World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

How do online banking scams affect consumer behaviour and financial system stability in developing economies like India?

Aarav Kapur *

Grade 12 Student, Kunskapsskolan International, Gurugram, Haryana, India.

World Journal of Advanced Research and Reviews, 2025, 27(02), 798-803

Publication history: Received on 30 June 2025; revised on 08 August; accepted on 11 August 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.27.2.2890

Abstract

Online banking has revolutionised financial transactions by bringing about efficiency, accessibility, and convenience never seen before. However, this shift towards digitalisation of finances has caused significant vulnerabilities, especially through online banking scams. This research paper examines the economic implications of such scams, focusing on how frauds affect consumer behaviour and the broader financial system, particularly in developing economies like India. By delving deeper into several scam typologies, such as phishing and vishing, the paper investigates how consumers' trust in digital banking may be eroded, potentially leading to increased cash dependency. Additionally, the study analyses the financial pressure on banks, regulators and fintech companies as they tend to invest large amounts in fraud detection, cybersecurity infrastructure, and compensation for victims. The paper concludes with policy recommendations aimed at enhancing digital security and restoring public trust in online banking platforms.

Keywords: Online banking scams; Phishing; Vishing; Consumer behaviour; Financial system stability; Developing economies

1. Introduction

The spurring growth of online banking over the last few years has revolutionised India's financial scenario entirely, with unprecedented convenience and accessibility to financial services for consumers. As stated in the RBI Report on Trend and Progress of Banking in India 2023-24, in March 2024, digital payments made up 97.1% of the total value. The Unified Payments Interface (UPI) contributes most of the transaction volume.[1] But this cyber revolution has also provided gullible customers with fresh methods to exploit them. Phishing and vishing attacks hit victims with deceptive messages to seize sensitive banking passwords and make unauthorised transactions.

Phishing typically comprises fraudulent emails or websites that represent legitimate financial institutions, intending to trick users into revealing personal details such as login information or one-time passwords (OTPS). Vishing, also referred to as "voice phishing," is a method of conducting phone calls that persuade victims into sharing private banking details. These calls are most often initiated by scammers acting as bank representatives or law enforcement officials. Phishing and vishing were reported to have contributed a large share of reported cases in 2023, as per the Indian Computer Emergency Response Team (CERT-In), rendering financial fraud the most dominant type of cybercrime in India.[2]

These scams not only make consumers lose money outright, but also create an environment of distrust and anxiety that might deter individuals from utilising digital banking, especially in low-income and rural areas. The financial consequence also extends to regulatory agencies that must implement cybersecurity policies and apply them, and banks that must invest heavily in fraud prevention infrastructure.

* Corresponding author: Aarav Kapur

Phishing and vishing attacks have become powerful enemies of India's digital banking economy, incurring huge monetary losses for consumers and draining confidence in online financial systems, restricting the usage of digital currencies and subjecting financial institutions to heightened economic and regulatory pressures.

2. Case study 1 - Phishing scam in Rajasthan

In January 2023, a 55-year-old farmer from Sri Ganganagar in Rajasthan fell prey to a sophisticated phishing attack that cost him over ₹8 lakh. The whole thing started when his son, Harsh Vardhan, who lives in Dwarka, Delhi, received an SMS stating that their State Bank of India (SBI) account was locked as they had incomplete KYC (Know Your Customer) information. The SMS had a link urging him to take immediate action. Convinced that the message was genuine, Vardhan clicked on the link, which resulted in the download of a fake SBI YONO app. Not knowing the trick, he entered the login details into the imitation application.[3]

Within minutes, ₹8,03,899 worth of unauthorised transactions were carried out from the farmer's account, with money spread across several platforms, including Payu, CCAvenue, and an Axis Bank account. Vardhan immediately alerted his father, who rang up the local bank branch. The bank manager moved fast, cooperating with the cyber cell in Sri Ganganagar to track the transactions. Their timely intervention resulted in the recovery of ₹6.24 lakh, mostly from Payu, which had retained the money pending verification. But the rest of the amount had already been withdrawn or spent, making further recovery difficult.

2.1. India Today

The case highlights the weaknesses of digital banking, particularly in the context of phishing attacks that take advantage of users' trust and sense of urgency. It also emphasises the need for prompt response and coordination among victims, banks, and cybercrime units to limit losses. Additionally, it raises the issue of greater public awareness about cybersecurity practices and the adoption of strong verification processes by financial institutions to avoid such incidents.

3. Case study 2 – Vishing scams in Indore

Early in 2025, Indore was hit by a vishing scam wave targeting unsuspecting credit cardholders with alarming consistency and precision. Scammers impersonating bank officials from highly respected establishments such as Axis Bank and IndusInd Bank called people, telling them that their credit card reward points were set to lapse. Victims were informed that they could immediately exchange these points by clicking on a link or installing a mobile app forwarded through SMS or WhatsApp. One victim, a 47-year-old businessman, was called and asked to act immediately so he would not lose his accumulated points. Thinking the caller was genuine, he installed the application and input his banking credentials and OTPs. In a matter of minutes, ₹4.05 lakh was drained from his account via a series of quick transactions. [5]

It was not a one-off case. Indore police registered more than 50 such cases in a period of a few weeks with an aggregate loss of more than ₹24 lakh. Most victims had complained of receiving similar calls with download links for imitated banking apps or to access fake websites mimicking authentic interfaces. In a few instances, the victims had downloaded .apk files onto their Android handsets, providing remote access to the perpetrators. Though cybercrime units quickly acted upon it, only a third of the stolen money could be traced and recovered, as the fraudsters rapidly transferred the money through electronic wallets and mule accounts.

These scams are much more than aberrant financial errors-they have profound, long-lasting impacts on both people and the financial system. Victims are left distressed, not merely because of the loss of savings, but also because of the psychological shock that results. Fear, anxiety, and an overarching sense of insecurity gain ground, particularly among the senior citizenry and the digitally illiterate sections. In most cases, the victims are discouraged from availing of digital banking again, and therefore, there is a surge in cash transactions again with a reversal of the overall objective of driving a digital economy.

The harm also propagates in the financial system as a whole. Banks have to spend large sums on fraud detection mechanisms, better cybersecurity infrastructure, and customer complaint redressal systems. Regulatory authorities such as the Reserve Bank of India are under increasing pressure to promulgate tighter guidelines, undertake public awareness campaigns, and intensify enforcement measures against cyber scams. The time and resources being invested in combating such scams tend to take away from developmental objectives such as enhancing financial inclusion and increasing digital access in rural regions.

All in all, vishing frauds such as those in Indore highlight an urgent test for developing economies like India. While the nation attempts a cashless economy, the faith and trust of the users in digital platforms becomes indispensable. In the absence of this, the digital divide might increase, and the very promise of financial technology-efficiency, inclusion, and transparency is jeopardised. Thus, combating such scams in the courts of law, educating the masses, and implementing systemic protection is not merely vital; it is imperative.

4. Current policy landscape: regulatory & institutional responses to online banking scams

India's path to a robust and secure digital banking landscape has been influenced by a multi-pronged regulatory approach that focuses on the prevention of fraud, consumer safeguarding, cybersecurity regulation, and user awareness. At the heart of the framework has been the Reserve Bank of India's (RBI) forward-thinking initiative for robust authentication in online transactions. In August 2024, the RBI issued a draft circular titled Alternative Authentication Mechanisms (AFA), opening up a new world beyond SMS-based OTPs. The round divides authentication methods into three security categories-knowledge (PINs, passphrases), possession (hardware/software tokens), and inherence (biometrics)-and requires all electronic payments (other than small, low-value exceptions) to be authenticated by a dynamic factor that is unique, transaction-dependent, and non-reusable. [5]

This risk-based strategy enables banks to adapt authentication methods based on transaction value, channel, and customer. While low-risk transactions such as small-value offline or recurring mandates are excluded, the RBI mandates issuers to secure express customer consent before the implementation of alternative methods of authentication and ensure simple deregistration procedures. [6] The objective is to substantially lower the dependence on phishing or vishing through the inclusion of more robust, customer-specific verification procedures.

In addition to authentication reforms, the RBI has released multiple cybersecurity and operational resilience mandates that banks and financial institutions must adhere to. In particular, the 2023 Master Directions on Information Technology Governance, Risk, Controls and Assurance Practices mandate regulated entities such as banks, NBFCs, and payments banks to enhance IT governance, implement robust cyber-risk frameworks like crisis-response plans, and collaborate in close coordination with CERT-In and RBI on incident reporting. [7]

This includes real-time threat detection and recovery strategies covering threats like phishing, vishing, malware, and DDoS attacks. Additionally, lenders are now obligated to utilise TRAI's Mobile Number Revocation List (MNRL) to identify and block calls from decommissioned numbers, which reduces the potential for fraudsters to pose as using recycled SIM numbers.

At the national level of cybersecurity, CERT-In (Indian Computer Emergency Response Team) has enhanced its role by mandating incident reporting regulations. In April 2022, it made it mandatory that critical organisations-such as banks and payment companies-have to report cyber incidents within six hours, store ICT logs locally, and take measures like NTP synchronisation and VPN auditing.[8]

Moreover, the revised IT Act penalties brought through the Jan Vishwas Amendment (2023) now encompass higher fines (maximum of ₹1 lakh) and imprisonment for default on reporting requirements, bolstering enforcement against violations. Continued international collaboration, including collaborative cyber defence exercises, also enhances national resilience. [9]

Later on, more recently, in February 2025, the RBI issued a new initiative bringing in an officially approved ".bank.in" domain for all banks-with a planned ".fin.in" domain for fintech firms-to give customers a secure, government-monitored URL space. For the purpose of lowering phishing through imitation websites, banks will need to shift by April 2025.[10] The government is also urging banks to use email and messaging authentication measures such as DMARC, SPF, and DKIM and to partner with platforms such as Google, Apple, and WhatsApp to prevent spoofing. [11]

Together, these measures-various as they are from sophisticated authentication protocols and grievance redressal mechanisms to cybersecurity regulations and public awareness-constitute a multi-faceted defence framework. They mitigate not just the technical aspects of fraud, but also consumer confidence and systemic stability. Whilst far from flawless in terms of take-up and consistency, this regulatory framework is evidence of a national determination to stabilise India's digital financial landscape and stem the rise of online bank scams.

5. Critique and recommendations: enhancing policy effectiveness

India's regulatory structure to thwart online banking fraud is strong, but various gaps and implementation issues compromise its effective functioning. This section critically evaluates existing measures and gives pragmatic suggestions to strengthen digital monetary safety.

5.1. Implementation Issues with Alternative Authentication Mechanisms:-

Despite efforts by the RBI to encourage alternative authentication methods (AAM), i.e., passphrases and biometrics, banks have resolutely held back. Private bank advisors have termed this transition as "hard to implement" and expensive, with no apparent incentive for the return on investment and difficulties in operations, especially for multi-channel support, including desktop banking[12]. The ubiquitous use of SMS-based OTPs continues even as SMS channel vulnerabilities increase, with increasing threats from SIM-swap attacks and SS7 protocol vulnerability exploits[13].

Recommendation: RBI should implement the adoption of AFA by a staged yet binding plan with deadline terms of compliance and audit obligations. To facilitate implementation, an AFA toolkit-consisting of open-source SDKs and technical frameworks-must be offered to banks, especially rural or small lenders. Standardisation of authentication methods on desktop and mobile devices must be supported to aid user convenience and adoption.

5.2. Limited Enforcement Beyond High-Level Guidelines

RBI policy is primarily advisory, focusing on principle-based guidelines not specifying obligatory methods. Media reports highlight bankers' wariness: as one fintech advisor suggested, "If it ain't broke, don't fix it," in an expression of institutional conservatism[14]. Lacking sanctionable guidelines, only high-profile banks with compliance problems (Kotak Mahindra, HDFC, etc.) are subject to curbs-this selective enforcement does not strengthen the digital safety net overall[15].

Recommendation: The regulator needs to move from advisories to binding mandates. A tiered enforcement model-starting with system-wide audits and penalising non-compliance, would spur quicker adoption. Public disclosure of compliance measures could spur lagging banks into action.

5.3. Gaps in Public Awareness and Education

Awareness programs such as "RBI Kehta Hai" bring critical warnings against phishing and usage of public Wi-Fi. Yet, they are not suited for targeted groups like rural users and seniors. Also, digital literacy is low. More than 95,000 UPI fraud cases took place in FY 2022–23, which shows that messaging isn't enough[16].

Recommendation: Launch multilingual campaigns to targeted user groups using local banks, self-help groups, and village centers. Integrating short educational videos and short quizzes into banking applications can maximize retention and engagement. Additionally, the implementation of a peer-driven ambassador program in villages may increase trust and awareness.

5.4. Technical Loopholes in Message Authentication and Domain Security

The RBI proposal to introduce a ".bank.in" domain for authentic banking sites has promise but falls short in addressing key areas. Existing wallet and mobile SMS/WhatsApp vulnerabilities, such as spoofed SMS/WhatsApp messages, are still not addressed[17]. No mandatory email security measures, such as DMARC, SPF, or authenticated badges on online platforms, have been enforced by authorities, making consumers susceptible to phishing through spoofed messages.

Recommendation: The RBI must mandate all banks and NBFCs to transition to the ".bank.in" domain and implement consistency in bank communication channels. It will also have to mandate DMARC, SPF, and DKIM email authentication and work with large messaging platforms to support verified organisational identity marks. These measures would abruptly cut down impersonation-based vishing and phishing attacks.

Through remedying these structural, technical, and behavioral deficiencies, India can deepen the confidence of consumers in digital banking. Enforcing AFA with compliance deadlines, improving user education, strengthening communication authenticity, and establishing a unified redressal authority are essential steps to make regulatory regimes a tangible protection for all users, urban or rural, and support the country's digital finance revolution.

6. Conclusion

Online banking fraud, especially phishing and vishing, largely threatens not just consumer confidence but also the institutional stability of financial systems of developing economies such as India. With the nation moving increasingly forward with its digital financial revolution through UPI and mobile banking platforms, these scams stand the chance of destroying long-earned ground through loss of public trust, especially in vulnerable categories such as rural users and elderly citizens. The two case studies examined in this paper capture not only the economic damage caused to people but also the profound psychological and systemic consequences that ensue.

Though the Reserve Bank of India and CERT-In have implemented strong measures to combat these threats through new authentication procedures, cybersecurity measures, and public awareness drives, there are still major challenges. These range from the slow pace at which banks have adopted strong security practices to a lack of coercive enforcement machinery, and too little outreach to those less digitally informed.

Thus, for bolstering the robustness of India's digital banking infrastructure, regulatory intent needs to be supported by enforceable mandates, tighter compliance, and village-level education. Banks need to be made accountable for embracing safer authentication technology, and digital literacy drives need to be brought locally into action and made context-specific. Simultaneously, institutional coordination has to be strengthened for the rapid identification, investigation, and rectification of scams.

In conclusion, the long-term sustainability of India's digital economy relies on building back consumer confidence through system-level protection, clear communication, and broad digital empowerment. Then only can the vision of a secure, inclusive, and effective financial future be realised in its entirety.

References

[1] Reserve Bank of India, & Herwadkar, S. S. (2024). Report on Trend and Progress of Banking in India 2023-24. Reserve Bank of India.

[2] Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics & Information Technology (MeitY), & Government of India. (2023). CERT-In Annual Report 2023 (pp. 1–26).

[3] Bhati, D. (2023, February 20). A man tricked by a fake KYC message lost more than 8 lakh after he clicked on a suspicious link. India Today. https://www.indiatoday.in/technology/news/story/man-tricked-by-a-fake-kyc-message-lost-more-than-8-lakh-after-he-clicked-on-a-suspicious-link-2337219-2023-02-20

[4] English, B. (2025, May 9). Reward point scam hits Indore: Over Rs 24 lakh lost in fake bank calls in 53 cases in 2025; 31% amount recovered. Bhaskar English. https://www.bhaskarenglish.in/local/mp/indore/news/reward-point-scam-hits-indore-over-rs-24-lakh-lost-in-fake-bank-calls-in-53-cases-in-2025-134994427.html

[5] ET Bureau. (2024, July 31). RBI proposes new ways to authenticate e-payments. The Economic Times. https://economictimes.indiatimes.com/news/economy/policy/rbi-releases-draft-rules-on-aeps-touchpoint-operators-to-prevent-frauds/articleshow/112175512.cms?from=mdr

[6] Khan, M. I. (2024, August 7). RBI rolls out new authentication methods for digital payments, alternatives to SMS-based OTPs: Check details. HT Tech. https://tech.hindustantimes.com/tech/news/rbi-rolls-out-new-authentication-methods-for-digital-payments-alternatives-to-sms-based-otps-check-details-71722941030738.html

[7] Linklaters LLP. (n.d.). India - A new and onerous cybersecurity framework, with breach reporting obligations. https://www.linklaters.com/en/insights/blogs/digilinks/2022/may/india-new-and-onerous-cyber-security-framework-and-breach-reporting-obligations

[8] Research, E., & Bfsi, E. (2024, August 2). Beyond OTP: RBI proposes new authentication measures to make digital payments more secure. ETBFSI.com. https://bfsi.economictimes.indiatimes.com/news/policy/beyond-otp-rbi-proposes-new-authentication-measures-to-make-digital-payments-more-secure/112205470

[9] Nishith DeSai Associates. (n.d.). https://www.nishithdesai.com/SectionCategory/33/Regulatory-Hotline/12/49/RegulatoryHotline/14910/1.html

[10] New RBI mandates domain migration: .bank.in for banks, .fin.in for NBFCs. (n.d.-b). https://blogs.compliancecalendar.in/news/company-law/new-rbi-mandates-domain-migration-bankin-for-banks-finin-for-nbfcs-202

[11] What are DMARC, DKIM, and SPF? (n.d.). CLOUDFLARE. https://www.cloudflare.com/en-gb/learning/email-security/dmarc-dkim-spf/

[12] Outlook Business Desk. (2024, September 4). Indian Banks Reluctant to Look for OTP Alternative for Digital Payments. Outlook Business. https://www.outlookbusiness.com/economy-and-policy/indian-banks-reluctant-to-look-for-otp-alternative-for-digital-payments

[13] Joshi, V. C. (2024b, August 1). RBI mulls new ways to authenticate digital payments besides OTP. Check the proposed options to verify online transactions. Mint. https://www.livemint.com/money/rbi-wants-all-digital-payments-to-have-additional-factor-of-authentication-afa-details-here-11722514431126.html

[14] Krol, K., Philippou, E., Emiliano, D. C., & Sasse, M. A. (2015b, January 19). "`They brought in the horrible key ring thing!" Analysing the Usability of Two-Factor Authentication in UK Online Banking. arXiv.org. https://arxiv.org/abs/1501.04434

[15] Kay, C. (2024, April 24). India's central bank bans Kotak Mahindra from signing up digital customers. Financial Times. https://www.ft.com/content/4d1d94dc-0c0c-4789-9d94-93d30fb3d716

[16] Panda, S., & Kawale, A. (2024, July 31). Draft framework: RBI for more options to authenticate digital payments. www.business-standard.com. https://www.business-standard.com/industry/banking/rbi-mandates-afa-for-all-digital-payment-transactions-in-draft-framework-124073101460_1.html

[17] India Cenbank governor pushes for stronger governance, cybersecurity in banks. (n.d.). Reuters. https://www.reuters.com/world/india/india-cenbank-governor-pushes-stronger-governance-cybersecurity-banks-2024-07-03/