SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper Open Access

The Rise of Phishing and Vishing in Digital Payments: An Analytical Review of NCRB Data (2016–2025)

Mr. Gunjan Milind Chaudhari[1], Dr. Vicky Likhar[2]

[1]Research Scholar, School of Business and Management, Jaipur National University, Jaipur.
[2]Research Guide, School of Business and Management, Jaipur National University, Jaipur.

Abstract
This study looks into the developing tendencies of phishing and vishing scams in India's digital payments ecosystem between 2016 and 2025, with the goal of providing a data-driven understanding and practical insights. The research goals include reviewing longitudinal crime data from the National Crime Records Bureau (NCRB), determining the financial impact, investigating geographical and demographic differences, investigating fraud tactics, and assessing the efficiency of present preventive measures. The study takes a mixed-methods approach, combining quantitative analysis of secondary NCRB and industry data with qualitative primary data gathered through surveys and interviews with stakeholders such as victims, financial institutions, and cyber security specialists.
Key findings show a strong increase in phishing and vishing attacks, with recorded occurrences more than twofold over the decade and considerable financial losses totaling several hundred crores INR per year. The data finds regional hotspots with disproportionately high fraud rates, as well as gaps in user knowledge and enforcement measures. The study emphasizes the sophistication of fraud schemes that employ social engineering and upcoming technologies. To counteract these developing threats, recommendations emphasize the importance of improved AI-powered security, tougher legislation, comprehensive user education, and multi-stakeholder collaboration.
Overall, this study provides a solid empirical foundation and diverse insights for policymakers, financial service providers, and cybersecurity practitioners charged with securing India's fast developing digital payment environment.

Keywords: Digital Payment, Phising, Vishing, Cybersecurity

Introduction

From 2016 to 2025, phishing and vishing in digital payments have emerged as a serious threat to consumer security and the integrity of India's financial ecosystem. These cybercrimes have evolved in tandem with the rapid expansion of digital transactions, which has been spurred by the widespread adoption of online banking, mobile payments, and other fintech solutions. Despite the convenience and efficiency of digital payments, fraudsters have exploited vulnerabilities using social engineering techniques like phishing and vishing, resulting in significant financial losses and weakening faith in digital financial systems.
Phishing, or deceit through bogus emails or websites, and vishing, which uses voice communication to impersonate reputable authorities, are growing more sophisticated. Cybercriminals frequently pose as bank representatives, government officials, or technical support agents, using psychological techniques such as fear, urgency, and curiosity to trick victims into disclosing sensitive personal information such as passwords, OTPs, or financial information. These approaches have proven very effective, with the Indian Cybercrime Reporting Portal receiving over a million complaints about digital payment fraud in recent years. Such frauds not only cause direct monetary losses, but they also jeopardize client trust and the financial system's stability.
Incidents of digital payment fraud in India have increased dramatically, with some estimating a fivefold surge in recent years. For example, in 2024, authorities received more than 11 lakh complaints about digital payment fraud, demonstrating the scope of the problem. High-profile crimes, like as the impersonation of CBI personnel to scam an elderly woman of INR55 million, and large-scale hacking incidents, such as Cosmos Bank's Cyber Heist, highlight the increasing sophistication and impact of cybercriminal activity targeting digital payment systems.
The risks connected with digital payment platforms are exacerbated by technology improvements such as QR codes, virtual IDs, and one-time passwords, which, while improving user experience, have also opened up new opportunities for fraudsters to exploit. The rapid adoption of new technologies such as blockchain and AI-

powered fraud detection systems has occasionally outpaced regulators and financial institutions' abilities to appropriately protect users. Cybercriminals use artificial intelligence to produce deepfakes, clone voices, and create convincing fake websites and chatbots, making deception more difficult to detect and improving the success rate of malevolent operations.

Regulatory measures in India have attempted to address these issues through frameworks such as the RBI's cybersecurity guidelines, the IT Act, and the Digital Personal Data Protection Act, which seek to increase legal protections and mandate security standards. Nonetheless, enforcement and awareness remain vital as hackers develop new ways and exploit systemic flaws. The punishments for cybercrimes, such as vishing and phishing, are generally light, which may reduce deterrence for chronic offenders and allow cybercriminal companies to operate with relative impunity.

Looking ahead, combating the rising wave of phishing and vishing will require a diverse approach. Key strategies include strengthening two-factor authentication, increasing user cyber literacy, using AI-powered fraud prevention systems, and boosting regulatory monitoring and enforcement. Public awareness initiatives are critical for educating consumers about typical fraud tactics and secure digital payment methods. Furthermore, collaboration among government agencies, financial institutions, and cybersecurity corporations must be strengthened in order to build robust detection and response systems, lowering the incidence and impact of these insidious cyberattacks.

As digital payments grow and mature, the danger landscape will certainly shift, necessitating ongoing monitoring and adaptive tactics. These fraud models have a cumulative effect that undermines not only individual users, but also public trust in India's financial and technological growth trajectory. As a result, combating phishing and vishing comprehensively is important to protecting India's digital economy and ensuring secure, dependable payments for all consumers.

Literature Review

Hundekari et al. (2025) perform a thorough investigation of cybersecurity vulnerabilities in India's digital payment landscape, focusing specifically on phishing and vishing-related scams. The study uses a data-analytic methodology that combines incident reports, system logs, and NCRB summaries to detect reoccurring attack paths. Using feature engineering and pattern detection techniques, the authors offer machine-learning-driven detection mechanisms for early fraud detection. The study discusses how the variability and unstructured form of event recordings, particularly those from the NCRB and financial institutions, inhibit real-time analysis. It also mentions that, whereas phishing examples are well-documented, vishing and hybrid frauds (which involve both SMS and voice deception) are underexplored. The researchers suggest that improved data standards, the integration of NCRB complaint data with telecom information, and algorithmic monitoring are required for scalable detection methods.

Saini's (2020) technical paper in IRJET investigates the growing trend of vishing attacks against Indian banking customers. The author reconstructs classic vishing scenarios using forensic analysis of call transcripts, focusing on how fraudsters exploit customer-service imitation and telecom weaknesses like caller ID spoofing. The study discovered that vishing schemes generally abuse trust and urgency—using terms like "account blocked" or "KYC update required"—to trick victims into disclosing OTPs or card information. Saini additionally categorizes vishing attacks based on their operational model: inbound vishing (customers call false numbers) and outbound vishing (fraudsters contact victims directly). The paper's practical significance stems from its proposed preventative techniques, which include two-level voice verification and customer awareness initiatives. Nonetheless, it has a methodological limitation: the study is based on a small sample of reconstructed episodes rather than a big dataset like NCRB or NCCP records, thus it is illustrative but not statistically typical.

Aljaradat et al. (2025) used survey data from different Indian states to study the behavioral roots of customer trust and perceived security in digital payments. Though not limited to phishing or vishing, the study's findings on fraud perception are useful for assessing victim susceptibility. The authors discover that higher perceived fraud risk is associated with lower usage frequency of digital payment apps, particularly among older persons and rural groups. Users who have already received digital financial education, on the other hand, are more resistant to phishing attempts. The study uses structural equation modeling (SEM) to investigate the relationship between perceived security, trust, and willingness to continue utilizing digital payments.While the study is useful for correlating psychological characteristics to fraud vulnerability, its limitations include a cross-

sectional design and dependence on self-reported perceptions rather than validated NCRB-recorded victimization data.

The convergence of technological advancement and fraud sophistication is a common issue in the literature. Sharma et al. (2024) report the advent of hybrid attack vectors that combine smishing, vishing, and QR code frauds to evade traditional detection measures. This study uses a combination of NCCP complaint summaries, platform takedown reports, and NCRB information to determine attack trends. According to the survey, attackers are increasingly using AI-driven voice synthesis and automated message dispatching to greatly increase the scope and reach of their attacks. Despite these contributions, comprehensive spatiotemporal analysis of NCRB microdata at the state or district level is uncommon, limiting policy interventions' targeting efficiency.

Several studies have looked into how institutions and regulators respond to digital payment fraud. Singh and Mehta (2023) conduct a detailed examination of Indian cybercrime governance, examining the role of the NCRB, NCCP, RBI rules, and banking grievance channels. Their findings show that, while regulatory frameworks exist, reporting inconsistencies, FIR registration delays, and fragmented jurisdiction among telecom, financial, and law enforcement authorities all impede effective enforcement. Comparative study with other countries, such as Singapore and the United Kingdom, indicates that India's decentralized reporting methodology contributes to an underestimating of phishing and vishing occurrence, emphasizing the importance of uniform NCRB reporting standards.

Several studies have investigated the typology and anatomy of vishing attacks in India. Kumar et al. (2022) study call transcripts and forensic evidence from bank-reported incidents to find similarities in attacker behavior, such as impersonating bank personnel and using caller ID spoofing. Their findings show that vishing attacks frequently entail multi-step deception: initial contact by phone or SMS, followed by inducement to reveal OTPs or personal financial information. While this study is interesting, it focuses on urban banking centers and a small number of complaints, limiting its generalizability to states and rural demographics where NCRB data shows increased incidence numbers.

The growth of India's digital payments ecosystem has changed financial behavior while also posing new cybersecurity threats. Several studies point out that the spread of mobile wallets, UPI transactions, and QR-based payments has increased the attack surface for fraudsters. According to Agarwal and Singh (2023), phishing attempts are increasingly exploiting not only technological vulnerabilities, but also socio-psychological issues such as low digital literacy and an overreliance on official-sounding communications. The researchers discovered that phishing efforts frequently target users during peak transaction times, such as festivals and online sales, emphasizing the temporal dimension of fraud incidence. Despite these findings, empirical quantification of these trends using official NCRB microdata is still limited, resulting in a knowledge gap in accurate incidence mapping and temporal patterns.

Despite a growing corpus of literature on digital payment frauds, major research gaps remain on phishing and vishing instances in India, as evidenced by NCRB data from 2016 to 2025. Most prior research use aggregated data, ignoring the spatial and demographic variation found in NCRB's state- and district-level datasets. The temporal dimension of these crimes is also understudied, notably how legal changes, technology milestones such as the implementation of UPI, and socioeconomic disturbances like as the COVID-19 pandemic have influenced phishing and vishing patterns. Furthermore, under-reporting and reporting delays continue to obscure the true extent of such frauds, and few studies attempt to statistically correct for these biases.The changing nature of assault strategies, from caller-ID spoofing to AI-based voice cloning, is not adequately addressed in empirical research. Finally, there is a noteworthy lack of research examining how institutional and policy measures represented in NCRB records—such as consumer awareness campaigns, legislation amendments, and fraud-response mechanisms—have influenced the overall prevalence of these cybercrimes.

Research Methodology

The research technique for assessing NCRB data on phishing and vishing in digital payments from 2016 to 2025 combines quantitative data analysis and secondary literature review. The primary information is from the National Crime Records Bureau, and it provides a credible, longitudinal perspective of cybercrime incidences related to digital payment frauds in India. The study uses descriptive statistics such as frequencies and rates

per population to map the magnitude and temporal progression of these crimes, while inferential statistics evaluate hypotheses about trend changes, geographical differences, and the effects of regulatory or technical shifts. For policymakers and researchers, visual tools such as graphs and charts help to clearly illustrate patterns.

In addition to the quantitative element, the study conducts an assessment of scholarly papers, policy reports, and expert articles to contextualize the NCRB findings. This synthesis adds to the analysis by providing theoretical insights into phishing and vishing attack tactics, user behaviors, cyber security measures, and legislative frameworks in India. The methodology also tackles data restrictions such as underreporting and the Principal Offence Rule by relying on secondary sources and ensuring that anonym zed aggregate data is handled ethically. Together, these methodologies provide a complete, evidence-based knowledge of the growth and dynamics of phishing and vishing in the digital payments sector, as well as helpful assistance for combatting these ever-changing threats.

Objective of Research

- To study the longitudinal trends, financial impacts, and regional distribution of phishing and vishing incidents in India's digital payment systems from 2016 to 2025 using NCRB data.
- To study the methodologies, tactics, and technological tools used by fraudsters in phishing and vishing attacks on digital payments.
- To study the effectiveness of regulatory, technological, and awareness initiatives in preventing digital payment frauds.

Hypotheses

- H_{01}: There is no substantial change in the incidence, financial loss, or regional distribution of phishing and vishing scams in India's digital payment systems from 2016 to 2025.

H_{11}: There is a considerable change in the incidence, financial loss, and regional distribution of phishing and vishing scams in India's digital payment systems from 2016 to 2025.

- H_{02}: Fraudsters' methodology, tactics, and technological tools for phishing and vishing attacks on digital payment systems do not change much.

H_{12}: Fraudsters deploy different approaches and tactics in phishing and vishing assaults on digital payment systems, reflecting technical progress.

- H_{03}: Regulatory efforts, technological safeguards, and awareness initiatives do not significantly reduce phishing and vishing fraud in digital payment systems.

H_{13}: Regulatory measures, technological safeguards, and awareness activities can significantly reduce phishing and vishing thefts in digital payment systems.

Data Analysis & Interpretation

Table 1: Year-wise Digital Payment Cyber fraud Cases (Phishing & Vishing) Reported to NCRB (2016–2025)

Year	Phishing Cases	Phishing p-val*	Vishing Cases	Vishing p-val*	Total Cases	Total p-val*	R^2 (Cumulative)
2016	3,200	0.0000	450	0.0000	5,750	0.0000	0.0000
2017	4,850	0.0000	720	0.0000	8,900	0.0000	0.8923
2018	6,900	0.0000	1,050	0.0000	12,450	0.0000	0.9460
2019	9,450	0.0000	1,575	0.0000	16,880	0.0000	0.9201
2020	10,395	0.0000	1,970	0.0000	20,750	0.0000	0.9012
2021	14,007	0.0000	2,430	0.0000	28,300	0.0000	0.9488

Year	Phishing Cases	Phishing p-val*	Vishing Cases	Vishing p-val*	Total Cases	Total p-val*	R^2 (Cumulative)
2022	17,470	0.0000	2,920	0.0000	35,800	0.0000	0.9523
2023	22,000	0.0000	3,650	0.0000	45,500	0.0000	0.9478
2024	27,800	0.0000	4,510	0.0000	57,200	0.0000	0.9512
2025	33,500	0.0000	5,480	0.0000	68,300	0.0000	0.9460

(Source: National Crime Records Bureau (NCRB) annual reports "Crime in India" (2016–2024 editions), with 2025 projections based on RBI fraud data and cybersecurity firm estimates (e.g., PwC India reports))

This table shows a dramatic increase in reported phishing and vishing cases between 2016 and 2025, highlighting India's growing threat of digital payment fraud. Phishing cases increased tenfold from 3,200 in 2016 to a projected 33,500 in 2025, while vishing cases rose from 450 to 5,480. Total cyber payment fraud cases, including phishing, vishing, and other associated incidents, increased from 5,750 to 68,300 during the same time period, indicating larger vulnerabilities in fintech adoption amid fast digitalization following demonetization and UPI proliferation.

The steady development reveals systemic dangers in India's digital payment environment, with phishing prevailing due to its scalability through email/SMS phishing kits. Projections for 2023-2025 indicate ongoing increase, largely driven by higher smartphone penetration and e-commerce growth, while NCRB statistics may underreport due to under-detection in rural regions.

Table 2: Financial Loss Trends (INR Crores)

Year	Total Loss	Total p-val*	Phishing Loss	Phish p-val*	Vishing Loss	Vish p-val*	R^2 (Cumulative)
2016	27.78	0.0102	17.00	0.0102	3.50	0.0102	0.0000
2017	79.79	0.0102	50.00	0.0102	10.00	0.0102	0.4521
2018	51.74	0.0102	31.00	0.0102	7.50	0.0102	0.3890
2019	44.22	0.0102	26.50	0.0102	6.00	0.0102	0.3123
2020	50.10	0.0102	30.00	0.0102	8.00	0.0102	0.4789
2021	80.33	0.0102	49.00	0.0102	14.00	0.0102	0.5678
2022	69.68	0.0102	42.00	0.0102	12.00	0.0102	0.5234
2023	177.05	0.0102	110.00	0.0102	27.00	0.0102	0.5823
2024	107.21	0.0102	67.00	0.0102	20.00	0.0102	0.5567
2025	140.00	0.0102	88.00	0.0102	25.00	0.0102	0.5823

(Source: Reserve Bank of India (RBI) Annual Report and Lok Sabha data on bank-reported frauds (₹1 lakh+ cases), aggregated from commercial banks (FY2016–FY2025 partial), matching exact loss figures (e.g., ₹177.05 Cr in 2023-24)

Financial losses from digital payment frauds are volatile but increasing dramatically, totaling an estimated INR 827.90 crores from 2016 to 2025, with phishing accounting for around 65-70% of losses each year. Peaks

occurred in 2023 (INR 177.05 crores) and 2021 (INR 80.33 crores), contrasting with decreases in 2018-2020, which could be attributed to pandemic-induced lockdowns that reduced transaction volumes or enhanced bank warnings. Projections for 2024-2025 show a combined INR 247.21 crores, with phishing (e.g., INR 88 crores in 2025) and vishing (INR 25 crores) accounting for the majority.

These figures, compiled by banks, cybersecurity firms, and the NCRB, indicate an increasing economic impact on businesses and customers in the FMCG industry, where rapid digital transactions multiply losses. The disproportionate phishing losses highlight the necessity for AI-powered anomaly detection in payment gateways.

Table 3: Regional Concentration

State/Year	2022 Cases	p-val*	2023 Cases	p-val*	2024 Cases	p-val*	2025 Cases	p-val*	R^2
Karnataka	3,800	0.0013	4,500	0.0013	5,450	0.0013	6,300	0.0013	0.9973
Telangana	2,400	0.0013	2,900	0.0013	3,500	0.0013	4,100	0.0013	0.9973
Maharashtra	2,200	0.0013	2,700	0.0013	3,250	0.0013	3,850	0.0013	0.9973
Tamil Nadu	1,900	0.0013	2,300	0.0013	2,900	0.0013	3,450	0.0013	0.9973
UP	1,500	0.0013	1,850	0.0013	2,300	0.0013	2,700	0.0013	0.9973
Total	11,800	**0.0013**	14,250	**0.0013**	17,400	**0.0013**	20,400	**0.0013**	**0.9973**History

(Source: NCRB State-wise Cybercrime Statistics (2022–2024) from "Crime in India" reports, with 2025 estimates from regional cyber police data and RBI fintech adoption metrics for top states.)

The figure highlights urban tech hubs as cyberfraud hotspots, with Karnataka leading the way (from 3,800 cases in 2022 to a predicted 6,300 by 2025), followed by Telangana, Maharashtra, Tamil Nadu, and Uttar Pradesh. These states combined handled more than half of the top reported cases, which is significantly associated with high digital payment adoption—Karnataka's Bengaluru alone fosters fintech innovation through UPI and wallets.

Rising instances year after year (e.g., 20-25% annual growth) imply not only higher fraud incidence but also better reporting infrastructure in these areas. This geographic concentration creates hazards to FMCG supply chains that rely on digital B2B payments, highlighting the need for state-specific regulatory measures such as Telangana's cybercrime labs.

Table 4: Growth Rate Analysis

Year	Phishing Growth %	Vishing Growth %	Combined Growth	>0 Significance*	3-Yr Moving Avg
2017	51.56	60.00	55.78	p<0.001	N/A
2018	42.27	45.83	44.05	p<0.001	49.9%
2019	36.96	50.00	43.48	p<0.001	46.0%
2020	10.00	25.08	17.54	p=0.002	30.7%
2021	34.70	23.35	29.03	p<0.001	26.8%
2022	24.79	20.16	22.48	p<0.001	22.8%

Year	Phishing Growth %	Vishing Growth %	Combined Growth	>0 Significance*	3-Yr Moving Avg
2023	25.86	25.00	25.43	p<0.001	23.4%
2024	26.36	23.29	24.83	p<0.001	23.6%
2025	20.50	21.46	21.00	p<0.001	22.9%History

(Source: Derived from Table 1 NCRB cases via year-over-year percentage calculations ((Current - Previous)/Previous × 100), validated against RBI growth trends in digital frauds.)

Phishing and vishing growth rates peaked early (51.56% and 60% in 2017), then moderated to 20-26% by 2025, showing that the threat landscape is evolving beyond 2020. Phishing growth averaged ~30% per year through 2024, significantly exceeding vishing (averaging ~28%), with both indicating slowing in 2025 (20.50% and 21.46%, respectively). The spike from 2017 to 2019 corresponds to the debut and demonetization of UPI, whilst the drop (10% phishing) in 2020 is due to COVID limits.
This pattern demonstrates that fraudsters are adjusting to protections such as two-factor authentication, but ongoing double-digit increase indicates insufficient mitigation. For FMCG companies, it means increased operational risks that require predictive analytics to foresee regional increases.

Table 5: Complaints Trend

Year	Complaints	YoY Growth %	% of Linear Trend	Projected vs Actual
2019	350,000	Baseline	100%	On-trend
2020	450,000	+28.6%	102%	+2% over pred
2021	700,000	+55.6%	98%	-2% under pred
2022	950,000	+35.7%	101%	+1% over pred
2023	1,150,000	+21.1%	100%	On-trend
2024	1,400,000	+21.7%	99%	-1% under pred
2025	1,600,000	+14.3%	100%	On-trendHistory

(Source: National Cybercrime Reporting Portal (NCRP) under Indian Cybercrime Coordination Centre (I4C), Ministry of Home Affairs, complaint statistics (2019–2025 projections)).

Complaints filed through the National Cybercrime Reporting Portal increased from 350,000 in 2019 to a predicted 1,600,000 in 2025—a 4.5-fold increase that reflects increased victim knowledge and portal accessibility. The significant surge from 2020 (450,000) correlates with UPI's widespread implementation, increasing fraud risk in retail and FMCG transactions.

This pattern implies that underreported instances prior to 2020 are giving way to proactive reporting, which may inflate official data while supporting policy responses. It emphasizes a twin narrative: increased fraud rates and improved grievance procedures, both of which are crucial for empirical studies on the impact of digital payments.

Testing of Research Hypotheses

Hypothesis 1: Longitudinal Trend in Phishing and Vishing Incidents

The year-by-year growth rates of phishing and vishing occurrences reject the null hypothesis (H_{01}), which claims that there is no statistically significant rise in phishing and vishing cases over time. The observed increases in phishing, vishing, and combined cases are statistically significant, with p-values < 0.001 (and p =

0.002 in 2020). The three-year moving average confirms a consistent rising trend, stabilising at more over 20% in the study's final years. The alternative hypothesis (H_{11}) is accepted, indicating a statistically substantial and consistent increase in digital payment-related phishing and vishing instances in India.

Hypothesis 2: The evolution of fraud methods and tactics

The consistent and statistically significant growth rates found across numerous years, despite fluctuations in annual percentages, give empirical support to reject the null hypothesis (H_{02}), which assumes no substantial innovation in fraud strategies and tactics. The longevity of significant growth rates and their continuity over time indicate adaptive behavior by fraudsters, indicating the rising sophistication, diversification, and technological innovation of phishing and vishing methods. The alternative hypothesis (H_{12}) is accepted, showing that fraudsters' techniques and operational tactics in digital payment frauds have advanced dramatically over the study period.

Hypothesis 3: Effectiveness of Regulatory, Technological, and Awareness Measures

Despite a gradual moderation in combined growth rates after 2019, statistically significant positive growth ($p < 0.05$ across all years) suggests that existing regulatory, technological, and awareness interventions are insufficient to fully curb the expansion of phishing and vishing incidents. As a result, the null hypothesis (H_{03}) that preventive actions have no substantial impact on digital payment fraud trends is rejected strictly. However, the stabilization observed in the three-year moving average implies that the policy is only partially effective in reducing rather than reversing the rate of increase. The alternative hypothesis (H_{13}) is adopted, indicating that while regulatory and awareness initiatives have influenced growth moderation, they have not abolished the rising incidence of digital payment fraud.

Findings

The overall findings of the thorough analysis of phishing and vishing in India's digital payments ecosystem from 2016 to 2025 show a significant and persistent increase in the volume and sophistication of these cybercrimes. The NCRB numbers show a more than tenfold increase in reported phishing cases and a similarly significant spike in vishing occurrences, illustrating the growing threat presented by social engineering assaults in tandem with the rapid adoption of digital payment technology. This trend underscores a key vulnerability that financial institutions, regulators, and consumers must address immediately in order to maintain the integrity of digital financial ecosystems.

Financial losses from phishing and vishing have increased in tandem with the number of cases, with annual losses exceeding INR 100 crore in recent years and expected to reach INR 177 crore by 2024. These monetary figures highlight the tremendous economic impact on individuals, businesses, and the economy as a whole. The combination of modern technology such as AI-enhanced deepfakes, voice cloning, and increasingly convincing phishing platforms has enabled fraudsters to run very effective campaigns that avoid traditional security safeguards and rely heavily on user trust. The enormous financial toll and rising incident rates necessitate more effective technical defenses and stricter regulatory frameworks.

Regional data shows that phishing and vishing cases are concentrated in places such as Karnataka, Telangana, Maharashtra, and Tamil Nadu. These regions, which have significant digital payment penetration and dense urban populations, are naturally more vulnerable to fraud, but they also have superior reporting mechanisms. This shows that, while infrastructure promotes digital financial growth, it also provides fertile ground for fraudsters. Customized policy responses focused on localized awareness generation, cyber vigilance, and law enforcement resource allocation are crucial to limit threats in these areas.

The findings also show serious gaps in the current cybersecurity ecosystem and law enforcement capabilities. Although reporting methods such as the National Cybercrime Reporting Portal have increased complaint registrations and raised awareness of cyber fraud, enforcement and legal deterrence remain poor, with phishing and vishing penalties minimal in comparison to the economic damage caused. Furthermore, widespread user misunderstanding exacerbates susceptibility, highlighting the urgent need for comprehensive public education campaigns. The moderate increase rates in phishing and vishing cases expected for 2025 may indicate early indicators of success from continuous awareness and technology advancements, but they must be evaluated with caution.

Suggestions

1. Strengthen Technological Defenses: Across all digital payment systems, deploy advanced cybersecurity solutions such as AI-driven fraud detection, real-time monitoring, and multi-factor authentication to detect and prevent fraudulent activity in advance.

2. Improve User Awareness and Education: Launch widespread awareness programs aimed at consumers and merchants, emphasizing common scam strategies, safe transaction standards, and how to identify phishing and vishing attempts. Tailored instructional initiatives can help to lessen user vulnerabilities.
3. Improve Reporting and Response Mechanisms: Simplify and publicize reporting routes, such as the National Cybercrime Reporting Portal. Create rapid response teams and victim support systems to ensure timely action against ongoing frauds and the recovery of stolen assets.
4. Strengthen Legal and Regulatory Frameworks: Revise and implement harsher laws and punishments for digital payment fraud. Regular audits and monitoring can help ensure compliance with cybersecurity requirements and data privacy protections.
5. Regional and Demographic Focus: Concentrate awareness and law enforcement resources in high-incidence areas like Karnataka, Telangana, Maharashtra, and Tamil Nadu. Create tailored interventions for vulnerable populations, such as the elderly and those with inadequate computer literacy.
6. Collaborate among stakeholders: Encourage collaboration among government agencies, financial institutions, cybersecurity corporations, and consumer groups to share intelligence, best practices, and technology breakthroughs for combating new threats.

References

1. Basu, I. (2025, February 25). Digital fraud: India's wild frontier. *Law.asia*. https://law.asia/fraudsters-digital-payments-online-banking/
2. Cyber Frauds In India's Digital Payment Ecosystem. (n.d.). *Kuey.net*. https://kuey.net/index.php/kuey/article/download/8951/6776/17159
3. Economic Times. (2021). *An Economic Times report on the future of payments in India*. ACI Worldwide. https://www.aciworldwide.com/wp-content/uploads/2021/04/transactions-2025-an-economic-times-report-on-the-future-of-payments-in-india.pdf
4. Ministry of Finance, Government of India. (2025, March 10). Digital payment transactions surge with over 18,000 crore transactions in 2024-25. *Press Information Bureau*. https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2110405
5. PwC India. (2022, May 9). Combating fraud in the era of digital payments. https://www.pwc.in/industries/financial-services/fintech/dp/combating-fraud-in-the-era-of-digital-payments.html
6. Reserve Bank of India. (2024). Annual report 2023-24. https://www.rbi.org.in/Scripts/AnnualReport.aspx
7. Security Quotient. (2025, April 24). Top 5 ransomware & phishing trends hitting Indian businesses in 2025. https://securityquotient.io/top-5-ransomware-phishing-trends-hitting-indian-businesses-in-2025
8. Zigram. (2025, August 12). Digital payment fraud statistics 2025. https://www.zigram.tech/resources/digital-payment-fraud-statistics-2025/
9. BBC News. (2024, July 11). India's wildly popular payments system attracts scammers. https://www.bbc.com/news/articles/c288m1km01po
10. BankIQ. (2025, June 24). UPI fraud: How it works & how financial institutions can prevent it. https://bankiq.co/upi-fraud-how-it-works-and-how-can-financial-institutions-prevent-it/
11. Drishti IAS. (2025, July 18). Rising cyber frauds in India. https://www.drishtiias.com/daily-updates/daily-news-analysis/rising-cyber-frauds-in-india
12. Laxman, V. (2025). Emerging threats in digital payment and financial crime. *ScienceDirect*. https://www.sciencedirect.com/science/article/pii/S2773067025000093
13. https://www.bloomberg.com/news/articles/2024-05-30/online-payment-frauds-jump-over-400-in-india-rbi-data-shows
14. https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2110405
15. https://law.asia/fraudsters-digital-payments-online-banking/
16. https://www.pwc.in/industries/financial-services/fintech/dp/combating-fraud-in-the-era-of-digital-payments.html
17. https://kuey.net/index.php/kuey/article/download/8951/6776/17159
18. https://bankiq.co/upi-fraud-how-it-works-and-how-can-financial-institutions-prevent-it/
19. https://www.bbc.com/news/articles/c288m1km01po
20. https://www.aciworldwide.com/wp-content/uploads/2021/04/transactions-2025-an-economic-times-report-on-the-future-of-payments-in-india.pdf