© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1722704

Impact of Cyber Frauds on Digital Banking Services: A Study with Reference to India Post Payments Bank (IPPB)

RANJITHA M[1], NAVYA MAHADEV NAIK[2]
[1,2]*Post Graduate Student, MBA in Finance and Digital Marketing, MBA Programme Bapuji Institute of Engineering and Technology (BIET), Davangere, Karnataka, India*

Abstract- ***Digital banking has fundamentally transformed the way customers access financial services, and India Post Payments Bank (IPPB) has played a central role in extending this transformation to rural and semi-urban India through its vast postal network. However, the rising adoption of digital transactions has been accompanied by a corresponding rise in cyber-fraud incidents such as phishing, OTP swindles, identity theft, fake UPI requests and Aadhaar-enabled payment fraud, which pose a serious threat to the security and credibility of digital banking. This article examines the impact of cyber fraud on the digital banking services of IPPB, drawing on primary data collected from sixty customers and secondary data from journals, reports and official sources. The study analyses the common types of cyber fraud experienced by customers, evaluates their level of cyber-security awareness, and assesses how such fraud incidents influence customer trust, satisfaction and continued adoption of digital banking. The findings indicate that a majority of respondents have encountered suspicious communications and a considerable proportion have suffered financial loss, which has measurably eroded trust despite IPPB's existing security infrastructure. The study concludes that sustained customer education, stronger real-time fraud detection and more accessible grievance-redressal mechanisms are essential to safeguard customer confidence and support the sustainable growth of digital banking under IPPB.***

Keywords: digital banking, cyber fraud, india post payments bank, customer trust, financial inclusion, cyber security awareness

I. INTRODUCTION

The rapid growth of digital banking has made it possible for customers across the banking industry to access financial services quickly and conveniently. Within this transformation, India Post Payments Bank (IPPB) has played an instrumental role in advancing financial inclusion, particularly for rural and semi-urban customers who were historically underserved by conventional banks. Established by the Government of India under the Department of Posts, Ministry of Communications, and launched nationwide on 1 September 2018, IPPB leverages the country's largest postal network — over 1.55 lakh post offices and around 3 lakh postal employees — to deliver banking services at the customer's doorstep.

IPPB offers a range of basic banking functions including savings accounts, money transfers, bill payments, insurance and pension products, mobile banking, and QR-code based payment solutions. As a payments bank, it is not permitted to offer loans or credit cards; instead, its focus remains on providing a secure and seamless transactional experience through Aadhaar-enabled payment systems, micro-ATMs, and a mobile banking application operated with the support of postmen and Gramin Dak Sevaks (GDS).

However, the very convenience that has driven adoption of digital banking has also expanded the attack surface available to cybercriminals. As customers increasingly rely on mobile applications, UPI and Aadhaar-based authentication, they are exposed to a growing range of cyber-fraud techniques, including phishing, OTP swindles, identity theft, fake payment links and SIM-swap fraud. When such incidents occur, they not only cause direct financial loss but also erode the confidence that is essential for the continued adoption of digital financial services, particularly among first-time and rural users. This study investigates the extent and nature of this problem within the specific context of IPPB's customer base.

1.1 Statement of the Problem

The rapid digitisation of banking services under IPPB has revolutionised financial accessibility across rural and semi-urban India, but this transition has occurred faster than the digital literacy of many customers has been able to keep pace with. This gap between the sophistication of digital services and the preparedness of users has created an opening that cybercriminals exploit — not primarily through complex hacking, but through social engineering techniques that target the customer directly. Rising incidents of Aadhaar-enabled payment fraud, UPI-related scams, vishing and phishing threaten to reverse the gains of financial inclusion by pushing frightened customers back toward cash-based, informal means of managing money, while simultaneously exposing the bank to reputational and operational risk. This creates an inherent tension between maximising the ease of use of digital banking and building security protocols robust enough to withstand user-targeted attacks — a tension that merits focused empirical investigation.

1.2 Need for the Study

This study is necessary to identify the structural and human vulnerabilities through which fraudulent activity slips past IPPB's transaction-monitoring safeguards. By examining the socio-economic profile of affected customers alongside the specific types of fraud they encounter, the research provides evidence that can inform more effective fraud-prevention strategies. The findings can help application developers design interfaces that are less exploitable by semi-literate users, and can give bank management concrete data with which to refine customer awareness programmes and convert vulnerable touchpoints into proactive lines of defence against financial crime.

1.3 Objectives of the Study

- To identify the common types of cyber fraud faced by IPPB customers.
- To examine the categories of customers who are most vulnerable to such frauds.
- To measure the overall impact of digital banking frauds on customer trust and behaviour.
- To assess the effectiveness of the bank's existing security measures and suggest possible solutions.

1.4 Scope of the Study

The scope of the study is confined to fraudulent activity of a digital nature — that is, offences committed through digital banking channels or targeting individual or institutional customers of IPPB through electronic means such as mobile banking, UPI and the Aadhaar Enabled Payment System (AEPS). Traditional physical bank fraud and internal employee malfeasance fall outside the scope of this study.

1.5 Hypotheses

H0(1): Cyber fraud has no significant effect on the usage of digital banking services among IPPB customers.

H1(1): Cyber fraud has a significant impact on the usage of digital banking services among IPPB customers.

H0(2): There is no significant relationship between cybersecurity awareness and vulnerability to cyber fraud among IPPB customers.

H1(2): There is a significant relationship between cybersecurity awareness and vulnerability to cyber fraud among IPPB customers.

1.6 Limitations of the Study

- The study is confined to a selected sample of IPPB customers and may not represent the views of all IPPB customers across India.
- The relatively small sample size may affect the extent to which the findings can be generalised.
- The study focuses only on cyber frauds related to digital banking and excludes traditional banking frauds.
- Findings rest largely on respondents' self-reported perceptions and experiences, which vary across individuals.
- Some respondents may have been reluctant to disclose fraud incidents due to privacy concerns or embarrassment.
- The study is regionally concentrated, which may limit generalisability to other parts of the country.
- Rapid changes in technology and cyber-security threats may affect the long-term applicability of the findings.

II. REVIEW OF LITERATURE

Cyber fraud refers to fraudulent operations conducted through digital platforms to steal money, personal information, or banking credentials. As financial institutions have expanded their use of digital technology and as customers increasingly conduct business online, exposure to cybercrime — including phishing, malware, identity theft, OTP fraud, fake accounts and social-engineering tactics — has grown correspondingly. A substantial body of research over the past several years has examined this relationship between digital banking growth and cyber-fraud risk, and the key strands of this literature are summarised below.

Several studies have traced the changing structure of the banking sector as it has shifted from traditional, branch-based operations toward digital and mobile-first models (Sai Manoj, 2021), and have shown that mobile banking meaningfully expands financial inclusion and accessibility, particularly for unbanked and low-income populations in developing economies (Akter, Anwar, Mustafa & Ali, 2021). At the same time, research consistently finds that the growth of digital and UPI-based payments has been accompanied by rising cybercrime risk. Neha Priya, Ahmed and Alam (2021) identified phishing, identity theft and unauthorised transactions as the principal threats to consumer trust and proposed a five-stage risk-mitigation framework covering monitoring, prediction, detection, data analysis and incident reporting. Similarly, Dr. Gulshan Kumar (2021), drawing on RBI data, found that internet- and card-based transactions are especially exposed to fraud and stressed the need for stronger security mechanisms and fraud-detection systems.

A parallel stream of research has examined the customer-experience side of digital banking. Metlo, Hussain, Saqib, Phulpoto and Abro (2021) found that perceived usefulness, ease of use and credibility are the core drivers of customer satisfaction with mobile banking, while Raja Sankaran and Chakraborty (2021), surveying 457 Indian mobile banking users, established that trust and perceived security are major determinants of continued adoption, and that cyber threats measurably reduce customer confidence. Vijayalakshmi, Priyadarshini and Umamaheswari (2021) similarly found that fear of financial loss and data breaches reduces customers' willingness to use online banking, while Sunil Sasi (2022) reported that phishing, unauthorised transactions and online payment fraud have emerged as significant threats requiring stronger fraud-prevention mechanisms and customer education.

Studies focused specifically on customer vulnerability have found that online behaviour and social-media activity increase susceptibility to fraud, as cybercriminals exploit publicly available information to conduct phishing and identity-theft attacks (Nilaya Murthy & Gopalkrishnan, 2022). Ramesh and Karthikeyan (2022) found that fear of cyber fraud actively discourages customers from using digital banking channels, underscoring the importance of continuous monitoring and awareness programmes. More recent studies have extended this line of inquiry: Adeniyi, Ojelade, Taiwo, Obunadike and Oloyede (2023) reviewed cybersecurity tactics — including encryption, access control and digital forensics — for mitigating a broad range of cybercrimes, while Venkatesh and Suresh Kumar (2023) and Anitha and Prabakaran (2023) both found that phishing, UPI-related fraud and OTP scams remain the dominant threats, and that low digital literacy significantly increases customer vulnerability.

Work published in 2024 and 2025 has reinforced these findings while extending them to newer technologies. Srivastava and Sharma (2024) found that data-privacy concerns and AI-based fraud detection both significantly shape customer trust in digital banking, while Sharma and Gupta (2024) linked rising cyber-fraud cases directly to reduced willingness to adopt digital banking. Afzal, Meraj, Kaur and Ansari (2024), studying 389 respondents across major Hindi-speaking cities, examined how cybersecurity initiatives shape financial inclusion for rural users, and Mehta (2024) characterised digital technology as a 'double-edged sword' that expands both the opportunities available to fraudsters and the tools available to institutions for detecting them. Akinbowale, Mashigo and Zerihun (2024) developed a regression-based model to estimate the monetary

cost of cybercrime to South African banks, while Afzal, Ahmad and Ansari (2024) demonstrated, using an extended Technology Acceptance Model, that customer awareness of cybersecurity is positively associated with intention to adopt e-banking. Most recently, Keerti Reddy and Kudachimath (2025) found that identity theft, digital-payment fraud and phishing attacks have all increased sharply, undermining consumer confidence and creating operational and reputational challenges for banks, and recommended stronger real-time fraud-detection tools alongside expanded customer education.

Taken together, this literature consistently points to three conclusions that motivate the present study: first, that digital banking growth and cyber-fraud incidence rise together; second, that customer trust and continued adoption are highly sensitive to fraud exposure; and third, that awareness and digital literacy are the most consistently cited mitigating factors. These conclusions are directly relevant to IPPB, whose customer base is disproportionately rural, semi-urban and, in many cases, new to formal banking — precisely the demographic that the literature identifies as most vulnerable.

III. RESEARCH METHODOLOGY

The study adopts a descriptive and analytical research design to examine both the structural patterns and the human dimensions of cyber fraud in digital banking. A structured questionnaire was administered to sixty (60) IPPB customers, and the data collected were supplemented with secondary information drawn from journals, articles, reports and official websites, including the annual reports of IPPB and RBI guidelines on digital banking and cyber security. The collected data were coded and analysed using percentage analysis, frequency distribution and Likert-scale interpretation to examine consumer vulnerability and perceptions of system reliability.

IV. DATA ANALYSIS AND INTERPRETATION

This section presents the results of the primary survey of sixty IPPB customers, covering respondent demographics, exposure to cyber fraud, awareness levels, and perceptions of IPPB's security and grievance-handling systems.

4.1 Demographic Profile of Respondents

Table 1: Gender-wise Distribution of Respondents

Gender	Respondents	Percentage (%)
Male	28	53
Female	32	47
Total	60	100

Of the sixty respondents surveyed, thirty-two were female and twenty-eight were male, indicating a fairly balanced sample with a slightly higher representation of women.

Table 2: Age-wise Distribution of Respondents

Age Group	Respondents	Percentage (%)
Below 25 years	15	25
25–35 years	10	17
36–45 years	30	50
Above 45 years	5	8
Total	60	100

Half of the respondents fell within the 36–45 age bracket, suggesting that middle-aged customers are the most active users of IPPB's digital banking services, while customers above 45 years represented only 8 percent of the sample.

Table 3: Educational Qualification of Respondents

Qualification	Respondents	Percentage (%)
No Formal Education	1	3
Primary Education	6	10
Secondary Education	10	16
Graduate	27	45
Postgraduate	16	26
Total	60	100

Graduates formed the largest group of respondents (45 percent), followed by postgraduates (26 percent), indicating that a considerable share of digital banking users hold higher educational qualifications, although customers with only secondary, primary or no formal education together still accounted for 29 percent of active users.

4.2 Digital Confidence and Fraud Exposure

Table 4: Confidence in Using Digital Banking Services Independently

Response	Respondents	Percentage (%)
Very Confident	10	16
Confident	39	65
Not Confident	9	15
Very Unconfident	2	4
Total	60	100

A large majority of respondents (81 percent, combining 'confident' and 'very confident') reported feeling capable of using digital banking services independently, suggesting reasonably strong familiarity with digital platforms even though this confidence does not necessarily translate into safe practices, as later tables show.

Table 5: Cyber Frauds Heard About or Experienced

Type of Fraud	Respondents	Percentage (%)
Aadhaar (AePS) Biometric Fraud	5	6
Fake UPI Payment Request	10	26
Phishing	11	24
OTP Fraud	15	28
SIM Fraud	11	16
Total	60	100

OTP fraud was the most commonly reported category (28 percent), followed closely by fake UPI payment requests (26 percent) and phishing (24 percent), while SIM fraud and Aadhaar-based biometric fraud were reported less frequently. This pattern indicates that customers are most exposed to fraud techniques that exploit direct communication with the victim rather than purely technical intrusion.

Table 6: Receipt of Suspicious Calls, Messages or Links

Response	Respondents	Percentage (%)
Yes	49	81
No	11	19
Total	60	100

A striking 81 percent of respondents reported having received a suspicious banking-related call, message or link, confirming that social-engineering attempts are widespread among IPPB's digital banking customers.

Table 7: Verification of Authenticity Before Sharing Banking Information

Response	Respondents	Percentage (%)
Always	16	26
Often	13	21
Sometimes	24	40
Rarely	6	10
Never	1	3
Total	60	100

Only 26 percent of respondents said they always verify the authenticity of a message, call or link before sharing banking information, while 40 percent do so only sometimes. This gap between reported confidence in Table 4 and actual verification behaviour here points to a meaningful awareness deficit.

4.3 Financial Impact and Trust

Table 8: Financial Loss Due to Cyber Fraud

Response	Respondents	Percentage (%)
Yes	41	68
No	19	32
Total	60	100

Sixty-eight percent of respondents reported having suffered financial loss due to a cyber-fraud incident connected to digital banking — a substantial figure that underscores the real and material cost of the vulnerabilities identified above.

Table 9: Effect of Cyber Fraud on Trust in IPPB's Digital Banking Services

Response	Respondents	Percentage (%)
Strongly Agree	8	13
Agree	24	40
Neutral	26	43
Disagree	2	4
Strongly Disagree	0	0
Total	60	100

More than half of respondents (53 percent, combining 'agree' and 'strongly agree') indicated that cyber fraud has reduced their trust in IPPB's digital banking services, while 43 percent remained neutral. Very few respondents disagreed, confirming that cyber-security concerns have a tangible effect on customer confidence.

Table 10: Perceived Impact of Cyber Fraud on Customers' Financial Security

Rating (1=Low, 5=High)	Respondents	Percentage (%)
1	7	12
2	13	22
3	22	36
4	6	10
5	12	20
Total	60	100

The largest share of respondents (36 percent) rated the impact of cyber fraud on their financial security as moderate, while a further 20 percent rated it as highly significant, reinforcing the demand for stronger protective measures.

4.4 Perceptions of IPPB's Security Measures

Table 11: Effectiveness of IPPB's Security Measures in Preventing Cyber Fraud

Rating (1=Low, 5=High)	Respondents	Percentage (%)
1	1	2
2	10	17
3	26	43
4	15	25
5	8	13
Total	60	100

Respondents generally rated IPPB's existing security measures — OTP verification, biometric authentication and fraud alerts — as moderately to highly effective, with 38 percent rating them 4 or 5 on a five-point scale, though 43 percent gave a neutral rating of 3, suggesting room for improvement.

Table 12: Perceived Adequacy of IPPB's Cyber-Fraud Awareness Programmes

Response	Respondents	Percentage (%)
Strongly Agree	5	8
Agree	30	50
Neutral	22	36
Disagree	3	5
Strongly Disagree	0	1
Total	60	100

Half of the respondents agreed that IPPB provides sufficient awareness programmes regarding cyber-fraud prevention, and a further 8 percent strongly agreed. However, more than a third remained neutral, indicating that a meaningful segment of customers do not feel adequately informed.

Table 13: Satisfaction with IPPB's Cyber-Fraud Reporting Process

Response	Respondents	Percentage (%)
Very Satisfied	7	12
Satisfied	28	46
Neutral	21	35
Dissatisfied	2	4
Very Dissatisfied	2	3
Total	60	100

A majority of respondents (58 percent) expressed satisfaction with IPPB's process for reporting cyber-fraud incidents, while 35 percent remained neutral and only 7 percent expressed dissatisfaction, suggesting that the reporting mechanism is functioning reasonably well but is not yet uniformly trusted.

Table 14: Effect of Cyber Fraud on Reputation and Continued Adoption

Response	Respondents	Percentage (%)
Strongly Agree	5 / 9	9 / 15
Agree	27 / 26	45 / 43
Neutral	26 / 24	43 / 40
Disagree	2 / 1	3 / 2
Strongly Disagree	0 / 0	0 / 0
Total	60 / 60	100 / 100

Note: figures show responses to two related statements side by side — reputational harm to IPPB,

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1722704

and discouragement from regular digital banking use. A majority of respondents agreed that frequent cyber-fraud incidents can harm IPPB's reputation, and a similar majority agreed that such incidents discourage regular use of digital banking, confirming that the consequences of cyber fraud extend beyond individual financial loss to the bank's broader standing and adoption trajectory.

V. FINDINGS

- Aadhaar Enabled Payment System (AePS) fraud, fake UPI payment requests, OTP fraud, phishing and suspicious calls or messages are the most prevalent forms of cyber fraud affecting IPPB's digital banking customers.
- Users with lower educational attainment, elderly customers, and those with limited digital banking experience are more vulnerable to cyber fraud due to insufficient awareness of online safety practices.
- A large proportion of customers (81 percent) have received suspicious calls, messages or links, indicating the widespread use of social-engineering techniques by cybercriminals targeting IPPB customers.
- Many customers do not consistently verify the authenticity of calls, messages or links before sharing sensitive information, which increases their exposure to fraud.
- Although IPPB has implemented security measures such as OTP verification, biometric authentication and fraud alerts, a significant share of customers believe that greater awareness and education efforts are still required.
- Cyber fraud causes both financial loss and psychological distress among customers, an effect that appears more pronounced in rural and low-income communities.
- IPPB's reputation is at risk if cyber-fraud incidents continue to rise, as customers who perceive digital banking as unsafe become less likely to adopt or continue using it.
- The efficiency of the bank's fraud-reporting and complaint-resolution system plays a significant role in sustaining customer confidence.

VI. SUGGESTIONS

- Strengthen customer awareness programmes through regular cyber-security workshops, village-level awareness campaigns and simple educational sessions delivered via Gramin Dak Sevaks.
- Provide cyber-safety information in regional languages through posters, SMS alerts, videos and demonstrations to improve comprehension among rural customers.
- Give special attention to elderly and less-educated customers through personalised guidance on safe digital banking practices.
- Regularly educate customers not to share OTPs, Aadhaar details, PINs, passwords or other banking information with unknown callers or through suspicious links.
- Improve real-time fraud-detection systems and send immediate transaction alerts so that customers can identify unauthorised activity quickly.
- Strengthen the fraud-reporting process through faster support, simpler complaint-registration methods and timely resolution of cyber-fraud cases.
- Encourage collaboration between the government, banks and cyber-security agencies to build stronger digital-safety mechanisms for rural banking users.
- Encourage customers to verify every digital transaction and to rely only on official IPPB channels for banking-related communication.

VII. CONCLUSION

Digital banking has meaningfully improved the accessibility and convenience of financial services, and IPPB has been central to extending this transformation into rural and semi-urban India. However, this study confirms that the corresponding rise in cybercrime — particularly phishing, OTP scams, fake UPI requests and identity theft — has a measurable and material impact on the trust customers place in digital banking. Sixty-eight percent of surveyed customers reported financial loss from cyber fraud, and just over half indicated that such incidents had reduced their trust in IPPB's

digital services, despite generally positive perceptions of the bank's existing security infrastructure.

The findings suggest that the primary vulnerability lies not in the technical security of IPPB's systems but in the gap between customers' confidence in using digital platforms and their actual practice of verifying communications before sharing sensitive information. Addressing this gap through sustained, regionally and demographically targeted awareness programmes, combined with stronger real-time fraud detection and a more responsive grievance-redressal process, is essential to protect customers and to support the continued, sustainable growth of digital banking under India Post Payments Bank.

REFERENCES

[1] Kothari, C. R. (2019). *Research Methodology: Methods and Techniques.* New Age International Pvt. Ltd., New Delhi.

[2] Gupta, S. P. (2020). *Statistical Methods.* Sultan Chand and Sons Publishers, New Delhi.

[3] Indian Institute of Banking & Finance (IIBF). (2022). *Digital Banking and Cyber Security.* Macmillan Education.

[4] Khan, M. Y. (2020). *Indian Financial System.* McGraw Hill Education.

[5] India Post Payments Bank. (2023). *Annual report 2022–23.* Retrieved from https://www.ippbonline.com

[6] India Post Payments Bank. (2024). *Annual report 2023–24.* Retrieved from https://www.ippbonline.com

[7] Reserve Bank of India. (2023). *Guidelines for payments banks.* Retrieved from https://www.rbi.org.in

[8] Digital India. (2025). *Digital India Programme.* Retrieved from https://www.digitalindia.gov.in

[9] India Post. Official website. Retrieved from https://www.indiapost.gov.in

[10] National Payments Corporation of India (NPCI). Official website. Retrieved from https://www.npci.org.in

[11] Ministry of Communications, Government of India. Department of Telecommunications. Retrieved from https://dot.gov.in

[12] Press Information Bureau (PIB), Government of India. Retrieved from https://pib.gov.in

Note: In-text citations for the individual studies discussed in the Review of Literature (2021–2025) follow the author names and years as reported in the source project report; full bibliographic details for each journal article should be verified against the original publications before submission.