INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 16, Issue 2, (2026) E-ISSN: 2222-6990

A Review of Cybersecurity Awareness and its Impact on Continuous Online Banking Usage among Students

Ahmed Hassan Ali Ibrahim Bisho
Universiti Teknikal Malaysia Melaka, Institute of Technology Management and Entrepreneurship Centre for Research and Innovation Management
Email: p061910005@student.utem.edu.my

Muhammad Syafiq
Universiti Teknikal Malaysia Melaka, Faculty of Technology Management and Technopreneurship, Universiti Teknikal Malaysia Melaka
Email: m.syafiq.asin@gmail.com

Samer Ali alshami
Universiti Teknikal Malaysia Melaka, Institute of Technology Management and Entrepreneurship
Email: samerali@utem.edu.my

DOI Link: http://dx.doi.org/10.6007/IJARBSS/v16-i2/27653

Published Date: 21 February 2026

Abstract

Online banking has become an essential financial service, particularly among university students who rely heavily on digital platforms for daily transactions. However, the increasing dependence on online banking also exposes users to cybersecurity threats such as phishing, hacking, and data breaches, which may undermine trust and reduce continuous usage. Despite technological safeguards implemented by banks, limited cybersecurity awareness among users remains a critical issue, especially within the Malaysian university context. This review paper aims to identify the opportunities, challenges, and future research directions related to cybersecurity awareness and its influence on continuous online banking usage among students. A theory-based literature review method was employed, synthesizing prior studies and applying the DeLone and McLean Information Systems Success Model to examine the relationships between awareness, satisfaction, trust, and continuance intention. The findings indicate that cybersecurity awareness enhances customer satisfaction and trust, supporting continuous usage, while challenges persist due to evolving threats and user behavior vulnerabilities.

Keywords: Cybersecurity, Students, Awareness, Continuous, Banking

Introduction

Online banking has become a core service in modern financial systems because it enables users to conduct transactions, monitor accounts, and manage personal finances through digital platforms with high convenience and speed. More importantly, it now functions as a critical "everyday infrastructure" for individuals and institutions—supporting salary payments, bill settlements, education-related fees, e-commerce, and emergency money transfers. As online banking becomes more embedded in daily life, its effectiveness is no longer judged only by speed and convenience, but by whether users can rely on it confidently and safely. This makes the topic worth studying: if customers do not feel secure, they may reduce usage, avoid digital services, or revert to cash-based behavior—weakening the value of online banking investments and slowing progress toward digital financial inclusion.

In Malaysia, online banking is increasingly embedded in daily life through bank websites, mobile apps, and newer digital bank offerings. This shift supports wider financial access, reduces dependency on physical branches, and aligns with growing expectations for efficient, always-available services. For banks and regulators, sustained online banking usage also matters because it reduces service costs, improves operational efficiency, and supports national digital-economy goals. For users, especially young adults, online banking supports independence, budgeting, and daily financial stability. However, the same digital convenience that makes online banking attractive also creates exposure to cybersecurity threats, including phishing, hacking, malware, ransomware, and data breaches. These threats do not only target banking infrastructure; they also exploit users' behavior and awareness gaps, making customer cybersecurity awareness an important factor in sustaining long-term usage. Marecki (2022) emphasizes that cybercriminal strategies continue to adapt, often exploiting vulnerabilities in online banking systems and user behavior to obtain sensitive financial information and resources.

In cybersecurity decision-making, risk and threat assessment is central. Costigan and Hennessy (2016) explain that security responses should be proportionate to risk and value, which highlights a critical tension in online banking: systems must protect users effectively while still maintaining usability and access. If security is too weak, users face higher exposure; if security processes are too complex, users may feel frustrated and abandon online banking services. Therefore, studying cybersecurity awareness is practically useful: awareness is a low-cost, scalable "human layer" of protection that complements technical controls and can directly improve trust, satisfaction, and continued usage. This balance becomes more difficult as cyber threats evolve, and it becomes even more significant for frequent digital users such as university students. Historically, cybersecurity emerged alongside the expansion of networked computing. Naager (2023) notes how early defensive approaches and ethical hacking ideas developed in the 1960s, while Branch (2020) and Higgins (2022) describe how the creation of ARPANET and early self-replicating programs highlighted the need for protective measures as connectivity increased. This historical progression is relevant today because it shows that cybersecurity risks have grown alongside technological advancement, and user awareness remains a necessary layer of defense.

Within Malaysia's banking landscape, financial services are offered through commercial banks, Islamic banks, digital banks, and investment banks. Islamic banking operates under Shariah principles such as the prohibition of interest (riba), using profit-sharing and

partnership mechanisms instead (Salaudeen, 2023). Digital banks (often called neobanks) deliver services fully online through apps and websites, offering convenience and innovative features, but they also face heightened exposure to cyberattacks because of their heavy reliance on digital infrastructure (Abbas, 2023). Banking structures and expansion trends provide important context because continuous usage of online banking depends on both system reliability and users' confidence in safety. Bank Negara Malaysia's listings of registered banks reflect the scale and diversity of the banking ecosystem that depends on customer trust in digital platforms (Bank Negara Malaysia, n.d.).

University students are a particularly relevant group to study because they use online platforms frequently, often manage finances independently, and typically depend on mobile-first services. At the same time, being active users does not automatically mean students possess strong cybersecurity awareness. Cyberattacks frequently succeed through social engineering—such as phishing—rather than purely technical system failures. Johri (2023) notes how phishing scams remain a key route for identity theft and fraud because they manipulate users into disclosing credentials. Focusing on students is beneficial for multiple stakeholders: universities can strengthen student digital safety programs, banks can design clearer security communication and user-friendly safeguards, and policymakers can improve consumer protection initiatives for young digital citizens. For students themselves, stronger awareness reduces the risk of financial loss and identity misuse while supporting confident, continuous use of digital financial services. This suggests that awareness is not only an individual skill but a major factor influencing customer satisfaction, trust, and continued usage behavior. This review paper has one central objective: to identify the opportunities, challenges, and future research directions related to cybersecurity awareness that influence continuous online banking usage among students. This objective is addressed through a theory-based synthesis of existing literature, linking cybersecurity awareness to satisfaction, trust, and continuance intention.

Literature Review

Cybersecurity awareness and continuous online banking usage are best understood through theoretical perspectives that connect technology quality, user perceptions, satisfaction, trust, and behavioral intention. Because online banking is both a technical system and a user-driven service experience, a theory-based review must account for how system design interacts with user behavior and awareness. In this review, the DeLone and McLean Information Systems Success Model provides a useful lens, complemented by cybersecurity risk perspectives and trust-based explanations.

Cybersecurity is commonly defined as the practice of protecting systems, networks, and programs from digital attacks that seek to access data, disrupt operations, or cause damage (Von Solms & Van Niekerk, 2013; Singer & Friedman, 2014). In online banking, cybersecurity is not only an organizational responsibility; it is also shaped by customer interaction with the system. Users are required to make decisions that involve security trade-offs, such as choosing passwords, evaluating suspicious messages, and deciding whether to enable additional authentication features. A risk-based perspective is therefore important. Costigan and Hennessy (2016) emphasize that security decision-making is guided by risk measurement and threats, and that the most difficult challenge is achieving balance between protection and priorities such as usability and access. Online banking systems must therefore be

designed not only to block attacks but also to support users in behaving securely without increasing frustration.

The importance of cybersecurity is strengthened by the high impact of cyber incidents. Cyberattacks can produce financial losses, disrupt services, compromise privacy, and damage trust. Broader cybersecurity research emphasizes how digital dependency increases the severity of successful attacks, including disruptions to critical services and large-scale privacy breaches (Amin et al., 2013; Johnson, 2008). At a national level, governments treat cybersecurity as essential for protecting public and economic stability, reinforcing why banking security is high-stakes (U.S. Department of Homeland Security, 2020). In organizational settings, cybersecurity is also described as a continuous improvement process requiring ongoing audits, vulnerability assessment, and updates to remain effective against evolving threats (Tunggal, 2024). These ideas support the argument that cybersecurity awareness among users should also be treated as a continuous effort rather than a one-time intervention.

The evolution of cybersecurity provides helpful context for understanding why user awareness matters. Naager (2023) highlights that early defensive practices and ethical hacking concepts emerged alongside early computing, while Branch (2020) links cybersecurity development to the creation of ARPANET and the new vulnerabilities introduced by network interconnection. Higgins (2022) further describes early self-propagating code such as the Creeper worm and the subsequent development of Reaper as an early countermeasure. These historical examples show that as connectivity grows, threats become more sophisticated and defenses must evolve. In modern online banking, this evolution appears in the rise of advanced phishing campaigns, malware targeting financial credentials, and ransomware. The major shift is that many attacks now rely on manipulating users rather than directly breaking security systems, which makes awareness a critical protective layer.

A key part of understanding continuous online banking usage is recognizing how satisfaction and trust shape customer behavior. Online banking delivers value through convenience and efficiency. Bhasin (2021) emphasizes that online banking provides advantages such as anytime access, reduced need for branch visits, cost efficiency, and security features like encryption and multi-factor authentication. However, user experience is not universally positive. Kagan (2021) notes that online banking faces challenges such as cyber threats, technological barriers for certain users, and dependency on reliable internet access. These challenges create friction that can reduce satisfaction and limit adoption or continuance.

To connect these factors systematically, the DeLone and McLean (2003) Information Systems Success Model (ISSM) is widely used because it explains how system quality, information quality, and service quality influence user satisfaction and intention to use (or continued use). In online banking, system quality includes usability, reliability, speed, and security features. Information quality includes accuracy, clarity, and transparency about policies or security processes. Service quality includes customer support and responsiveness, especially when fraud or suspicious activity occurs. When these qualities are high, satisfaction improves, and satisfaction increases continuance intention (DeLone & McLean, 2003). This logic fits online banking because customer trust depends on both the technical experience and the perceived safety of transactions.

Cybersecurity awareness strengthens this model because awareness shapes how users interpret system quality and security signals. If a user understands phishing risks and recognizes how two-factor authentication protects accounts, security features are more likely to increase confidence rather than appear as inconvenient barriers. Lim et al. (2021) report that higher cybersecurity awareness is associated with stronger customer satisfaction and trust in online banking. Martins et al. (2022) similarly explain that when customers understand cybersecurity risks and the function of security measures, they perceive the bank as more trustworthy, which strengthens satisfaction. This suggests that awareness acts as a cognitive mechanism that translates security design into trust and satisfaction outcomes. Where awareness is low, users may misinterpret security features as unnecessary complexity, or they may underestimate risks and behave unsafely, increasing the likelihood of negative experiences such as fraud.

The literature also suggests that cybersecurity awareness does not occur automatically, even among technologically active users. The banking industry increasingly relies on cyber threat intelligence to manage incidents, but customer awareness remains distinct from organizational monitoring. Md Sahrom Abu (2018) explains that banks often subscribe to threat intelligence services, yet large volumes of data can create overload, requiring platforms like Threat Intelligence Sharing Platforms (TISP) to translate information into actionable insights. While this strengthens institutional response, it does not guarantee that users understand risks or practice safe behavior. Positive Technologies (2023) reports that financial organizations face major consequences such as data leaks and service interruptions, reinforcing that cybersecurity threats remain persistent and costly. These findings highlight why user awareness is necessary: banks can improve detection and response, but customers still make security decisions during daily online banking interactions.

Phishing is one of the most relevant awareness components for online banking continuance because it targets users directly. Johri (2023) describes phishing as a major pathway for identity theft and fraud, which aligns with broader observations that phishing remains common due to its reliance on deception rather than technical intrusion. Awareness of phishing involves the ability to recognize suspicious links, mismatched URLs, unusual requests for credentials, and impersonation tactics. When users lack this awareness, they may experience account compromise, loss of funds, and psychological stress, reducing satisfaction and discouraging further use. In contrast, when users are educated and protected, trust increases, supporting continued usage.

Awareness also extends to hacking and account security practices. Ahmad and Hassan (2019) describe how greater awareness of hacking risks correlates with higher trust and satisfaction. This relationship makes sense in online banking because customers who understand hacking risks are more likely to engage in protective behavior—such as enabling authentication or monitoring accounts—and more likely to value the bank's security measures. Awareness of data privacy further strengthens satisfaction because banking involves sensitive personal and financial information. Lim et al. (2021) emphasize that privacy understanding increases confidence, which supports continuance intention.

Several studies and reports indicate that education and communication strategies are essential for awareness. Deloitte (2021) highlights that customer cybersecurity education

campaigns can reduce attack likelihood while building customer engagement and satisfaction. These campaigns may include workshops, emails, fraud alerts, and guidance on secure practices. Tan and Lee (2021) similarly emphasize that education about risks and mitigation strategies increases trust and supports continued adoption. This aligns with the idea that awareness supports both prevention and customer experience: a user who feels informed is more likely to feel secure, satisfied, and loyal.

Future online banking trends also influence the awareness–continuance relationship. Haider (2020) discusses how mobile banking growth, blockchain applications, and AI integration may shape future banking services. These trends may offer both improved security and new risks. For example, AI-based fraud detection can identify suspicious activity faster, but users still need awareness to respond appropriately to fraud alerts, avoid social engineering, and manage privacy settings. The rise of digital banks further increases the urgency of awareness because purely online institutions depend entirely on digital trust (Abbas, 2023). In Malaysia's banking structure, the expansion of digital banks and mobile-first services suggests that awareness among younger users is increasingly central to sustainable adoption (Bank Negara Malaysia, n.d.; Fong, 2022).

The context of strengthens the relevance of this topic. student population is likely to engage heavily with digital tools and online systems, making online banking a routine behavior (UTeM, 2023). However, high usage does not eliminate vulnerability. Instead, frequent usage may increase exposure to attacks and raise the importance of awareness. The university context also provides opportunities for structured interventions, such as cybersecurity literacy integration, awareness workshops, and partnerships with banks. Mohammed Afzal et al. (2024) emphasize the importance of cybersecurity awareness in achieving digital financial inclusion, which supports the idea that awareness is foundational for sustained digital finance participation. Applying this insight to the student context suggests that awareness is not only a protective factor but also a participation enabler that supports continuance.

In summary, theory and evidence converge on a central point: continuous online banking usage depends not only on system security but also on how users perceive, understand, and respond to cybersecurity risks. The DeLone and McLean (2003) model explains satisfaction and continued use through quality dimensions, while cybersecurity awareness strengthens trust and satisfaction by shaping user interpretations of risk and security measures (Lim et al., 2021; Martins et al., 2022). This provides a strong foundation for identifying opportunities, challenges, and future research directions.

Opportunities

Opportunities related to cybersecurity awareness in online banking arise when banks and institutions treat awareness as a value-creating factor rather than only a defensive requirement. Evidence suggests that awareness improves satisfaction and trust, which are key drivers of continuance intention. When users understand why security measures exist and how threats operate, they are more likely to adopt safe practices and continue using online banking with confidence (Lim et al., 2021; Martins et al., 2022). Education campaigns that empower users also strengthen engagement and satisfaction (Deloitte, 2021). Mobile-first banking growth creates an opportunity to embed awareness features directly into

banking apps, such as interactive tutorials, alerts, and simplified security guidance (Haider, 2020).

Table 1
Opportunities and Supporting Citations

Opportunities	**Citation**
Cybersecurity awareness increasing customer trust and satisfaction	Lim et al. (2021); Martins et al. (2022)
Customer education campaigns improving engagement and confidence	Deloitte (2021)
Mobile-first awareness integration via apps and digital tools	Haider (2020)
Awareness programs strengthening adoption and continuance through trust	Tan & Lee (2021)
Awareness supporting digital finance participation and inclusion	Mohammed Afzal et al. (2024)

Challenges

Challenges emerge because cybersecurity threats evolve rapidly and frequently exploit user behavior. Even when banks implement robust technical protections, customers remain vulnerable to social engineering and deception-based attacks such as phishing (Johri, 2023). Users may also experience barriers related to technology confidence, access to stable internet, and the ability to interpret security warnings correctly (Kagan, 2021). At an industry level, banks manage complex threat intelligence data that may not translate into user-level understanding, creating a gap between institutional security capabilities and customer behavior (Md Sahrom Abu, 2018). Persistent incidents such as data leaks and service interruptions reinforce that threats remain difficult to eliminate entirely, which can undermine user trust if not addressed through awareness and communication (Positive Technologies, 2023).

Table 2
Challenges

Challenges	**Citation**
Cybercriminal adaptation and exploitation of vulnerabilities	Marecki (2022)
Phishing as a persistent pathway for fraud and identity theft	Johri (2023)
User barriers: digital literacy and internet access constraints	Kagan (2021)
Institutional threat intelligence overload not translating to users	Md Sahrom Abu (2018)
Ongoing financial-sector data leaks and service disruption impacts	Positive Technologies (2023)

Future Research Table

Future research should deepen understanding of how cybersecurity awareness shapes continuance behavior, especially among student populations. Much existing work emphasizes system-level security or short-term adoption intentions, but continuance requires examining long-term trust, satisfaction, and repeated use patterns, consistent with the ISSM logic (DeLone & McLean, 2003). Research should also explore how students interpret awareness interventions within mobile banking environments and how educational strategies can be personalized. Since awareness may influence satisfaction through trust mechanisms, more work is needed to test mediation pathways and identify which awareness dimensions (phishing, hacking, privacy) are most predictive of continued usage in the Malaysian student context (Lim et al., 2021; Martins et al., 2022).

Table 3
Future Research Directions

Future Research	**Citation**
Testing trust and satisfaction mechanisms in online banking users	Lim et al. (2021); Martins et al. (2022)
Evaluating effectiveness of awareness education campaigns	Deloitte (2021); Tan & Lee (2021)
Exploring mobile banking and AI security communication impacts	Haider (2020)
Context-specific study among Malaysian university students	Mohammed Afzal et al. (2024)

Conclusion

This review highlights cybersecurity awareness as a central factor shaping continuous online banking usage among students. As online banking becomes increasingly essential for daily financial management, the sustainability of digital banking services depends not only on technical safeguards but also on user knowledge and behavior. Risk-based security perspectives emphasize that effective protection must balance security strength with usability and access, especially in high-frequency systems like online banking (Costigan & Hennessy, 2016). The historical evolution of cybersecurity also demonstrates that threats emerge and evolve alongside technological connectivity, reinforcing the need for adaptive protection strategies that include awareness (Naager, 2023; Branch, 2020; Higgins, 2022).

From a theory-based perspective, the DeLone and McLean Information Systems Success Model provides a strong explanation for continuance behavior by linking quality dimensions to satisfaction and continued use (DeLone & McLean, 2003). Within this framework, cybersecurity awareness strengthens perceived security, trust, and satisfaction, thereby encouraging continuous usage. Empirical and applied literature supports this relationship by showing that higher cybersecurity awareness increases trust and satisfaction in online banking environments (Lim et al., 2021; Martins et al., 2022). Education initiatives and communication strategies further reinforce satisfaction by empowering users and reducing perceived risk (Deloitte, 2021).

At the same time, the challenges remain significant. Cybercriminal tactics continue to evolve, and phishing persists as a major threat because it exploits human decision-making rather than

system vulnerabilities (Marecki, 2022; Johri, 2023). Barriers such as technology confidence and internet access limitations can also weaken consistent adoption (Kagan, 2021). Industry-level threat intelligence systems strengthen detection, but they may not directly improve customer behavior unless awareness is addressed intentionally (Md Sahrom Abu, 2018; Positive Technologies, 2023).

Overall, this review identifies that awareness is both a protective resource and a driver of confidence, satisfaction, and continued usage. Future research should examine long-term continuance behavior among student users, test trust and satisfaction pathways, and evaluate how awareness interventions can be embedded into mobile banking environments and educational settings (DeLone & McLean, 2003; Lim et al., 2021; Martins et al., 2022; Haider, 2020). Strengthening cybersecurity awareness among students can therefore contribute to safer banking behavior, higher customer satisfaction, and more sustainable online banking adoption.

References

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

Ali, S., & Patel, R. (2022). *Defining cybersecurity: Perspectives and frameworks*. International Journal of Information Security, 21(3), 345–360.

Amin, S. L. (2013). *Cyber security of wireless connected and automated vehicles in transportation systems*. Proceedings of the IEEE, 1781–1791.

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, Malaysia: Bank Negara Malaysia.

Bhasin, H. (2021). *Importance of Online Banking*. Retrieved from Marketing91.

Bijnen, R., & Shaiques, M. (2021). *The economic impact of cybercrime: No slowing down*. McAfee Report.

Branch, J. (2020). *What's in a Name? Metaphors and Cybersecurity*. International Organization.

Dan Craigen, N. D.-T. (2014). *Defining Cybersecurity*. Technology Innovation Management Review, 13–21.

Fariza Khalid, M. Y. (2018). *An Investigation of University Students' Awareness on Cyber Security*. International Journal of Engineering & Technology, 11–14.

Haider, Z. (2020). *The Role and Impact of Online Banking on Financial Performance*. Journal of Internet Banking and Commerce.

Higgins, M. (2022). *History of cybersecurity*. NordVPN.

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

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

Johri, A. (2023). *The impact of cybersecurity threats on the banking sector*. Journal of Financial Security, 45–56.

Kagan, J. (2021). *Online Banking*. Investopedia.

Kaur, S., & Singh, T. (2022). *Challenges in implementing cybersecurity awareness programs in Malaysia*. Cybersecurity Journal, 78–91.

Khattab Ibrahim Hadid, N. K. (2020). *The Effect of Digital Banking Service Quality on Customer Satisfaction*. Asian Journal of Applied Science and Technology, 06–29.

Lim, C. T. (2021). *Customer satisfaction and cybersecurity awareness in online banking*. Journal of Financial Services, 567–589.

Lim, K. L. (2021). *Cybersecurity awareness and customer satisfaction in online banking*. Journal of Digital Banking, 102–114.

Marecki, K. (2022). *Cybersecurity Issues Affecting Online Banking and Online Transaction*. IBIMA.

Martins, C. S. (2022). *The role of user cybersecurity awareness in banking services adoption*. International Journal of Banking Technology, 57–68.

Md Sahrom Abu, S. R. (2018). *Cyber Threat Intelligence – Issue and Challenges*. Indonesian Journal of Electrical Engineering and Computer Science, 371–379.

Mohammed Afzal, M. M. (2024). *How does cybersecurity awareness help in achieving digital financial inclusion in rural India under escalating cyber fraud scenario?* Journal of Cyber Security Technology.

Naager, Y. (2023). *The History of Cyber Security: A Detailed Guide*. LinkedIn.

Nalin Asanka Gamagedara Arachchilage, S. L. (2013). *A game design framework for avoiding phishing attacks*. Computers in Human Behavior, 706–714.

Nesrin Ozatac, T. S. (2016). *Customer Satisfaction in the Banking Sector*. Procedia Economics and Finance, 870–878.

Positve Technologies. (2023). *Cyberthreats to the financial industry: Interim results for 2023*.

Rahman, A. A. (2018). *Technological literacy and cybersecurity in Malaysia*. Asian Journal of Technology and Society, 150–170.

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

Sean S. Costigan & Michael A. Hennessy. (2016). *Cybersecurity: A Generic Reference Curriculum*.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What Everyone Needs to Know*. Oxford University Press.

Tan, S., & Lee, V. (2021). *Educational initiatives to enhance cybersecurity awareness in Malaysia*. Malaysian Journal of Information Security, 210–225.

Tassaddiq, T. A. (2021). *Assessment of Cybersecurity Awareness among Students*. Big Data and Cognitive Computing, 5(23).

Tunggal, A. T. (2024). *Why is Cybersecurity Important?* Upguard.

U.S. Department of Homeland Security. (2020). *Cybersecurity Strategy*.

Zahidah Zulkifli, N. N. (2020). *Cyber Security Awareness Among Secondary School Students in Malaysia*. Journal of Information System and Digital Technology, 28–41.