System Success Model (ISSM), this paper positions awareness as a critical antecedent to satisfaction, demonstrating that cybersecurity is not only a technical challenge but also a behavioral and educational issue. The proposed conceptual framework contributes theoretically by extending ISSM to the digital banking domain, while practically offering a foundation for banks, regulators, and policymakers to design awareness campaigns, customer training, and communication strategies that strengthen resilience and foster long-term digital adoption. Ultimately, the study emphasizes that safeguarding customer confidence in Malaysia's digital banking ecosystem requires a balance between robust institutional defenses and empowered, security-conscious users.

Limitations and Future Research

Although this study provides important insights, it is not without limitations. First, as a conceptual paper, the framework has not yet been empirically validated, limiting its ability to demonstrate causal relationships between awareness and satisfaction. Future research should test the proposed model using quantitative methods such as surveys or structural equation modeling (SEM) across different customer segments in Malaysia. Second, the current framework focuses on four awareness dimensions—cyberattacks, phishing, hacking, and data privacy—yet other relevant factors such as mobile app usability, social engineering threats, or institutional communication quality could further enrich understanding. Third, this study is context-specific to Malaysia; cross-country comparative studies within ASEAN or other emerging economies could reveal cultural, institutional, or technological differences that shape cybersecurity behaviors. Finally, future research should explore moderating and mediating variables, such as trust, perceived risk, or digital literacy, to capture the nuanced pathways through which awareness translates into satisfaction and loyalty.

References

Abbas, Z. (2023). *Digital banks or traditional banks? Which one is likely to dominate the future of banking?* LinkedIn. Retrieved from https://www.linkedin.com

Ahmad, N., & Hassan, S. (2019). Cybersecurity awareness among bank customers in Malaysia. *Journal of Information Security*, 9(3), 123–135.

Amar Johri, S. K. (2023). Exploring customer awareness towards their cyber security. *Human Behavior and Emerging Technologies*, 5(2), 345–356.

Andress, J. (2014). *The basics of information security: Understanding the fundamentals of InfoSec in theory and practice.* Syngress.

Bank Negara Malaysia. (2020). *Annual report on banking and finance.* Kuala Lumpur: Bank Negara Malaysia.

Bauer, J. M. (2015). The new cybersecurity agenda: Economic and social challenges to a secure internet. *Oxford Global Cybersecurity Project, Oxford Martin Institute, University of Oxford and the Quello Center at Michigan State University*.

Bijnen, R., & Shaiques, K. (2021, July 12). The economic impact of cybercrime: No slowing down. *McAfee Report*. Retrieved from https://www.mcafee.com

Branch, J. (2020). What's in a name? Metaphors and cybersecurity. *International Organization*, 74(3), 489–512.

DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean model of information systems success: A ten-year update. *Journal of Management Information Systems*, 19(4), 9–30.

Fong, V. (2022, April 29). Bank Negara Malaysia announces much anticipated digital banking licenses. *Fintech News Malaysia.* Retrieved from https://fintechnews.my

GDSLINK. (2023, April 27). *Investment banking 101: Understanding services, strategies, and financial activities.* Retrieved from https://www.gdslink.com

Higgins, M. (2022, October 31). NordVPN: History of cybersecurity. *NordVPN Blog.* Retrieved from https://nordvpn.com/blog/history-of-cybersecurity/

Jackson, R. S., & Smith, J. J. (2020). Best practices in cybersecurity awareness for online banking. *International Journal of Cybersecurity*, 12(4), 345–360.

Jang-Jaccard, J., & Nepal, S. K. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80(5), 973–993.

Lim, C. T., Tan, S., & Lee, K. W. (2021). Customer satisfaction and cybersecurity awareness in online banking. *Journal of Financial Services Marketing*, 26(4), 567–589.

Lalankesh, G., Prasad, R., & Narayan, S. (2020). User satisfaction in health information systems: An application of the DeLone and McLean model. *Health Informatics Journal*, 26(2), 137–152.

Marecki, K. (2022). Cybersecurity issues affecting online banking and online transactions. *IBIMA Business Review*, 2022(14), 1–10.

Naager, Y. (2023). *The history of cyber security: A detailed guide.* LinkedIn. Retrieved from https://www.linkedin.com

Ozatac, N., Saner, T., & Sen, Z. (2016). Customer satisfaction in the banking sector: The case of North Cyprus. *Procedia Economics and Finance*, 39, 870–878.

Qureshi, M. I. (2022). Extending the DeLone and McLean model of information systems success in financial services. *Journal of Information Systems Research*, 33(2), 156–173.

Ramayah, T., Ahmad, N. H., & Halim, H. (2021). Information system success model in financial services: An empirical validation. *Asian Journal of Business and Accounting*, 14(1), 23–45.

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, 2(2), 121–135.

Salaudeen, A. O. (2023, July 19). Introduction to Islamic finance. *ETHIS Blog.* Retrieved from https://ethis.co/blog

Saravanakumar, N. (2024, March 19). Islamic banking. *Wallstreetmojo.* Retrieved from https://www.wallstreetmojo.com/islamic-banking/

Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What everyone needs to know.* Oxford University Press.

Smith, J. J., & Jackson, R. S. (2020). Factors influencing cybersecurity awareness. *Journal of Cyber Studies*, 8(2), 87–104.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102.