International Journal of Research in Commerce and Management Studies

ISSN 2582-2292

Vol. 8, No. 03 May-June; 2026 Page. No. 614-621

To cite this article: Dr. Subramanya S.V. and Dr. Anil N (2026). CYBERSECURITY CHALLENGES IN DIGITAL BANKING: CUSTOMER AWARENESS AND RISK PERCEPTION, International Journal of Research in Commerce and Management Studies (IJRCMS) 8 (3): 614-621 Article No. 778 Sub Id 1298

CYBERSECURITY CHALLENGES IN DIGITAL BANKING: CUSTOMER AWARENESS AND RISK PERCEPTION

Dr. Subramanya S.V.[1] and Dr. Anil N.[2]

[1]Associate Professor, Department of Commerce, Government First Grade College, KR Puram, Bangalore – 560036, Karnataka, India.
[2]Associate Professor, Department of Commerce, Government College for Women, Kolar – 563101, Karnataka, India.

DOI: https://doi.org/10.38193/IJRCMS.2026.8340

ABSTRACT

The rapid digital transformation of the banking sector has significantly enhanced financial accessibility, efficiency, and convenience for customers. With the widespread adoption of internet banking, mobile banking, and digital payment systems, financial institutions have increasingly relied on technology-driven platforms to deliver services. However, this digital evolution has simultaneously exposed banking systems and users to a wide range of cybersecurity threats, including phishing attacks, malware intrusions, identity theft, ransomware, and data breaches. These threats not only compromise financial assets but also erode customer trust in digital banking ecosystems. This study focuses on examining the cybersecurity challenges in digital banking with particular emphasis on customer awareness and risk perception. Customer awareness refers to the level of knowledge and understanding users possess regarding safe digital banking practices, while risk perception relates to how customers interpret and respond to potential cybersecurity threats. The study is based on secondary data collected from recent scholarly articles, industry reports, and institutional publications from 2022 to 2025. The findings indicate that although digital banking adoption has grown rapidly, customer awareness regarding cybersecurity measures remains moderate and often inadequate. Many users lack practical knowledge of essential security practices such as strong password management, recognizing phishing attempts, and using multi-factor authentication. Furthermore, risk perception varies significantly among users, influencing their behavior and decision-making in digital financial transactions. A gap between perceived and actual risk levels has been observed, leading to either overconfidence or excessive fear among users. The study concludes that enhancing customer awareness and aligning risk perception with real-world threats are critical for improving cybersecurity resilience. It recommends that banks, policymakers, and financial institutions implement targeted awareness programs, strengthen technological safeguards, and promote digital literacy to ensure a secure and trustworthy digital banking environment.

KEYWORDS: Internet Banking, Digital payments, financial institutions

International Journal of Research in Commerce and Management Studies

ISSN 2582-2292

Vol. 8, No. 03 May-June; 2026 Page. No. 614-621

INTRODUCTION

The banking industry has undergone a profound transformation in recent years, driven by rapid advancements in digital technology. The emergence of digital banking platforms—including internet banking, mobile banking applications, and unified payment interfaces—has revolutionized the way financial services are delivered and consumed. Customers can now perform a wide range of banking activities, such as fund transfers, bill payments, account management, and investments, with unprecedented ease and convenience. This shift has been further accelerated by increasing smartphone penetration, internet accessibility, and government initiatives promoting digital financial inclusion.

Despite these advancements, the expansion of digital banking has introduced significant cybersecurity challenges. As financial transactions increasingly occur in virtual environments, cybercriminals have developed sophisticated methods to exploit system vulnerabilities and target unsuspecting users. Common threats such as phishing attacks, malware infections, identity theft, and unauthorized access to sensitive data have become prevalent, posing serious risks to both customers and financial institutions. The consequences of such cyberattacks extend beyond financial loss, affecting customer confidence, institutional reputation, and overall financial stability.

In this context, cybersecurity has emerged as a critical concern in the digital banking ecosystem. While financial institutions invest heavily in advanced security technologies, the human element remains one of the weakest links in cybersecurity. Customers often lack adequate awareness and understanding of potential threats and safe digital practices, making them vulnerable to cyber fraud. For instance, users may unknowingly share sensitive information, use weak passwords, or fail to recognize fraudulent communications, thereby increasing their exposure to cyber risks.

Customer awareness plays a pivotal role in mitigating cybersecurity threats. It encompasses knowledge of security features, understanding of potential risks, and the ability to adopt preventive measures. Alongside awareness, risk perception is another crucial factor influencing customer behavior. Risk perception refers to how individuals evaluate the likelihood and severity of cybersecurity threats and how this perception shapes their actions. A mismatch between actual risk and perceived risk can lead to either negligent behavior or excessive avoidance of digital banking services.

Understanding the interplay between cybersecurity challenges, customer awareness, and risk perception is essential for developing effective strategies to enhance digital banking security. While technological solutions are necessary, they must be complemented by user education and behavioral interventions. This study aims to explore these dimensions by analyzing existing literature and identifying key gaps in customer awareness and perception.

International Journal of Research in Commerce and Management Studies

ISSN 2582-2292

Vol. 8, No. 03 May-June; 2026 Page. No. 614-621

By focusing on these aspects, the study contributes to the growing body of research on digital banking security and provides practical insights for financial institutions, policymakers, and researchers. Strengthening cybersecurity awareness and improving risk perception among customers will not only reduce vulnerabilities but also foster greater trust and adoption of digital banking services in the long run.

OBJECTIVES OF THE STUDY

1. To identify major cybersecurity challenges in digital banking
2. To examine the level of customer awareness regarding cybersecurity practices
3. To analyze customer risk perception towards digital banking
4. To study the relationship between awareness and cybersecurity behavior

REVIEW OF LITERATURE

- A study (2025) found that many users lack awareness of basic cybersecurity practices such as secure password usage and fraud reporting, despite trusting banking systems.
- Research on digital banking users revealed that cybersecurity knowledge significantly influences user behavior, and awareness alone is not sufficient without proper knowledge.
- Another study highlighted that cybersecurity awareness positively impacts cyber fraud prevention, especially among younger users.
- Research conducted in Malaysia identified key factors influencing risk perception, including user behavior, mobile security, and perceived threats.
- A study in Chennai emphasized that customers are aware of some threats but lack deep understanding of security protocols, which affects safe usage of digital banking.
- Literature also shows that phishing, malware, and data breaches are the most common cybersecurity threats in digital banking environments.

RESEARCH METHODOLOGY

The present study adopts a descriptive research design to systematically examine cybersecurity challenges in digital banking, with a specific focus on customer awareness and risk perception. The research is entirely based on secondary data, which has been collected from a wide range of credible sources, including peer-reviewed journal articles, research papers, industry reports, and institutional publications. The data considered for the study primarily covers recent developments and findings

International Journal of Research in Commerce and Management Studies

ISSN 2582-2292

Vol. 8, No. 03 May-June; 2026 Page. No. 614-621

from the period 2022 to 2025, ensuring the relevance and timeliness of the analysis. To interpret and synthesize the collected information, the study employs content analysis and comparative analysis techniques. Content analysis is used to identify recurring themes, patterns, and key insights related to cybersecurity threats, awareness levels, and risk perceptions among customers, while comparative analysis facilitates the evaluation of findings across different studies to draw meaningful conclusions. This methodological approach enables a comprehensive understanding of the subject by integrating diverse perspectives and existing empirical evidence.

- **Major Cybersecurity Threats**

The analysis of secondary data reveals that digital banking systems are increasingly exposed to a variety of cybersecurity threats, primarily due to the rapid expansion of digital financial services.

Among these, **phishing attacks** are one of the most prevalent forms of cybercrime, where fraudsters impersonate legitimate banking institutions through emails, messages, or fake websites to deceive customers into revealing sensitive information such as login credentials and OTPs. Malware and ransomware attacks also pose significant risks, as malicious software can infiltrate users' devices, steal confidential data, or lock systems until a ransom is paid.

In addition, data breaches have become a major concern, involving unauthorized access to banking databases and leakage of sensitive customer information. Such breaches not only result in financial losses but also damage the reputation of financial institutions. Identity theft is another critical issue, where cybercriminals misuse personal and financial information to conduct fraudulent transactions. The findings indicate that the frequency and sophistication of these threats are increasing in parallel with the growth of digital banking, making cybersecurity a pressing concern for both customers and banks.

- **Customer Awareness Level**

The study finds that customer awareness regarding cybersecurity practices remains relatively low, despite the widespread use of digital banking platforms. Many users lack basic knowledge of essential security measures, such as creating strong and unique passwords, avoiding suspicious links, and regularly updating their banking applications. A significant proportion of customers are unaware of secure browsing practices, making them vulnerable to fraudulent websites and online scams.

Furthermore, the understanding and adoption of advanced security features, such as two-factor authentication (2FA) and biometric verification, are limited among users. Even when such features are available, customers often fail to utilize them effectively due to lack of awareness or perceived

International Journal of Research in Commerce and Management Studies

ISSN 2582-2292

Vol. 8, No. 03 May-June; 2026 Page. No. 614-621

inconvenience. The analysis highlights that insufficient awareness directly contributes to increased vulnerability, as users unknowingly engage in risky behaviors that expose them to cyberattacks. This gap in awareness underscores the need for continuous education and awareness initiatives by financial institutions.

- **Risk Perception**

Risk perception plays a crucial role in shaping customer attitudes and behavior towards digital banking. The findings indicate that customers generally perceive digital banking as highly convenient and efficient, but at the same time, they associate it with significant security risks. Many users express concerns about potential financial loss, unauthorized transactions, and misuse of personal data.

This perception often leads to cautious behavior, such as avoiding high-value transactions through digital platforms or limiting the use of certain services. In some cases, customers may even refrain from adopting digital banking altogether due to fear of cyber threats. However, the study also reveals inconsistencies in risk perception, where some users underestimate the actual risks and engage in unsafe practices, while others overestimate risks and avoid beneficial digital services. This imbalance highlights the importance of aligning customer perception with real-world cybersecurity threats through proper awareness and education.

Relationship Between Awareness and Behavior

- The analysis demonstrates a strong relationship between customer awareness and cybersecurity behavior. Higher levels of awareness are associated with safer banking practices, such as using strong passwords, enabling security features, and verifying the authenticity of online communications. Customers who possess adequate knowledge about cybersecurity are more likely to identify potential threats and take preventive measures, thereby reducing their risk of falling victim to cyber fraud.
- Moreover, the findings suggest that knowledge has a more significant impact than awareness alone. While awareness refers to general familiarity with cybersecurity concepts, knowledge involves a deeper understanding and practical application of security measures. Educated and informed users tend to exhibit more responsible behavior and are less susceptible to phishing attacks, scams, and other cyber threats. This indicates that effective cybersecurity strategies should focus not only on raising awareness but also on enhancing users' practical knowledge and skills.

FINDINGS

- The analysis of secondary data highlights several important findings regarding cybersecurity challenges in digital banking. Firstly, it is evident that cybersecurity threats are increasing in

International Journal of Research in Commerce and Management Studies

ISSN 2582-2292

Vol. 8, No. 03 May-June; 2026 Page. No. 614-621

direct proportion to the rapid growth and widespread adoption of digital banking services. As more customers rely on online and mobile banking platforms for their financial transactions, cybercriminals are simultaneously developing more sophisticated techniques to exploit system vulnerabilities. This has led to a significant rise in incidents such as phishing, malware attacks, data breaches, and identity theft, making cybersecurity a critical concern in the digital financial ecosystem.

- Secondly, the study reveals that customer awareness regarding cybersecurity practices is moderate but not sufficient to effectively mitigate risks. While many users possess a basic understanding of digital banking security, they often lack comprehensive knowledge of essential protective measures. This partial awareness results in inconsistent security behavior, where users may follow certain precautions but ignore others, thereby increasing their exposure to cyber threats.

- Another key finding is that risk perception plays a significant role in influencing customer usage behavior. Customers who perceive digital banking as highly risky tend to limit their usage, particularly for high-value transactions, whereas those with lower perceived risk may engage more freely but sometimes neglect necessary security precautions. This variation in perception affects not only the adoption of digital banking services but also the level of caution exercised by users during transactions.

- Furthermore, the study identifies lack of knowledge as a major cause of cyber vulnerability. Awareness alone is not enough; users require a deeper understanding of cybersecurity practices and the ability to apply them in real-life situations. Many cyber fraud cases occur because users are unable to recognize fraudulent activities or respond appropriately, highlighting the gap between awareness and practical knowledge.

- Finally, the findings emphasize that awareness programs and educational initiatives significantly contribute to improving customer trust and reducing cybersecurity risks. When customers are provided with clear guidance, training, and timely information about potential threats, they are more likely to adopt safe banking practices. This not only enhances their confidence in using digital banking services but also strengthens the overall security framework of the financial system.

SUGGESTIONS

1. **Customer Education Programs**
   Banks should conduct regular awareness campaigns on cybersecurity practices

International Journal of Research in Commerce and Management Studies

ISSN 2582-2292

Vol. 8, No. 03 May-June; 2026 Page. No. 614-621

2. **Implementation of Advanced Security Measures**
    - Multi-factor authentication
    - Biometric verification
    - Encryption technologies
3. **User-Friendly Security Guidelines**
   Simplified instructions for customers on safe digital banking usage
4. **Regular Alerts and Notifications**
   Inform customers about new cyber threats and fraud techniques
5. **Government and Regulatory Support**
   Strong policies and awareness initiatives by central banks and regulators
6. **Digital Literacy Programs**
   Focus on rural and less-educated users to improve awareness

CONCLUSION

Cybersecurity is a critical challenge in digital banking, and customer awareness plays a significant role in mitigating risks. While digital banking offers numerous benefits, inadequate awareness and poor risk perception expose users to cyber threats. The study highlights that improving customer knowledge and awareness can significantly enhance cybersecurity behavior and trust in digital banking systems. Financial institutions must adopt proactive strategies to educate users and strengthen security measures to ensure a safe digital banking environment.

REFERENCES

1. Shukla, K. et al. (2025). *Assessing Customer's Awareness of Cybersecurity Measures in Online Banking*.
2. Sankararaman, G. & Suresh, S. (2025). *Customer Awareness on Security Issues in Digital Banking*.
3. Nagari, S. & Raharja, S. (2024). *Cybersecurity Awareness, Knowledge and Behavior of Digital Banking Users*.
4. Novianti, I. & Chariri, A. (2025). *Cybersecurity Awareness and Fraud Prevention*.
5. Mohidin, R. et al. (2025). *Cybersecurity Risk Awareness in Mobile Banking*.
6. *Cyber Security Threats in Digital Banking in India*.

International Journal of Research in Commerce and Management Studies

ISSN 2582-2292

Vol. 8, No. 03 May-June; 2026 Page. No. 614-621

7. Akter, S. et al. (2022). *Cybersecurity Awareness Capability in Digital Economy*