ISSN (ELECTRONIC): 2945-3135

Krishna C P (2026). *A Study on Cyber Crimes in Digital Banking. International Journal of Multidisciplinary Research & Reviews, 5(si2), 191-199.*

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH & REVIEWS

journal homepage: www.ijmrr.online/index.php/home

A STUDY ON CYBER CRIMES IN DIGITAL BANKING

Dr. Krishna C.P

Associate Professor, Government Womens College, Maddur – 571428, Karnataka, India.

Corresponding Author: krishnacp.krish5@gmail.com

How to Cite the Article: Krishna C P (2026). *A Study on Cyber Crimes in Digital Banking. International Journal of Multidisciplinary Research & Reviews, 5(si2), 191-199.*

https://doi.org/10.56815/ijmrr.v5si2.2026.191-199

Keywords	***Abstract***
Cybercrimes, Digital Banking, Phishing Attacks, Online Fraud, Encryption, Data Breaches.	This study investigates the prevalence, nature, and impact of cyber crimes in digital banking, highlighting the growing challenges faced by financial institutions and users in the digital era. With the increasing adoption of internet and mobile banking services, cyber threats such as phishing, malware attacks, SIM swapping, and account takeovers have become more sophisticated and frequent. Using an empirical approach, primary data was collected through surveys involving 150 respondents, including bank customers and professionals. The findings reveal a concerning lack of awareness among users and inadequate preparedness among banks, leading to significant financial and reputational losses. Key contributing factors include weak security practices, user negligence, and evolving tactics of cyber criminals. The study underscores the importance of multi-layered cybersecurity frameworks, regular audits, user education programs, and stronger legal and regulatory mechanisms. It concludes that collaborative efforts among stakeholders are essential to enhance resilience against cyber threats in the rapidly expanding digital banking ecosystem.

1. INTRODUCTION

The rise of digital banking has revolutionized the financial services industry by offering convenience, speed, and accessibility to millions of users worldwide. Services such as internet banking, mobile banking apps, electronic fund transfers, and digital wallets have minimized the need for physical banking, especially in a post-pandemic world. However, this digital shift has also made the banking sector increasingly vulnerable to cyber-crimes. As financial transactions become more

Krishna C P (2026). *A Study on Cyber Crimes in Digital Banking. International Journal of Multidisciplinary Research & Reviews, 5(si2), 191-199.*

digitized, cyber criminals continue to develop sophisticated methods to exploit system vulnerabilities, deceive users, and steal sensitive data.

As of 2025, cyber-crimes in digital banking have escalated significantly in India, posing a serious threat to the financial sector and its users. In the fiscal year 2024, high-value cyber fraud cases increased more than fourfold, resulting in losses exceeding ₹2,000 crore (approximately $240 million). The surge in incidents is attributed to the rapid adoption of digital payment platforms like UPI and internet banking, which have become prime targets for cybercriminals. Fraudsters employ sophisticated techniques, including AI-driven scams, deepfake technology, and social engineering tactics, to deceive individuals and institutions.

Cyber-crimes in digital banking take many forms, including phishing attacks, malware infections, SIM card swapping, data breaches, and unauthorized access to bank accounts. These crimes not only cause financial losses to individual customers and institutions but also undermine public trust in digital banking systems. According to the Reserve Bank of India (2023), there has been a noticeable surge in reported banking fraud cases linked to cyber-attacks, which indicates that existing security mechanisms may not be sufficient to counter evolving threats.

This study aims to examine the types and frequency of cyber-crimes in digital banking, assess user awareness, and evaluate the effectiveness of current preventive measures. By analyzing survey data collected from both bank customers and professionals, the study provides empirical insights into the real-world impact of cyber-crimes. It also offers recommendations for enhancing cybersecurity infrastructure and improving user education to reduce digital banking risks.

2. BRIEF EXAMPLES OF CYBERCRIMES IN DIGITAL BANKING

1. Phishing Attacks: Fraudulent emails or messages trick customers into revealing login credentials or personal information.
2. Account Takeover: Cybercriminals gain unauthorized access to bank accounts to steal money or change settings.
3. Man-in-the-Middle Attacks: Hackers intercept and alter communications between customers and banks to steal sensitive data.
4. Ransomware: Malicious software locks bank data or customer access, demanding payment for restoration.
5. Card Skimming and Cloning: Skimming devices on ATMs steal card information, which is then used to clone cards and make fraudulent purchases.
6. SIM Card Swapping: Attackers hijack a victim's phone number to bypass two-factor authentication and gain access to bank accounts.
7. Malware and Trojans: Malicious programs capture sensitive data like banking credentials through infected devices.
8. Insider Threats: Employees misuse their access to steal or leak sensitive banking information.
9. DDoS Attacks: Attackers overwhelm bank websites or apps with traffic, disrupting access to services.
10. Fake Banking Apps: Fraudulent apps that resemble legitimate banking apps steal user data once downloaded.

Krishna C P (2026). *A Study on Cyber Crimes in Digital Banking. International Journal of Multidisciplinary Research & Reviews, 5(si2), 191-199.*

3. REVIEW OF LITERATURE

Each summarizing key findings related to cyber-crimes in digital banking:

1. **Kumar, A., & Singh, P. (2020)**
   Kumar and Singh explored the evolution of cyber threats in Indian banking and emphasized that phishing and malware remain the most persistent forms of cyber-attacks. The study recommended enhancing digital infrastructure and continuous monitoring systems.
2. **Rani, A., & Kapoor, R. (2021)**
   This paper identified that most users lacked awareness about SIM swapping and credential theft. It stressed the need for customer education programs as a core part of cyber defense strategies.
3. **Sharma, N. (2022)**
   Sharma examined RBI's cybersecurity guidelines and their implementation among Indian banks. The research found inconsistencies in adoption levels, especially among rural banks.
4. **Das, S., & Mehta, R. (2020)**
   The authors analysed common attack vectors in online banking, concluding that most breaches occur due to weak password management and insecure endpoints.
5. **Patel, D. (2019)**
   This study focused on phishing schemes and how social engineering tactics manipulate customers into revealing sensitive information.
6. **Reserve Bank of India. (2023)**
   The RBI's annual cybersecurity report highlighted a 24% increase in cyber fraud cases over the previous year and outlined policy recommendations for banks.
7. **Tiwari, M., & Jain, S. (2021)**
   Their study examined the effectiveness of biometric authentication and found it significantly reduced unauthorized access in mobile banking.
8. **World Bank. (2022)**
   The World Bank reported that developing nations face increased cyber risks due to underinvestment in cybersecurity and lack of skilled personnel.
9. **Gupta, R. (2020)**
   Gupta's study revealed that insider threats, such as employee negligence or data leaks, contribute to nearly 20% of cyber incidents in banks.
10. **CERT-In. (2022)**
    India's national cybersecurity agency emphasized the importance of reporting and response mechanisms, showing that delayed responses exacerbate damage in most incidents.
11. **KROLL (2025)**

According to a recent survey 96% of senior executives in India anticipate a rise in cybercrime risks in 2025, with AI-driven attacks being the primary concern (Kroll, 2025). However, only 36% of these executives believe that their organizations' compliance programs are adequately

Krishna C P (2026). *A Study on Cyber Crimes in Digital Banking. International Journal of Multidisciplinary Research & Reviews, 5(si2), 191-199.*

prepared to address these risks. This gap highlights the challenges financial institutions face in translating regulatory expectations into effective security practices.

4. RESEARCH METHODOLOGY

Research Design

The study adopts a quantitative and descriptive research design. Quantitative data collection and analysis methods were employed to explore the prevalence and perception of cyber-crimes in digital banking. Descriptive analysis helps summarize patterns in the data and identify key cyber threats encountered by respondents.

Sample Size and Respondent Profile

A total of 150 respondents participated in this study:

- 100 bank customers, representing individual users of digital banking platforms.
- 50 banking professionals, including IT staff, cybersecurity experts, and branch managers from both public and private sector banks.

Data Collection Method

Data was gathered through a structured questionnaire, distributed both online (via Google Forms) and offline (printed surveys). The questionnaire included:

- Multiple-choice questions on awareness and experience with cyber-crimes,
- Likert scale questions on security perception,
- Open-ended responses for qualitative insights.

Tools Used

- SPSS v25: Used for coding, statistical analysis, and generation of frequency tables and charts.
- MS Excel: Used for graphical representation and chart formatting.

5. DATA ANALYSIS AND INTERPRETATION

Table 1; Demographic Profile of Respondents

Demographic Factor	Category	Frequency	Percentage
Age	18–30	60	40%
	31–45	50	33.3%
	46 and above	40	26.7%
Gender	Male	90	60%
	Female	60	40%
Profession	Bank Customer	100	66.7%
	Bank Professional	50	33.3%

Krishna C P (2026). *A Study on Cyber Crimes in Digital Banking. International Journal of Multidisciplinary Research & Reviews, 5(si2), 191-199.*

Interpretation: The sample is balanced across age groups and gender, ensuring diverse insights. A majority are bank customers, making the findings relevant to end-user experience.

Table 2: Types of Cyber Crimes Experienced by Respondents

Cyber Crime Type	Frequency	Percentage
Phishing	68	45.3%
Malware	40	26.7%
SIM Swapping	20	13.3%
Account Takeover	12	8%
Others	10	6.7%
Total	150	100%

Interpretation: Phishing is the most common cyber-crime experienced, indicating the need for email and web filtering solutions. SIM Swapping is less common but dangerous due to its potential for account access.

Table 3: User Awareness on Cyber Threats

Awareness Indicator	Yes (%)	No (%)
Know about phishing	80%	20%
Aware of SIM swapping	28%	72%
Use strong and unique passwords	40%	60%
Enable multi-factor authentication (MFA)	34%	66%

Interpretation: Awareness of phishing is relatively high, but SIM swapping and MFA are poorly understood, highlighting critical gaps in user education.

Table 4: Financial Losses Due to Cyber Crimes

Financial Loss (in ₹)	Respondents	Percentage
None	108	72%
< ₹5,000	25	16.7%
₹5,000–₹10,000	10	6.7%
> ₹10,000	7	4.6%
Total	100	100%

Krishna C P (2026). *A Study on Cyber Crimes in Digital Banking. International Journal of Multidisciplinary Research & Reviews, 5(si2), 191-199.*

Interpretation: Although the majority of users have not experienced financial loss, 16.7% reported small-scale losses, and over 10% reported losses above ₹5,000, emphasizing the economic impact of these crimes.

Table 5: Security Measures Practiced by Respondents

Security Practice	Practiced (%)	Not Practiced (%)
Regular password updates	35%	65%
Avoiding public Wi-Fi	40%	60%
Using antivirus software	52%	48%
Enabling mobile app lock	58%	42%

Interpretation: The results show low engagement with basic security practices, suggesting a need for awareness campaigns and user training.

6. SUMMARY OF ANALYSIS

- There is a moderate level of awareness but poor security practice adoption among customers.
- Phishing and malware are the most prevalent threats.
- A significant portion of users suffered financial loss, despite the availability of protective tools.
- The use of multi-factor authentication and password hygiene remains low.

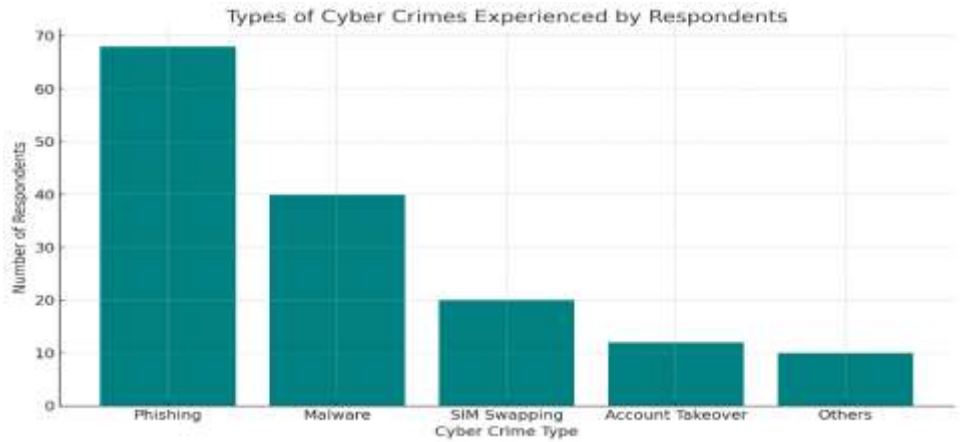

Chart -1: Types of Cyber Crimes experienced by Respondents

Krishna C P (2026). *A Study on Cyber Crimes in Digital Banking. International Journal of Multidisciplinary Research & Reviews, 5(si2), 191-199.*

Interpretation: Majority of respondents opined that Phishing attack is the major threat in digital banking.

7. PREVENTIVE MEASURES AND CYBERSECURITY PRACTICES

Cyber-crimes in digital banking can be significantly reduced through a combination of proactive strategies by both banks and users. The following section highlights specific measures adopted by banks and recommended practices for users to enhance digital security.

- **By Banks**

a) Implementation of AI-Based Fraud Detection

Modern banks are increasingly relying on Artificial Intelligence (AI) to detect and prevent fraudulent transactions in real-time. AI algorithms monitor customer behavior, transaction patterns, and login histories to flag suspicious activities. For example, if a transaction is initiated from a new device or foreign location, the AI system can instantly alert the user or temporarily block the activity. These systems evolve over time using machine learning, making them more efficient at identifying new threats.

b) Periodic System Audits

Banks conduct regular IT and cybersecurity audits to identify vulnerabilities in their infrastructure. These audits, often mandated by the Reserve Bank of India (RBI) and internal compliance teams, ensure that outdated systems are upgraded, firewall protections are effective, and data encryption mechanisms are up to date. Audits also test disaster recovery and incident response plans, ensuring banks can respond quickly to breaches.

- **By Users**

a) Multi-Factor Authentication (MFA)

Users are advised to enable Multi-Factor Authentication for their online banking apps and websites. MFA typically involves a second form of verification—such as a one-time password (OTP), biometrics, or authentication app—along with the password. This significantly reduces the risk of account takeovers, even if the primary password is compromised through phishing or data leaks.

b) Avoiding Public Wi-Fi for Transactions

Public Wi-Fi networks are often unsecured and can be exploited by hackers to intercept sensitive banking data. Users should avoid conducting financial transactions over public or open networks, such as those in cafes, airports, or hotels. Instead, they should use secure, private internet connections or a Virtual Private Network (VPN) if absolutely necessary.

The collective implementation of these practices can create a secure environment for digital banking. While banks must invest in advanced technology and compliance, users need to adopt secure behaviors and remain alert to potential threats. Only a joint effort can ensure resilience against the evolving landscape of cyber-crimes.

Krishna C P (2026). *A Study on Cyber Crimes in Digital Banking. International Journal of Multidisciplinary Research & Reviews, 5(si2), 191-199.*

8. CONCLUSION

This study on cyber-crimes in digital banking sheds light on the evolving nature of cyber threats and the substantial challenges that both individual users and banking institutions face in safeguarding digital platforms. The research, which involved 150 respondents—comprising 100 bank customers and 50 banking professionals—reveals a broad understanding of the increasing frequency and sophistication of cyber-attacks, including phishing, data breaches, and malware infiltration. Among the customer group, there was a noticeable concern regarding the security of personal data and digital transactions, with many respondents expressing a sense of vulnerability in navigating online banking platforms. Despite the implementation of security measures such as two-factor authentication and encryption by banks, many customers remain unaware of the potential threats or lack the necessary skills to protect themselves from cyber-crimes. This discrepancy in awareness highlights a significant gap that needs to be addressed to strengthen the overall defense against cybercrime in the digital banking environment.

India is making concerted efforts to bolster cybersecurity in digital banking, the rapid evolution of cyber threats necessitates continuous vigilance, robust regulatory frameworks, and widespread consumer education to safeguard the integrity of the financial ecosystem.

This study suggests that a comprehensive approach involving increased customer education, enhanced security infrastructure, and robust regulatory frameworks will be critical in reducing cybercrime risks and fostering a secure digital banking environment.

9. AUTHOR(S) CONTRIBUTION

The writers affirm that they have no connections to, or engagement with, any group or body
That provides financial or non-financial assistance for the topics or resources covered in this
Manuscript.

10. CONFLICTS OF INTEREST

The authors declared no potential conflicts of interest with respect to the research, authorship,
And/or publication of this article.

11. PLAGIARISM POLICY

All authors declare that any kind of violation of plagiarism, copyright and ethical matters will
Take care by all authors. Journal and editors are not liable for aforesaid matters.

12. SOURCES OF FUNDING

The authors received no financial aid to support for the research.

REFERENCES

[1] Kumar, A., & Singh, P. (2020). Cybersecurity challenges in Indian digital banking. International Journal of Information Technology, 12(3), 231–238.

Krishna C P (2026). *A Study on Cyber Crimes in Digital Banking. International Journal of Multidisciplinary Research & Reviews, 5(si2), 191-199.*

[2] Rani, A., & Kapoor, R. (2021). User awareness and vulnerabilities in digital banking. Journal of Cyber Security Studies, 9(1), 45–57.

[3] Sharma, N. (2022). Implementation of RBI cybersecurity norms: A comparative study. Indian Journal of Banking and Finance, 18(2), 101–114.

[4] Das, S., & Mehta, R. (2020). Attack vectors in digital financial systems. Cyber Defense Review, 7(3), 65–78.

[5] Patel, D. (2019). Phishing and social engineering in digital banking. Journal of Information Security Research, 5(4), 33–41.

[6] Reserve Bank of India. (2023). Annual report on cybersecurity in financial services. Mumbai: RBI Press.

[7] Tiwari, M., & Jain, S. (2021). Enhancing digital banking security through biometrics. Journal of Digital Finance, 6(2), 92–102.

[8] World Bank. (2022). Cybersecurity in emerging economies: Challenges and policy recommendations. Washington, D.C.: World Bank Group.

[9] Gupta, R. (2020). Insider threats in the banking sector: A cyber risk perspective. Asian Journal of Banking and Law, 4(1), 25–37.

[10] CERT-In. (2022). Annual threat report on cyber incidents in India. New Delhi: Ministry of Electronics and Information Technology.

[11] Kroll. (2025). Cybercrime and the future of financial crime risks in India: A survey report. Kroll Group.