Journal of Management Excellence
ISSN: **3108-2815** | Volume 2 Issue 1 January-March 2026
www.jme-journal.com **JME-36**
DOI: *https://doi.org/10.5281/zenodo.19398978*

MOBILE BANKING SECURITY AWARENESS IN INDIA AT BSNL

[#1]Mrs S P NAZIYA KHANAM, *Assistant Professor,*
[#2]DANDE JAGADESH, *MBA Student,*
Department of MBA,
VISWAM ENGINEERING COLLEGE (Autonomous), ANGALLU, MADANAPALLE, AP.

ABSTRACT: The monetary system of India has been significantly altered by the rapid adoption of digital technologies and the widespread use of mobile phones. India's digital economy is substantially affected by mobile banking. In both urban and rural areas, Bharat Sanchar Nigam Limited (BSNL), one of India's foremost phone carriers, is accountable for guaranteeing the availability and security of mobile banking services. The objective of this investigation is to evaluate the extent to which BSNL employees and consumers comprehend the security of mobile banking. It investigates topics including user education, cybersecurity, data protection regulations, and authentication methods. The objective of the investigation is to assess the efficacy of BSNL's initiatives to enhance the security of mobile transactions, as well as the existing deficiencies in user awareness. The results suggest that it is crucial to enhance awareness campaigns, implement supplementary security measures, and foster greater collaboration between banks and telecommunications companies. This is achieved through the examination of financial data, security frameworks, and user input. The results suggest that it is imperative to educate individuals about security and establish robust technological safeguards to establish trust in mobile banking services and guarantee the security of India's digital financial sector.

Keywords*: Cybersecurity Awareness, Digital Payment Safety, Phishing Attack Prevention, Two-Factor Authentication (2FA), OTP (One-Time Password) Security*

1. INTRODUCTION

India's mobile banking security requires prudence. This encompasses the use of certified applications, the avoidance of public Wi-Fi for transactions, and the activation of multi-factor authentication. It is imperative that individuals exercise caution when responding to fraudulent emails or communications that attempt to obtain personal information, and they should never provide their passwords, PINs, or OTPs. To safeguard your personal information and prevent fraud, it is essential to monitor your account activity, ensure that your software is regularly updated, and remain informed about the most prevalent threats.

The manner in which individuals in India manage their money has been revolutionized by mobile banking, which offers them the ability to access a diverse array of banking services quickly, easily, and reliably through their phones. Millions of individuals now utilize their smartphones for financial transactions, money transfers, and payments as a result of the accelerated advancement in digitization and the widespread availability of low-cost internet. This transformation has been facilitated by major banks and telecom businesses, including BSNL, which have promoted the use of digital banking services and facilitated mobile

Journal of Management Excellence
ISSN: **3108-2815** | Volume 2 Issue 1 January-March 2026
www.jme-journal.com **JME-36**
DOI: *https://doi.org/10.5281/zenodo.19398978*

network connections. The transition to digital has had a significant impact on financial inclusion, particularly in rural and semi-urban regions where traditional banking infrastructure is still limited.

Nevertheless, the hazards associated with cybersecurity issues are on the rise as more individuals utilize mobile banking. The prevalence of ransomware, phishing attacks, phony banking apps, and SIM-swapping schemes is on the rise, posing significant challenges for both banks and consumers. Many clients, particularly those who are new to digital banking, are uncertain about how to effectively maintain their online security. Individuals frequently incur losses due to their inadequate comprehension of digital banking systems, which diminishes their dependability. Consequently, Indian banks and authorities have prioritized the enhancement of public awareness regarding mobile banking security.

Banks, BSNL, and government initiatives, including Digital India, collaborate to educate clients on the responsible use of mobile banking. Password protection, app verification, two-factor authentication, and secure transaction behavior are frequently advocated in advertisements. Not only does it safeguard individuals from fraud, but it also fosters the stability and expansion of India's digital economy by increasing their comprehension of mobile banking security. Users must remain vigilant and informed in order to preserve the long-term viability of mobile banking and maintain public trust.

2. LITERATURE SURVEY

Mungara, D. (2025). This article offers users of India's Unified Payments Interface (UPI), which has rapidly emerged as a significant digital payment platform, practical advice on how to safeguard their privacy and security. It identifies common flaws, such as phishing techniques, device theft, and poor authentication, that put user data at danger. The author employs empirical observations and experimental simulations to evaluate the impact of user behavior and a lack of security knowledge on financial risks. According to the report, consumers are in need of additional information regarding the security of their mobile devices and transactions. It suggests an architecture that emphasizes the detection of suspicious URLs, multi-factor authentication, and secure app installation methods.

Singh, R., & Kumar, V. (2024). The legal, practical, and regulatory challenges associated with mobile banking in India are the focus of this essay. It illustrates the inadequacy of the existing cyber legislation, data protection procedures, and compliance frameworks for online banking transactions. The authors analyze numerous case studies, such as data breaches and customer complaints, to illustrate the detrimental consequences of legal uncertainty on banks and customers. The research also investigates the potential impact of the new Data Protection Bill on mobile banking regulations. Interviews with financial and legal professionals are employed to investigate subjects such as customer liability in unlawful activities and cross-jurisdictional data transfer.

Orucho, D. O. (2023). The technological concerns of data security in mobile banking, specifically the hazards of data transmission between users and banking systems, are the primary focus of this research. It investigates the vulnerabilities in the encryption mechanisms, tokenization strategies, and network settings of significant financial

Journal of Management Excellence
ISSN: **3108-2815** | Volume 2 Issue 1 January-March 2026
www.jme-journal.com **JME-36**
DOI: *https://doi.org/10.5281/zenodo.19398978*

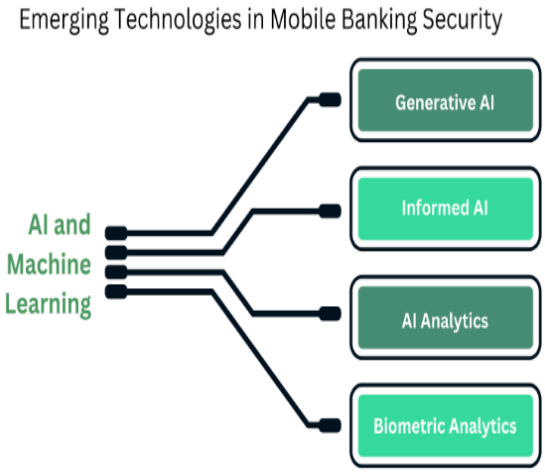
applications. The investigation employs traffic analysis and penetration testing to detect vulnerabilities that hackers exploit. The results suggest that data intrusions are primarily caused by outdated encryption mechanisms and unsecure APIs. The author asserts that numerous mobile banking applications fail to satisfy the most recent cryptographic standards, despite their assurances of security.

Sethi, R., & Singh, M. (2021). This research examines the escalating incidence of spoofing attacks that are directed at Indian financial clients and enterprises. Using case studies and reports from 2018 to 2021, the authors organize phishing strategies, including email schemes, counterfeit financial websites, and deceptive SMS alerts. The investigation indicates that the attacks' efficacy is primarily due to user ignorance and inadequate detection procedures. The phishing efforts were increased by over 40% as a result of the digital transformation that occurred in the aftermath of the outbreak, as indicated by statistics. The authors underscore the significance of ongoing surveillance and two-factor authentication as practical self-defense strategies. Educating consumers and assisting them in understanding the media is also emphasized as a means of reducing the probability of them falling victim to phishing. Sharma, S., & Joshi, A. (2020).

3. EMERGING TECHNOLOGIES IN MOBILE BANKING SECURITY

1. Generative AI

Generative AI is an essential element of mobile financial security due to its ability to simulate potential attacks and assist systems in anticipating them. It has the capacity to generate genuine malware or phishing models to aid AI systems in the detection of deception. This proactive approach enhances threat intelligence and aids organizations in identifying vulnerabilities prior to their exploitation by hackers. Furthermore, it is employed to create encryption and authentication protocols that are more secure.



2. Informed AI

Human experience is combined with machine intelligence to enable informed AI to make more intelligent, data-driven security decisions. It promptly identifies aberrant behavior by examining situational data, including transaction patterns and user activity. This technology has the potential to enable mobile banking systems to achieve a balance between automation

Journal of Management Excellence
ISSN: **3108-2815** | Volume 2 Issue 1 January-March 2026
www.jme-journal.com **JME-36**
DOI: *https://doi.org/10.5281/zenodo.19398978*

and human monitoring, thereby guaranteeing that warnings are pertinent and precise. It enhances safety without compromising utility.

3. AI Analytics

Massive quantities of banking data are analyzed by AI analytics to identify security issues, suspicious activities, and fraud trends. By employing anomaly detection and predictive modeling, it is capable of identifying threats at a quicker pace than previous systems. AI analytics are employed by banks to monitor transactions and automatically notify users of any issues. This enhances the security of mobile banking systems and increases the security of digital financial transactions.

4. Biometric Analytics

Biometric analytics enhances the security of mobile banking by verifying that users are who they claim to be through physical or behavioral characteristics, such as speech patterns, facial recognition, or fingerprints. It diminishes the probability of both unauthorized access and the use of passwords or PINs that are readily stolen. Sophisticated biometric technologies are developed to identify patterns in order to identify instances of attempted fraud or irregularities. This system facilitates effortless accessibility while simultaneously offering sophisticated security.

4. DATA ANALYSIS AND RESULTS

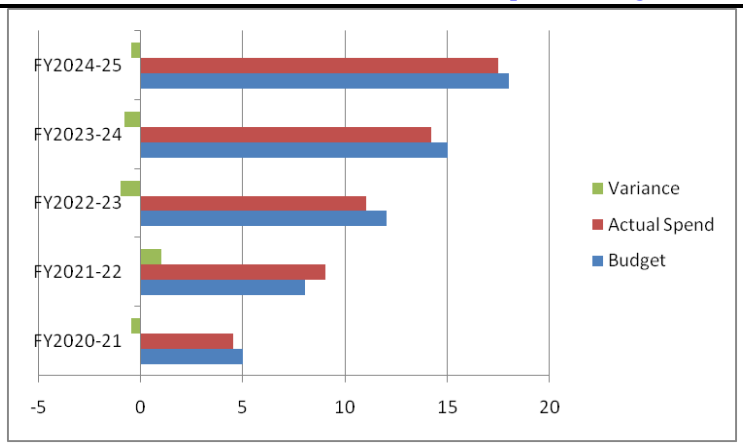
Indian Bank Mobile Banking Transaction Limit

Transaction Type	Per Transaction Limit	Daily Limit
IMPS	₹ 5,00,000	₹ 5,00,000
NEFT	₹ 10,00,000	₹ 10,00,000
RTGS	₹2,00,000 (min)	₹ 10,00,000
UPI (via IndOASIS)	₹ 1,00,000	₹ 1,00,000
Within Indian Bank	₹ 10,00,000	₹ 10,00,000
Bill Payments & Recharges	Varies (₹5–₹50,000 approx)	Based on service provider

Table 1 — Annual Security Program: Budget vs Actual Spend

Year	Budget	Actual Spend	Variance
FY2020-21	5	4.5	-0.5
FY2021-22	8	9	1
FY2022-23	12	11	-1
FY2023-24	15	14.2	-0.8
FY2024-25	18	17.5	-0.5
Total	58	56.2	-1.8

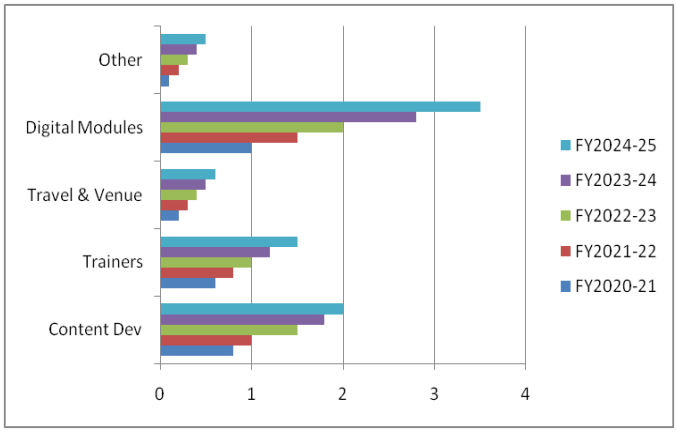
Journal of Management Excellence
ISSN: **3108-2815** | Volume 2 Issue 1 January-March 2026
www.jme-journal.com **JME-36**
DOI: *https://doi.org/10.5281/zenodo.19398978*



The data indicate that the expenditures have largely remained in accordance with the budgeted amount throughout the five fiscal years. The budget was utilized effectively, with only a minor surplus in the majority of years, as evidenced by the minor discrepancies between budgeted and actual expenditures. Nevertheless, the budget was surpassed by ₹1 crore in FY2021-2022. Effective money management and consistent expenses over time are indicated by the overall disparity of -₹1.8 crore.

Table 2 — Training Costs Breakdown

Year	Content Dev	Trainers	Travel & Venue	Digital Modules	Other	Total
FY2020-21	0.8	0.6	0.2	1	0.1	2.7
FY2021-22	1	0.8	0.3	1.5	0.2	3.8
FY2022-23	1.5	1	0.4	2	0.3	5.2
FY2023-24	1.8	1.2	0.5	2.8	0.4	6.7
FY2024-25	2	1.5	0.6	3.5	0.5	8.1
Total	7.1	5.1	2	10.8	1.5	26.5



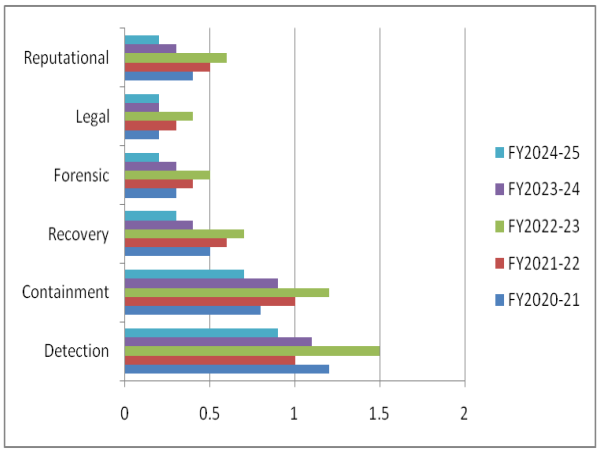
The data indicates that expenditure in all sectors increased consistently between FY2020-2021 and FY2024-2025. This is due to the increased allocation of funds to digital development and training. The preponderance of investment is consistently made up of digital modules, which indicates a shift in the educational landscape toward technology. The caliber of training is improving as the cost of materials and trainers continues to increase. The

Journal of Management Excellence
ISSN: **3108-2815** | Volume 2 Issue 1 January-March 2026
www.jme-journal.com **JME-36**
DOI: *https://doi.org/10.5281/zenodo.19398978*

company's dedication to the enhancement of its digital and overall capabilities is evidenced by the allocation of ₹26.5 crore over a five-year period.

Table 3 — Incident Response Costs

Year	Detection	Containment	Recovery	Forensic	Legal	Reputational	Total
FY2020-21	1.2	0.8	0.5	0.3	0.2	0.4	3.4
FY2021-22	1	1	0.6	0.4	0.3	0.5	3.8
FY2022-23	1.5	1.2	0.7	0.5	0.4	0.6	4.9
FY2023-24	1.1	0.9	0.4	0.3	0.2	0.3	3.2
FY2024-25	0.9	0.7	0.3	0.2	0.2	0.2	2.5
Total	5.7	4.6	2.5	1.7	1.3	2	17.8

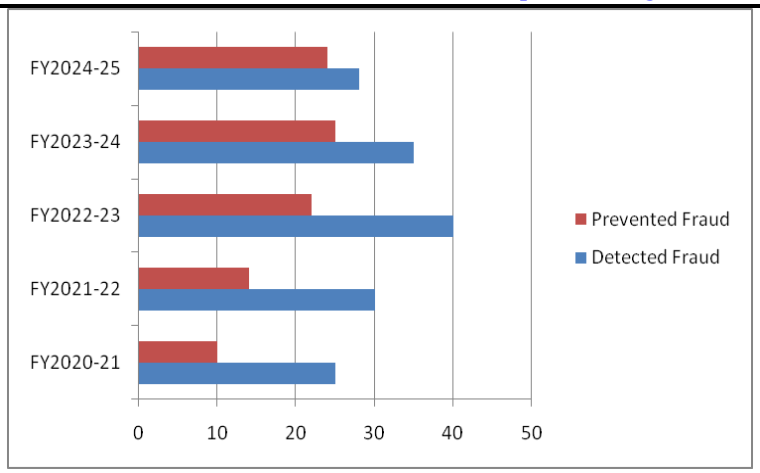


The data indicates that the expenditures associated with the different phases of cybersecurity response have fluctuated over the past five years. The relevance of detection and containment is underscored by the fact that they are consistently the most costly components of incident management. In FY2022-2023, costs increased, suggesting either the implementation of additional preventive measures or a significant security incident. The consistent decrease in the years that have followed indicates that there has been a reduction in the impact of errors, greater control, and increased effectiveness. The total expenditure amounted to ₹17.8 crore.

Table 4 — Fraud: Detected Vs Prevented Vs Net Loss

Year	Detected Fraud	Prevented Fraud	Net Loss (Detected − Prevented)
FY2020-21	25	10	15
FY2021-22	30	14	16
FY2022-23	40	22	18
FY2023-24	35	25	10
FY2024-25	28	24	4
Total	158	95	63

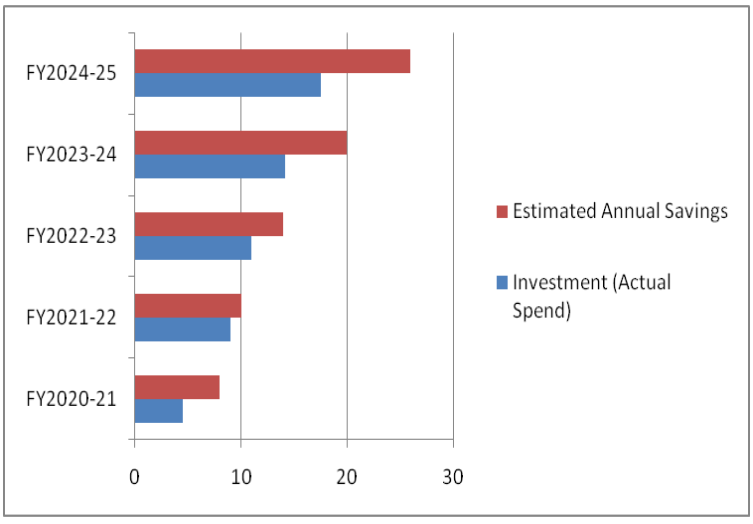
Journal of Management Excellence
ISSN: **3108-2815** | Volume 2 Issue 1 January-March 2026
www.jme-journal.com **JME-36**
DOI: *https://doi.org/10.5281/zenodo.19398978*



The data indicates that the effectiveness of measures to prevent transgression has increased over the past five years. Initially, a greater number of fraud cases were identified; however, the distance between the forgeries that were detected and those that were halted decreased. This illustrates the advancement of security measures and monitoring systems. In the fiscal year 2024-25, the net loss decreased substantially from ₹15 crore in FY2020-21 to ₹4 crore. This illustrates that fraud detection is enhancing, and preventative strategies are being implemented with greater vigor. Efforts to mitigate financial hazards are illustrated by a net loss of ₹63 crore.

Table 5 — Annual ROI on Security Investments

Year	Investment (Actual Spend)	Estimated Annual Savings	ROI (%)
FY2020-21	4.5	8	177.78%
FY2021-22	9	10	111.11%
FY2022-23	11	14	127.27%
FY2023-24	14.2	20	140.85%
FY2024-25	17.5	26	148.57%
Cumulative	56.2	78	138.79%



Journal of Management Excellence
ISSN: **3108-2815** | Volume 2 Issue 1 January-March 2026
www.jme-journal.com **JME-36**
DOI: *https://doi.org/10.5281/zenodo.19398978*

The results indicate that the return on investment (ROI) had a consistent and positive trend between FY2020-2021 and FY2024-2025. Annual investments increased over time, but the savings they generated increased at an even quicker pace, suggesting that resources were being utilized effectively. Throughout the period, the return on investment (ROI) averaged over 100%, reaching a high of 177.78% in FY2020-21 and remaining consistent thereafter. Over the course of five years, the initiatives generated substantial revenue while maintaining low costs, as evidenced by the aggregate ROI of 138.79%.

5. CONCLUSION

Mobile banking in India has significantly altered the way individuals manage their finances by simplifying, expediting, and streamlining the process. Nevertheless, the reliance of individuals on digital platforms increases their susceptibility to data breaches, cyberattacks, and fraud. In order to guarantee the security of mobile banking, it is necessary to implement a variety of technological solutions, such as secure passwords, frequent upgrades, dependable security software, and two-factor authentication. In order to prevent phishing, utilize secure networks, and supervise your account activities, it is imperative to exercise caution. Additionally, it is imperative that consumers comprehend the best practices, potential hazards, and secure usage of their devices. By emphasizing technical safeguards and continuous education, fostering trust in digital banking services, and contributing to the safety and security of India's mobile banking ecosystem, individuals can substantially mitigate their risk of financial loss.

REFERENCES

1. Krishnan, Sankar. The Power of Mobile Banking. John Wiley & Sons, Inc., 2014.
2. Grabner, Constantin, Rajnish Tiwari, and Stephan Buse. Perspektiven des Mobile Banking in Deutschland. Springer Fachmedien Wiesbaden, 2016.
3. Wittkamp, Bernd. "Mobile Banking." In Köpfe der digitalen Finanzwelt. Springer Fachmedien Wiesbaden, 2020.
4. Cross, Richard F. Self-paced security and fraud training for banks. Sheshunoff, 2004.