International Journal of Scientific Research and Engineering Development-– Volume 8 Issue 5, Sep-Oct 2025
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Online Banking Scams with Bank Customers in India: Reasons & Resolutions

Author: Dr. K. R. Kaushik
Visiting Faculty at Ramanujan College (DU) Amity University (ASoDL), FIIB, K K Modi University
&
Former Dy. Director General (ACE) & Vice President (CR) GSFC
Mail ID: krkgsfc@gmail.com
kedarkaushik@rediffmail.com

Abstract

The rapid digitization of India's banking ecosystem has significantly increased the convenience of financial transactions. However, this transformation has simultaneously created vulnerabilities that cybercriminals exploit through online scams. This paper explores the prevalence, nature, and impact of online scams targeting bank customers in India. It provides a typology of major frauds, assesses their economic and social consequences, examines the role of bank officials, and evaluates current policy responses. The study draws on case studies, secondary data, and comparative global frameworks to suggest comprehensive strategies—preventive, punitive, regulatory, and cooperative—that can strengthen resilience against online scams. Recommendations include stricter punishments, enhanced digital literacy, cross-border enforcement, and improved accountability for financial and telecom institutions. The findings contribute to ongoing policy debates on consumer protection, financial security, and cyber resilience in India.

Keywords: Online scams, Banking fraud, Cybercrime, Financial security, India, Digital economy

JEL Codes: G21 – Banks; Other Depository Institutions, K24 – Cyber Law, O33 – Technological Change: Choices and Consequences and D18 – Consumer Protection

1. Introduction

India's rapid shift to digital banking, spurred by government initiatives like Digital India and the Unified Payments Interface (UPI), has revolutionized access to financial services. Millions of Indians now rely on mobile banking, internet banking, and digital wallets for everyday transactions. However, this surge has created new vulnerabilities. Online scams—ranging from phishing and SIM swaps to identity theft and fraudulent mobile applications—are eroding customer trust, straining regulatory systems, and leading to significant financial losses.

According to the National Crime Records Bureau (NCRB), reported cyber fraud cases in India have grown exponentially over the last five years, with bank-related scams accounting for a major share. The Reserve Bank of India (RBI) has issued several circulars on consumer protection, but enforcement gaps remain. This paper investigates these scams in depth, situating them within broader debates on financial inclusion, cybersecurity, and consumer protection. The financial impact has been equally devastating. From Rs 551 crore in 2021, losses have skyrocketed to Rs 22,812 crore in 2024, representing a growth rate that far exceeds any legitimate economic expansion

2 Literature Review

Scholars and policymakers have increasingly turned their attention to cyber fraud in banking:

Indian Studies: Research by Singh (2021) highlights how low digital literacy exacerbates susceptibility to phishing scams. NITI Aayog (2022) emphasizes the need for cross-sectoral regulatory frameworks. Studies from RBI Working Papers identify poor grievance redressal as a systemic weakness.

Global Perspectives: Anderson et al. (2019) outline the economics of cybercrime, noting how fraud networks exploit weak jurisdictions. European Central Bank reports show how the EU's strong data protection laws

reduce scams. US-based research highlights the effectiveness of dedicated cybercrime task forces.

This literature establishes that while digital adoption increases efficiency, it must be accompanied by strong consumer protection and regulatory safeguards.

3. Methodology

This paper adopts a mixed-method approach:

Secondary Data Analysis: RBI reports, NCRB statistics, CERT-In advisories, and international cybercrime studies.

Case Study Method: Analysis of selected scams, including phishing, UPI fraud, and insider-assisted scams.

Comparative Framework: Cross-country comparison (Singapore, US, EU, Australia) to benchmark India's punitive and preventive measures.

Analytical Framework: The study uses the Fraud Triangle Theory (incentive, opportunity, rationalization) to explain why scams persist.

4. Typology of Online Scams in India

Phishing and Vishing: Fraudulent emails, SMS, or calls extracting confidential information.

SIM Swap Fraud: Criminals duplicate SIMs to intercept banking OTPs.

UPI and Mobile App Frauds: Fake payment apps or misuse of "collect request" features.

ATM Skimming and Carding: Devices that capture card details.

Identity Theft and Account Takeover: Use of stolen Aadhaar/PAN for fraudulent accounts.

Insider-Assisted Scams: Corrupt bank staff facilitating illegal withdrawals or ignoring suspicious accounts.

5. Impact of Online Scams

Economic: Billions lost annually by consumers; indirect losses due to reduced trust in digital banking.

Social: Elderly, rural, and digitally illiterate populations most vulnerable.

Psychological: Victims face stress, anxiety, and stigma.

Institutional: Erodes credibility of banks and fintech companies.

Case Studies

UPI Scam 2022 (Delhi): Fraudsters sent fake payment links, tricking customers into authorizing debits.

Phishing Attack (Mumbai, 2021): Hundreds fell prey to emails imitating a major bank, losing lakhs.

Insider Fraud (Punjab, 2020): A branch employee colluded with fraudsters to siphon customer funds these cases illustrate diverse techniques and institutional vulnerabilities.

7. Suspected Role of Bank Officials in Online Scams

Bank officials play both positive and negative roles:

Insider Involvement: Some collude with scammers by creating fraudulent accounts or ignoring suspicious transactions.

Negligence: Poor KYC compliance, weak monitoring, and failure to block red-flagged accounts.

Accountability Measures: RBI mandates audits, staff training, and whistle-blower systems, but enforcement gaps persists

Preventive steps include biometric KYC, AI-driven monitoring, rotation of staff, and stronger whistle-blowers protections.

8. Tackling Online Scams: Comprehensive Strategies

Regulatory: Stronger RBI guidelines, mandatory reporting, enhanced cybersecurity norms.

Institutional: Dedicated fraud monitoring cells in banks, real-time fraud detection systems.

Technological: Use of AI/ML to detect unusual patterns, block chain-based identity protection.

Consumer-Centric: Nationwide digital literacy campaigns, multilingual awareness drives.

Telecom Integration: Mandatory KYC for SIMs, AI-based spam call filters.

Legal: Updating IT Act provisions, increasing punishments, streamlining jurisdictional overlaps.

International Cooperation: Participation in global cybercrime treaties and data-sharing.

9. Punitive Measures and Deterrence

9.1 Stricter Legal Punishments

- Enhanced penalties under IT Act and IPC.
- Mandatory minimum sentences for high-value frauds.
- Asset confiscation from convicted criminals.

9.2 Fast-Track Cybercrime Courts

- Specialized courts to ensure trials within 3–6 months.
- Training judges and prosecutors in digital forensics.

9.3 Cross-Border Enforcement

- Strengthened MLATs and regional cooperation.
- Extradition of cybercriminals abroad.

9.4 Accountability of Bank and Telecom Officials

- Penalties for negligence.
- Performance-linked accountability.

9.5 Public Blacklisting and Social Sanctions

- Registry of convicted fraudsters.
- Employment bans in finance/IT sectors.

9.6 Victim-Centric Restitution

- Criminal restitution to victims.
- Compensation funds from fines and penalties.

9.7 Comparative Global Examples

Singapore: Up to 10 years' imprisonment under Computer Misuse Act.

United States: Long-term imprisonment under CFAA; restitution mandatory.

European Union: GDPR + EU Cybercrime Directive; Europol's EC3 enables cross-border collaboration.

Australia: ACSC support framework; strict penalties under Criminal Code Act.

India can adopt a hybrid model: stricter punishment + restitution + global cooperation.

10. Findings and Discussion

- Online scams are rising faster than institutional capacity to counter them.
- Consumers remain the weakest link due to low awareness.
- Punitive measures are inadequate compared to global best practices.
- Banks and telecom companies face accountability deficits.
- Technology-driven detection is underutilized.

11. Recommendations

Strong punitive and deterrent actions are essential to curb online scams. Here are additional suggestions focusing on punishment and accountability:

1. Stricter Legal Punishments

- Increase imprisonment terms and monetary fines under the Information Technology Act, 2000 and Indian Penal Code (IPC) for cyber fraud.
- Introduce minimum mandatory sentencing for large-value scams to reduce judicial leniency.
- Confiscation of properties and digital assets of convicted scammers to weaken the economic incentive.

2. Fast-Track Cyber Crime Courts

- Establish specialized cybercrime courts in each state to ensure quick trials (within 6–12 months).
- Reduce case backlogs by training judges and prosecutors in cyber law.

3. Cross-Border Punishment Mechanisms

- Strengthen mutual legal assistance treaties (MLATs) to extradite cybercriminals operating from abroad.
- Regional cooperation (SAARC/ASEAN frameworks) to jointly punish scam syndicates.

4. Accountability of Bank & Telecom Officials

- Penalize negligent bank staff or telecom operators who fail to block suspicious accounts/SIMs despite red flags.
- Introduce performance-linked accountability for officials handling fraud prevention.

5. Blacklist & Social Sanctions

- Maintain a public registry of convicted cyber fraudsters, preventing them from holding financial/telecom accounts.
- Social sanction mechanisms (e.g., employment bans in financial/IT sectors post-conviction).

6. Victim-Centric Punishment Measures

- Criminals must compensate victims as part of sentencing.
- Create a victim restitution fund sourced from fines imposed on convicted fraudsters.

These punitive measures, when combined with strong preventive and regulatory frameworks, will create both fear of law and loss of incentive for criminals, reducing scams significantly.

7. Punitive Measures and Deterrence

Legal Reform: Amend IT Act with stronger penalties.

Cross-Sector Coordination: RBI, TRAI, and MeitY must create joint monitoring cells.

Global Cooperation: Join international cybercrime treaties.

Customer Awareness: Launch sustained digital literacy programs.

Bank Accountability: Impose liability on banks that fail to protect customers.

Data Analytics: Deploy AI/ML-based fraud detection systems nationwide.

12. Conclusion

India's journey toward a digital economy cannot be sustained without addressing the surge in online banking scams. Preventive frameworks, punitive measures, and international cooperation must converge to build a resilient ecosystem. Strengthening laws, holding institutions accountable, raising awareness, and learning from global best practices will protect consumers and reinforce trust in India's banking system. Tackling scams is not merely a financial issue—it is integral to ensuring the credibility and inclusiveness of India's digital transformation.

References

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M. & Savage, S. (2019). Measuring the Cost of Cybercrime. Journal of Cybersecurity.

NITI Aayog (2022). Digital Payments and Cybersecurity in India.

Reserve Bank of India (2021–2023). Annual Reports and Consumer Protection Circulars.

Singh, A. (2021). Cybercrime and Financial Fraud in India. Economic and Political Weekly.

Europol (2022). Internet Organised Crime Threat Assessment (IOCTA).

Federal Trade Commission (2021). Consumer Sentinel Network Data Book.

