Frontiers in Health Informatics
ISSN-Online: 2676-7104
www.healthinformaticsjournal.com
2024; Vol 13: Issue 4
Open Access

Cyber Security Threats In The Age Of Digital Banking

Dr. M Josephine Renjith[1], Sindoora S[2]

[1]Assistant Professor and Research Supervisor PG & Research Department of Commerc Malankara Catholic College Mariagiri, Kaliakkavilai 629153 Affiliated to Manonmaniam Sundaranar University Abhishekapatti, Tirunelveli 627012, Tamil Nadu. Email id: sabiselva2006@gmail.com

[2]Reg No : 22113081012002 PhD & Research Scholar Commerce (Full Time) PG & Research Department of Commerce Malankara Catholic College, Mariagiri, Kaliakkavilai 629153 Affiliated to Manonmaniam Sundaranar University Abhishekapatti, Tirunelveli 627012, Tamil Nadu. Email Id: sindoora007@gmail.com

Cite this paper as: Dr. M Josephine Renjith, Sindoora S (2024) Cyber Security Threats In The Age Of Digital Banking. *Frontiers in Health Informatics, 13* (4),1797-1807

Abstract

The surge in digital banking in Kerala has facilitated financial inclusion but has also intensified exposure to cybersecurity threats. This study investigates the relationship between users' awareness levels, security practices, and vulnerability to cyber threats among digital banking users in Kerala. A structured questionnaire with 40 Likert-scale items was administered to a random sample of 300 users. Data analysis was conducted using EDUSTAT, applying descriptive statistics, Pearson correlation, independent samples t-tests, and percentages. Results indicate that higher awareness correlates with lower susceptibility, stronger security practices reduce cyber incidents, and elderly users are more vulnerable to cyber threats than younger users. The findings underscore the need for enhanced cybersecurity education and targeted interventions. This paper offers insights into improving user-side cybersecurity resilience in digital banking environments.

Keywords: Digital Banking, Cybersecurity Awareness

Introduction

The emergence of digital banking has revolutionized the financial services landscape, offering customers unprecedented convenience, efficiency, and accessibility for conducting transactions. Digital platforms have minimized the need for physical bank visits, allowing users to manage their finances remotely through internet banking, mobile banking applications, and electronic wallets. The transition from traditional brick-and-mortar banking to digital interfaces represents a significant technological advancement that has reshaped consumer expectations and operational models within the banking sector. In India, the momentum towards digital banking has been strongly propelled by the Digital India initiative, launched in 2015, which sought to enhance online infrastructure and increase internet connectivity across the nation. Kerala, with its high literacy rates and extensive internet penetration, has been at the forefront of adopting digital banking services (Kaur & Arora, 2020).

However, the rapid digital shift has not been without consequences. Alongside the many benefits of digital banking, there has been a concurrent amplification of cybersecurity threats, exposing users to a wide range of risks including phishing attacks, malware infiltration, identity theft, ransomware incidents, and data breaches. The vulnerabilities introduced by digital financial interactions are complex, stemming not only from technical flaws but also from human errors, inadequate cybersecurity awareness, and unsafe online behaviours. These threats have increasingly targeted individual users, who often lack the sophisticated tools and training available to large financial institutions to defend against cyberattacks. Consequently, as the banking industry continues

its digital transformation, it also faces mounting pressure to safeguard user data and ensure secure transaction environments.

Recent research highlights that user-related factors, such as cybersecurity awareness, vigilance, and adherence to recommended security practices, significantly determine the extent of an individual's vulnerability to cyber threats (Sharma & Patel, 2021). It is no longer sufficient for banks alone to maintain robust cybersecurity infrastructures; users themselves play a critical role in protecting their financial data. In Kerala, despite widespread adoption of smartphones, online banking applications, and e-commerce platforms, a considerable portion of the population remains inadequately informed about basic cyber hygiene. Issues such as weak password practices, falling victim to social engineering attacks, sharing sensitive information over unsecured networks, and delayed software updates continue to contribute to the growing incidence of digital fraud and cybercrimes. This gap between technological advancement and cybersecurity preparedness at the user level presents a major challenge for the sustainable growth of digital banking.

While financial institutions in Kerala and across India have invested heavily in strengthening their cybersecurity frameworks through firewalls, encryption technologies, two-factor authentication, and real-time monitoring systems, user-side vulnerabilities remain a significant weak point (Nair & Menon, 2022). Many cyber incidents occur not because banks fail to secure their systems, but because end-users unknowingly engage in risky behaviours that compromise security. Addressing this dichotomy between institutional security measures and user behaviours requires a holistic approach that encompasses technological innovations, educational initiatives, and behaviour modification strategies. Bridging the gap between cybersecurity infrastructure and user engagement is therefore crucial for developing a secure and resilient digital banking ecosystem. Against this backdrop, the present study focuses on exploring the behavioural dimensions influencing cybersecurity practices among digital banking users in Kerala, seeking to identify factors that contribute to user vulnerability and proposing measures to enhance user-side cybersecurity resilience.

Review of Literature

Chakraborty and Mitra (2021) investigated cybersecurity threats within the Indian digital banking ecosystem and highlighted the growing sophistication of cyberattacks targeting financial transactions. Their study found that phishing and identity theft were the most prevalent threats, often exploiting human vulnerabilities rather than system flaws. They concluded that cybersecurity awareness among customers was a critical defines mechanism and emphasized the need for banks to engage in proactive educational initiatives to mitigate risks.

Kaur and Arora (2020) explored the dual-edged nature of digital banking advancement and cybersecurity challenges in India. Their research revealed that while banks invested heavily in infrastructure security, the effectiveness of these measures was significantly undermined by low user awareness and negligent online behaviours. They proposed a framework integrating technology, user training, and regulatory oversight to build a more resilient digital banking environment, particularly in regions like Kerala with high digital adoption rates.

Sundararajan (2021) conducted a study focused on cybersecurity strategies in the banking sector and emphasized the role of user-centric cybersecurity policies. The study revealed that technical upgrades alone were insufficient without accompanying behaviour modification among users. Sundararajan's findings underscored the importance of continuous customer education, regular cybersecurity audits, and customized interventions for vulnerable groups such as elderly users who exhibited higher risk profiles in digital banking.

Mohan and Raj (2020) examined the impact of the Digital India initiative on banking practices and associated cybersecurity risks. They found that while digitalization improved service efficiency, it also introduced vulnerabilities due to uneven cybersecurity literacy among users. Their study highlighted that elderly users, rural populations, and first-time digital bankers were particularly susceptible to cyberattacks, thereby calling

for tailored cybersecurity programs aimed at these demographics.

Nair and Menon (2022) explored cybersecurity awareness among millennials in Kerala and found that although this demographic exhibited higher digital literacy, many lacked comprehensive cybersecurity knowledge. Their study showed a positive correlation between cybersecurity training and safe online banking behaviour. They recommended that banks introduce mandatory cybersecurity education modules during the onboarding of new digital banking customers to enhance overall system resilience.

Sharma and Patel (2021) conducted an empirical analysis of emerging cyber threats in digital banking and found that the frequency of attacks had increased notably after the COVID-19 pandemic, as more users adopted digital platforms for transactions. The study indicated that while banks had strengthened server-side protections, client-side vulnerabilities—particularly phishing susceptibility and password reuse—remained prominent issues. They advocated for behaviourally informed security designs that nudge users toward safer practices.

Gupta and Sharma (2020) analysed the behavioural patterns associated with cybersecurity practices among Indian banking customers. Their research found that awareness did not always translate into secure behaviour. For instance, users aware of phishing risks still occasionally clicked on suspicious links due to behavioural biases like overconfidence. The study recommended designing security systems that account for psychological tendencies, promoting automatic protections rather than relying solely on user vigilance.

Patel and Desai (2019) examined the relationship between demographic variables and vulnerability to cyber threats in digital banking. Their findings showed that age, educational background, and previous exposure to technology significantly influenced cybersecurity behaviours. Elderly users and users from non-technical educational backgrounds were particularly vulnerable. The study concluded that digital banking cybersecurity strategies must adopt a segmented approach, offering differentiated security features and awareness programs based on user demographics.

Agarwal and Sengupta (2021) analysed the effectiveness of cybersecurity policies implemented by Indian banks and emphasized the critical role of customer behaviour in ensuring policy success. Their findings suggested that while technological upgrades were essential, the real challenge lay in creating cybersecurity-conscious customers. They highlighted that awareness programs must be interactive and contextualized to users' everyday digital experiences to achieve tangible reductions in cyber risks.

Thomas and Mathew (2020) studied phishing attacks in digital banking and noted a sharp rise in social engineering-based cybercrimes post-2018 in India. Their study found that despite technological interventions like two-factor authentication, phishing continued to be effective because of low user vigilance. They recommended banks develop behavioural nudges, such as regular SMS alerts and in-app notifications about common scam tactics, to combat phishing more effectively.

Iyer and Sharma (2020) investigated the cybersecurity challenges faced by rural banking customers in India. Their research revealed that rural users, although enthusiastic adopters of mobile banking, often lacked basic cybersecurity knowledge, making them prime targets for fraudsters. They argued for region-specific digital literacy campaigns that address language barriers and cultural perceptions around banking security.

Jain and Aggarwal (2019) conducted a comparative study between public and private sector banks in India regarding cybersecurity preparedness. Their findings indicated that private banks generally had better cybersecurity infrastructure and more user-centric education programs compared to public sector banks. However, the study also emphasized that regardless of infrastructure, user negligence remained a significant threat, calling for universal customer awareness efforts.

Bansal and Kaur (2019) explored the psychological aspects of cybersecurity behaviour in digital banking users. They found that users who perceived cybersecurity as a shared responsibility between themselves and banks

exhibited safer online behaviours. Conversely, users who placed complete trust in banks without personal vigilance were more prone to cyber incidents. The study recommended that banks frame cybersecurity not only as a service but also as a shared responsibility.

Das and Nayak (2018) examined the effects of cybersecurity training on digital banking safety in Indian metropolitan cities. Their study demonstrated that users who had received structured cybersecurity training reported significantly fewer cyber incidents. They stressed the importance of continuous, modular training rather than one-time awareness programs to keep users updated about evolving threats.

Kavitha and Devi (2018) focused on the elderly population's experiences with digital banking and cybersecurity in southern India. Their study showed that elderly users faced challenges not only due to technological unfamiliarity but also because of a lack of tailored cybersecurity guidance from banks. They recommended that banks offer specialized workshops for elderly customers and simplify interfaces to minimize security breaches.

Menon and Kumar (2017) assessed the influence of trust and perceived security on digital banking adoption among Indian users. Their findings highlighted that perceived security had a significant impact on adoption behaviour, especially among first-time users. The study suggested that building user trust through transparent communication about cybersecurity practices could enhance both adoption rates and secure usage.

Background of the Study

Kerala's banking landscape has witnessed an unprecedented wave of digitalization over the past decade, catalysed by advancements in internet connectivity, smartphone penetration, and state-level initiatives promoting financial inclusion. Digital banking services such as online fund transfers, mobile banking applications, UPI transactions, and e-wallet services have become integral components of daily financial activities for a significant segment of the population. Public sector banks, private banks, and new-age fintech companies have actively promoted digital platforms to enhance service accessibility and operational efficiency. However, this widespread adoption of digital banking has also inadvertently opened up new avenues for cybercriminals. As highlighted by Mohan and Raj (2020), cybercrimes targeting both banking institutions and their customers have risen in parallel with the growth of digital financial services, threatening to erode user trust and destabilize digital financial ecosystems.

Cybercriminals frequently exploit gaps in user awareness and behavioural weaknesses to orchestrate sophisticated attacks such as phishing, ransomware attacks, social engineering scams, and credential theft. Despite robust technological defences employed by banks, the human element often remains the weakest link in cybersecurity (Chakraborty & Mitra, 2021). Studies have consistently shown that awareness and structured training can significantly reduce user-side cybersecurity risks. Nevertheless, user negligence persists even among well-educated and digitally literate populations in Kerala. Common behaviours such as setting weak or easily guessable passwords, sharing personal financial information over unsecured networks, ignoring software updates, and failing to recognize fraudulent communication channels continue to expose users to potential cyber threats. These behavioural patterns suggest that technology alone cannot safeguard the digital banking ecosystem; behavioural interventions and widespread cybersecurity education are equally crucial.

In addition to general awareness gaps, demographic factors also play a critical role in determining an individual's vulnerability to cyber threats. Age, in particular, has emerged as a significant determinant. As noted by Sundararajan (2021), elderly users, who often have limited familiarity with digital technologies, tend to be more susceptible to online frauds such as phishing attacks, identity theft, and deceptive financial schemes. Unlike younger, tech-savvy generations, elderly users may find it challenging to differentiate between legitimate and malicious online communications. Their lower propensity to adopt security best practices, such as enabling two-factor authentication or regularly updating applications, further increases their risk. Therefore,

a nuanced understanding of demographic vulnerabilities, in conjunction with overall cybersecurity awareness and behaviour patterns, is essential for designing effective and inclusive cybersecurity strategies in the context of digital banking in Kerala. Addressing these dimensions holistically can significantly strengthen the resilience of the digital financial ecosystem against emerging cyber threats.

Research Objectives

1. To examine the relationship between users' awareness levels and their susceptibility to cyber threats in digital banking.
2. To assess the impact of adopting stronger security measures on the occurrence of cyber incidents.
3. To analyse the difference in vulnerability to cyber threats between elderly and younger digital banking users.

Research Questions

1. What is the relationship between cybersecurity awareness and susceptibility to cyber threats among digital banking users?
2. How do security practices influence the occurrence of cyber incidents?
3. Are elderly users more vulnerable to cyber threats compared to younger users?

Hypotheses

- H_1: There is a significant relationship between users' awareness levels and their susceptibility to cyber threats.
- H_2: Users who adopt stronger security measures experience fewer cyber incidents.
- H_3: Elderly users are more vulnerable to cyber threats compared to younger users.

Methodology

This study adopted a descriptive and analytical research design to systematically investigate the cybersecurity threats faced by digital banking users in Kerala. A descriptive approach was employed to profile the users' awareness levels, security practices, and susceptibility to cyber threats, while the analytical component was intended to explore the relationships between these variables and demographic factors. The study focused specifically on individuals who actively engage in digital banking services, such as internet banking, mobile banking, and electronic wallet transactions. The choice of Kerala as the context was justified based on its high internet penetration, strong financial inclusion indices, and rapid adoption of digital technologies.

The population for the study comprised digital banking users residing in various districts of Kerala. A simple random sampling technique was employed to select the participants, ensuring that each member of the population had an equal chance of being included. The final sample size was 300 respondents, adequately representing different age groups, occupational sectors, and geographic regions (urban and rural areas). Care was taken to ensure demographic diversity so that the findings could provide a holistic understanding of cybersecurity behaviours across the state's digitally active population. The sample size was considered statistically appropriate for the scope of the study, allowing for meaningful generalization of results.

Primary data were collected using a structured questionnaire specifically developed for the study. The instrument contained 40 items distributed across key domains: cybersecurity awareness, security practices, susceptibility to cyber threats, and demographic information such as age, gender, educational background, and location. Each item was framed on a 5-point Likert scale, ranging from 1 (Strongly Disagree) to 5 (Strongly Agree). The maximum attainable score for each construct measured was 200, with each item contributing up to 5 points. This design enabled the researcher to capture a range of user perceptions and behaviours quantitatively, facilitating robust statistical analysis.

Data collection was carried out through a combination of online and offline modes to maximize reach and

representativeness. Online surveys were disseminated via email and social media platforms, while offline distribution was conducted through select bank branches across Kerala, with appropriate permissions. Participants were briefed about the purpose of the study, and ethical considerations were rigorously observed throughout the process. Informed consent was obtained from all respondents, assuring them of the confidentiality and anonymity of their responses. Participation was entirely voluntary, and respondents retained the right to withdraw at any stage without any repercussions.

For the analysis of collected data, the statistical software **EDUSTAT** was used. Descriptive statistical techniques, including means, standard deviations, and percentage analysis, were applied to summarize the data and interpret general trends. Pearson's product-moment correlation coefficient was utilized to test Hypothesis 1 (H_1), examining the relationship between users' cybersecurity awareness levels and their susceptibility to cyber threats. Independent samples t-tests were conducted to test Hypotheses 2 and 3 (H_2 and H_3), comparing the incidence of cyber incidents based on users' security practices and analysing the differences in susceptibility between elderly and younger users, respectively. Hypotheses were tested at appropriate significance levels (typically 0.05), and tenability was determined based on the outcomes of the statistical tests.

Data Analysis and Interpretation

Descriptive Analysis

To provide an initial overview of the data, descriptive statistics were computed for the main variables under study: cybersecurity awareness, security practices, and susceptibility to cyber threats. The descriptive analysis helped in understanding the overall distribution and central tendencies of the responses gathered from the 300 digital banking users sampled across Kerala. The results are presented in Table 1.

Variable	N	Maximum Score	Mean Score	Standard Deviation	Interpretation
Cybersecurity Awareness	300	200	157.2	22.8	Moderate to High
Security Practices	300	200	145.6	25.4	Moderate
Susceptibility to Cyber Threats	300	200	134.8	26.9	Moderate

The mean score for cybersecurity awareness was found to be 157.2 out of a maximum possible score of 200, with a standard deviation of 22.8, indicating that awareness levels among digital banking users in Kerala are generally moderate to high. In contrast, the mean score for security practices was lower, at 145.6, suggesting that despite reasonable levels of awareness, the actual implementation of security practices remains only moderate. The susceptibility to cyber threats recorded a mean score of 134.8, indicating that users perceive themselves as moderately vulnerable to cybersecurity risks. These findings highlight a potential gap between awareness and behavioural execution, an important aspect to address for enhancing cybersecurity resilience among users.

Hypotheses Testing

Following the descriptive analysis, inferential statistical techniques were applied to test the formulated hypotheses. Hypothesis testing was carried out at a 0.01 level of significance using Pearson's correlation and independent samples t-tests, as appropriate to the nature of the hypotheses.

Test of H_1

H_1: There is a significant relationship between users' awareness levels and their susceptibility to cyber

threats.

To test H_1, Pearson's product-moment correlation coefficient was calculated between cybersecurity awareness and susceptibility to cyber threats. The analysis yielded the following result:

- **Pearson's correlation coefficient (r) = -0.512, p < 0.01**

The negative correlation coefficient indicates that as cybersecurity awareness increases, susceptibility to cyber threats decreases. The relationship is statistically significant at the 0.01 level, implying that higher awareness levels are associated with lower vulnerability to cyber threats among digital banking users. This finding is consistent with existing literature emphasizing the protective role of cybersecurity awareness (Chakraborty & Mitra, 2021).

Conclusion:

Hypothesis H_1 is substantiated. A significant inverse relationship exists between cybersecurity awareness and susceptibility to cyber threats.

Test of H_2

H_2: Users who adopt stronger security measures experience fewer cyber incidents.

To test H_2, an independent samples t-test was conducted comparing the mean number of reported cyber incidents between users with high-security practices and users with low-security practices. The results are as follows:

- **Group 1 (High Security Practice Users) Mean Cyber Incidents Score = 2.4**
- **Group 2 (Low Security Practice Users) Mean Cyber Incidents Score = 4.9**
- **t(298) = -6.73, p < 0.01**

The significant negative t-value indicates that users who reported stronger adherence to security practices experienced significantly fewer cyber incidents compared to those with weaker security behaviours. The findings support the proposition that proactive adoption of cybersecurity measures, such as using two-factor authentication, setting complex passwords, and avoiding unsecured networks, effectively reduces the risk of falling victim to cyberattacks.

Conclusion:

Hypothesis H_2 is substantiated. Stronger security practices are associated with a lower incidence of cyber threats among digital banking users.

Test of H_3

H_3: Elderly users are more vulnerable to cyber threats compared to younger users.

To test H_3, an independent samples t-test was carried out comparing susceptibility scores between elderly users and younger users. The analysis produced the following results:

- **Elderly Users Mean Susceptibility Score = 148.5**
- **Younger Users Mean Susceptibility Score = 127.6**
- **t(298) = 5.28, p < 0.01**

The results reveal a statistically significant difference between the two groups, with elderly users exhibiting a notably higher mean susceptibility score. This suggests that elderly individuals are at greater risk of falling prey to cyber threats, possibly due to lower familiarity with digital banking interfaces, lesser exposure to cybersecurity training, and cognitive factors associated with aging. These findings are aligned with prior research emphasizing the need for targeted interventions for elderly users (Sundararajan, 2021).

Conclusion:

Hypothesis H_3 is substantiated. Elderly users are significantly more vulnerable to cyber threats compared to their younger counterparts.

Summary of Hypotheses Tenability

Hypothesis	Result
H_1: Significant relationship between awareness and susceptibility	Substantiated
H_2: Stronger security measures reduce cyber incidents	Substantiated
H_3: Elderly users are more vulnerable than younger users	Substantiated

The successful substantiation of all three hypotheses underscores the crucial roles of awareness, behaviour, and demographic factors in influencing cybersecurity risks within the digital banking sector in Kerala.

Discussion of the Results

The finding of a significant negative correlation between cybersecurity awareness and susceptibility to cyber threats corroborates the observations of Chakraborty and Mitra (2021), emphasizing that user awareness plays a vital role in mitigating digital risks. Individuals who possess a higher level of cybersecurity knowledge are more capable of identifying threats, practicing safe online behaviour, and avoiding common pitfalls such as phishing scams and fraudulent websites. In the context of Kerala's rapidly digitizing banking sector, this relationship holds particular significance, as it highlights a critical area where targeted interventions can yield substantial improvements in cybersecurity resilience. Educational programs focusing on digital safety, including workshops, online tutorials, and interactive awareness campaigns, could have a measurable impact on reducing user vulnerability. Strengthening user knowledge about cybersecurity protocols not only empowers individuals to protect their assets but also contributes to the overall robustness of the banking ecosystem.

In addition, the results demonstrate that users who proactively adopted stronger cybersecurity measures—such as enabling two-factor authentication, employing complex and regularly updated passwords, avoiding unsecured public networks, and staying vigilant against suspicious communications—reported significantly fewer cyber incidents. This finding echoes the conclusions drawn by Sundararajan (2021), affirming the critical role that proactive user behaviour plays in enhancing cybersecurity. It is not merely awareness but the consistent application of secure practices that serves as a strong defines against cyber threats. These results advocate for a paradigm shift in the design of cybersecurity interventions by banks: moving beyond passive awareness campaigns to implementing active, user-centric security training programs. For instance, banks could integrate cybersecurity modules into the digital onboarding processes, send regular security tip notifications through mobile apps, and provide incentives for users who adopt advanced security features. Such behaviourally informed strategies could significantly elevate the cybersecurity posture of digital banking users in Kerala.

The study also confirms that elderly users are disproportionately vulnerable to cyber threats compared to their younger counterparts, a finding that aligns with previous studies such as those by Mohan and Raj (2020). Elderly individuals, who often have lower digital literacy and reduced familiarity with evolving threat landscapes, are more susceptible to phishing attacks, online fraud, and identity theft. Cognitive decline associated with aging, combined with a lack of targeted cybersecurity education, further exacerbates their vulnerability. This necessitates the design and implementation of age-specific cybersecurity awareness initiatives tailored to the unique needs of older digital banking users. Banks and financial institutions should consider organizing specialized training sessions, simplifying digital interfaces, offering dedicated support lines for elderly users, and designing intuitive security systems that minimize the risk of accidental exposure to threats. Ensuring the digital safety of elderly users is not only an ethical imperative but also a critical component of promoting inclusive digital banking growth in Kerala.

Implications of the Study

The findings of this study have significant implications for banks and financial institutions seeking to strengthen cybersecurity defences within the digital banking ecosystem. One of the foremost priorities should be the design and implementation of comprehensive cybersecurity awareness programs. Rather than adopting a one-size-fits-all model, banks must tailor their educational materials to address the varying needs and capacities of different demographic groups. This includes using simple, jargon-free language, infographics, videos, and interactive modules that make cybersecurity concepts accessible to users of all literacy levels. Special attention must be paid to elderly users, who have been shown to be particularly vulnerable to cyber threats. Customized training sessions, helplines dedicated to cybersecurity queries, and periodic refresher programs can ensure that elderly customers remain well-informed and vigilant. By prioritizing demographic-specific awareness initiatives, financial institutions can empower all segments of the population to engage safely with digital banking platforms.

From a policy perspective, there is an urgent need for government and regulatory bodies in Kerala to institutionalize cybersecurity education as part of broader financial literacy campaigns. The state could introduce mandatory cybersecurity certification programs for individuals accessing digital banking services for the first time, thereby ensuring a basic level of cybersecurity competence across the user base. These certification programs could be delivered through online portals, mobile applications, or even in collaboration with banks during customer onboarding processes. Special provisions should be made to facilitate the participation of elderly users and rural populations, who may face challenges related to technology access and digital literacy. By making cybersecurity education a regulatory requirement, Kerala can enhance the overall resilience of its banking community, reduce the incidence of digital fraud, and build stronger user trust in digital financial systems.

Technology providers and banking application developers also have an important role to play in enhancing cybersecurity outcomes. The complexity of security features often acts as a deterrent to their adoption among average users. Therefore, simplifying security interfaces is critical. Features such as two-factor authentication, biometric verification, fraud alerts, and secure password management should be made intuitive, easy to configure, and seamlessly integrated into digital banking apps. Automatic prompts, visual guides, and user-friendly design principles can significantly improve security adoption rates. Furthermore, embedding cybersecurity tips within banking applications—delivered contextually as users perform transactions—can bridge the gap between awareness and action. By designing for security without sacrificing usability, technology providers can facilitate safer digital banking practices among diverse user groups, ultimately contributing to a more secure digital economy.

Conclusion

The rise of digital banking has brought undeniable benefits in terms of convenience, efficiency, and financial inclusion. However, it has also created new vulnerabilities, especially for users who are inadequately prepared to navigate the complex landscape of cyber threats. This study examined the relationship between cybersecurity awareness, security practices, and susceptibility to cyber threats among digital banking users in Kerala. The findings reveal that while awareness levels are moderate to high, there remains a critical gap between awareness and the actual adoption of safe security practices. Users who demonstrated higher cybersecurity awareness reported lower susceptibility to cyber threats, while those who proactively adopted stronger security measures experienced fewer incidents. Additionally, elderly users were found to be significantly more vulnerable compared to their younger counterparts. These results underscore the need for a holistic approach that combines technological advancement with targeted cybersecurity education and user behaviour modification strategies.

Going forward, banks, policymakers, and technology developers must collaborate to address the human

dimensions of cybersecurity in digital banking. Initiatives aimed at enhancing cybersecurity awareness must be customized to suit the needs of different demographic groups, particularly the elderly and first-time digital banking users. Policy interventions mandating cybersecurity training and certification can reinforce a culture of digital safety. Furthermore, simplifying security features within digital platforms can encourage broader adoption of safe practices among users. By prioritizing user empowerment alongside technological defences, stakeholders can create a resilient digital banking environment that supports sustainable growth, fosters user trust, and minimizes the risks associated with cyber threats. The insights derived from this study can serve as a foundation for designing more inclusive, user-cantered cybersecurity frameworks in the digital banking sector of Kerala and beyond.

References

Chakraborty, R., & Mitra, S. (2021). Cybersecurity threats and digital banking: An Indian perspective. *Journal of Financial Crime*, 28(2), 601-616.

Kaur, P., & Arora, S. (2020). Digital banking and cybersecurity: Challenges and future strategies. *International Journal of Management (IJM)*, 11(7), 1194-1204.

Mohan, R., & Raj, P. (2020). Impact of Digital India on the banking sector: An empirical study. *Journal of Banking and Finance*, 6(3), 45-52.

Nair, R., & Menon, S. (2022). Cybersecurity awareness and digital banking: A study among millennials in Kerala. *South Asian Journal of Business and Management Cases*, 11(1), 75-85.

Sharma, V., & Patel, M. (2021). Digital banking and cyber threats: An emerging issue. *Indian Journal of Finance*, 15(5), 33-45.

Sundararajan, V. (2021). Cybersecurity in banking: Challenges and strategies. *Global Business Review*, 22(4), 983-1002.

Chakraborty, R., & Mitra, S. (2021). Cybersecurity threats and digital banking: An Indian perspective. *Journal of Financial Crime*, 28(2), 601–616.

Gupta, A., & Sharma, P. (2020). Behavioural patterns and cybersecurity practices among Indian banking customers. *Journal of Internet Banking and Commerce*, 25(3), 1–15.

Kaur, P., & Arora, S. (2020). Digital banking and cybersecurity: Challenges and future strategies. *International Journal of Management (IJM)*, 11(7), 1194–1204.

Mohan, R., & Raj, P. (2020). Impact of Digital India on the banking sector: An empirical study. *Journal of Banking and Finance*, 6(3), 45–52.

Nair, R., & Menon, S. (2022). Cybersecurity awareness and digital banking: A study among millennials in Kerala. *South Asian Journal of Business and Management Cases*, 11(1), 75–85.

Patel, D., & Desai, M. (2019). Demographic differences in vulnerability to cybersecurity threats among digital banking users. *International Journal of Cyber Research and Education*, 4(2), 88–101.

Sharma, V., & Patel, M. (2021). Digital banking and cyber threats: An emerging issue. *Indian Journal of Finance*, 15(5), 33–45.

Sundararajan, V. (2021). Cybersecurity in banking: Challenges and strategies. *Global Business Review*, 22(4), 983–1002.

Agarwal, A., & Sengupta, S. (2021). Strengthening cybersecurity policies in Indian banking: Challenges and user behaviour implications. *Journal of Banking Security and Technology*, 12(2), 75–89.

Bansal, S., & Kaur, M. (2019). Psychological determinants of cybersecurity behaviour among digital banking users. *Indian Journal of Cyber Behaviour*, 5(1), 21–35.

Das, P., & Nayak, S. (2018). Impact of cybersecurity training on safe digital banking practices: Evidence from

metropolitan India. *International Journal of Information Security and Privacy*, 12(4), 65–78.
Iyer, R., & Sharma, K. (2020). Cybersecurity challenges in rural digital banking: An Indian perspective. *Asian Journal of Information Technology*, 19(6), 150–158.
Jain, R., & Aggarwal, S. (2019). Cybersecurity preparedness in public and private sector banks: A comparative study. *Journal of Financial Services and Management*, 8(2), 45–59.
Kavitha, R., & Devi, V. (2018). Elderly users and cybersecurity challenges in digital banking: A study in Southern India. *Journal of Gerontology and Digital Society*, 3(1), 11–25.
Menon, A., & Kumar, P. (2017). The role of trust and perceived security in digital banking adoption in India. *Indian Journal of Marketing*, 47(8), 42–53.
Thomas, A., & Mathew, J. (2020). Phishing and cybersecurity awareness in Indian digital banking: A behavioural analysis. *International Journal of Cyber Criminology*, 14(1), 137–151.
Kaur, P., & Arora, S. (2020). Digital banking and cybersecurity: Challenges and future strategies. *International Journal of Management (IJM)*, 11(7), 1194–1204.
Nair, R., & Menon, S. (2022). Cybersecurity awareness and digital banking: A study among millennials in Kerala. *South Asian Journal of Business and Management Cases*, 11(1), 75–85.
Sharma, V., & Patel, M. (2021). Digital banking and cyber threats: An emerging issue. *Indian Journal of Finance*, 15(5), 33–45.