Safer Internet Lab

Research report

Online Fraud and Scams in India

Safer Internet Lab

ONLINE FRAUD AND SCAMS IN INDIA

Safer Internet Lab

A Research Report by Safer Internet Lab

The views expressed here are solely those of the author(s) and do not represent an official position of SAIL, CSIS, Google, or any other organization. Please contact the author(s) directly with any comments or questions.

Online Fraud and Scams in India

Tuhinsubhra Giri[4]

BACKGROUND AND CONTEXT

The Rise of GenAI Online Scams and Implications

The digital revolution has ushered in an era where artificial intelligence (AI) is being weaponized by cybercriminals with alarming sophistication. Generative AI tools, which were originally designed to enhance creative and professional workflows, are now being exploited to orchestrate complex scams that are increasingly difficult to detect. According to Europol's 2025 SOCTA report, AI-driven scams are rapidly expanding in scale and sophistication, with deepfake technology and AI-generated phishing campaigns emerging as major threats to global cybersecurity. These scams often involve impersonating trusted entities, such as corporate executives, government officials, political leaders, celebrities or even family members, to manipulate victims into transferring money or divulging sensitive information. For instance, in 2023, a multinational company in Hong Kong lost $25 million after an employee was deceived by a deepfake video call featuring digitally recreated colleagues (South China Morning Post, 2024). Similarly, in the United States, AI voice cloning scams have surged, with criminals replicating the voices of loved ones to fabricate emergencies and extort money (Belanger, 2023). These cases underscore the global reach and adaptability of AI-powered fraud, highlighting the urgent need for robust countermeasures.

The proliferation of AI-driven scams is fueled by the accessibility of advanced tools. Open-source AI models and affordable cloud computing have democratized the ability to create convincing deepfakes and automated phishing schemes. Cybercriminals no longer require extensive technical expertise; instead, they can leverage user-friendly platforms to generate fraudulent content at scale. This trend is particularly concerning in regions with high digital penetration but limited cybersecurity awareness. For example, in Southeast Asia, AI-generated investment scams have proliferated on social media, luring victims with promises of unrealistic returns (Interpol, 2023). The global nature of these scams also complicates enforcement, as perpetrators often operate across jurisdictions, exploiting gaps in international cooperation. As AI technology continues to evolve, the threat landscape will likely expand, making it imperative for governments, businesses, and individuals to stay ahead of these emerging risks.

GenAI Online Scams in India

India, with its rapidly expanding digital economy, has become a prime target for AI-driven scams. The country's internet user base surpassed 800 million in 2023, making it the second-largest online market globally after China (India Foundation, 2025). This, combined with the explosive growth of digital payments, has created fertile ground for cybercriminals.

According to data presented in Parliament, Unified Payments Interface (UPI) fraud cases surged by 85% in FY24, rising from 7.25 lakh in FY23 to 13.42 lakh in FY24, with many involving phishing links and OTP theft (CNBC TV18, 2024). While the Reserve Bank of India (RBI) has not attributed a specific percentage

[4] Assistant Professor of Economics, Christ University

of these to AI, the growing use of AI-generated phishing and impersonation tactics has been widely acknowledged by cybersecurity experts.

One of the most alarming trends is the use of deepfake technology to spread misinformation and perpetrate fraud. During the 2024 Indian general elections, AI-generated videos of politicians making false or misleading statements circulated widely, raising concerns about their impact on democratic processes (The Hindu, 2024).

Another prevalent scam involves AI voice cloning, where fraudsters replicate the voices of family members to fake emergencies and extort money. In one case reported in March 2024, a Delhi-based businessman transferred ₹10 lakh after receiving a call from someone mimicking his son's voice using AI (Times of India, 2024).

India's cybersecurity infrastructure, while improving, struggles to keep pace with these advanced threats. The Indian Computer Emergency Response Team (CERT-In) has issued multiple advisories warning about deepfake scams and AI-generated fraud, including CIAD-2024-0060, which outlines threats and countermeasures (CERT-In, 2024). However, enforcement remains difficult due to the cross-border nature of many fraud operations. Scam call centers targeting Indian victims have been traced to countries like Cambodia and Myanmar, where jurisdictional limitations hinder effective crackdowns (Free Press Journal, 2023).

India's legal framework also lacks AI-specific provisions. The Information Technology (IT) Act, 2000, while foundational for cybersecurity, does not explicitly address generative AI misuse. The Digital Personal Data Protection (DPDP) Act, 2023 introduces important safeguards for data privacy, but it does not directly regulate AI-generated content or deepfake fraud (Chitranshi, 2023). This regulatory lag underscores the urgent need for policy to combat the escalating threat of AI-driven scams.

The economic ramifications of AI-driven scams are profound, particularly in a country like India, where digital financial inclusion is a key driver of growth. Indian Cyber Crime Coordination Centre (I4C), which reported ₹10,319 crore lost to online frauds between April 2021 and December 2023 (Times of India, 2024). However, the indirect costs are equally concerning. Scams erode public trust in digital platforms, discouraging adoption and stifling innovation. Small businesses and rural users, who are critical to India's digital transformation, may revert to cash transactions out of fear of fraud, undermining the government's efforts to promote a cashless economy. Furthermore, financial institutions and fintech companies are forced to invest heavily in AI-based fraud detection systems, driving up operational costs that are eventually passed on to consumers. These economic disruptions highlight the urgent need for systemic solutions to safeguard India's digital ecosystem.

AI-driven scams inflict significant social harm. Victims often experience psychological trauma, including anxiety, depression, and a lasting loss of trust in digital interactions. The societal impact is exacerbated by the targeting of vulnerable groups, such as the rural-urban digital divide, the elderly, and less tech-savvy individuals, who are disproportionately affected by voice cloning and phishing scams. Moreover, the spread of AI-generated misinformation, such as deepfake political content, threatens social cohesion and democratic processes. The erosion of trust in institutions, from banks to government agencies, poses a long-term challenge that extends beyond immediate financial losses.

India’s Digital Landscape and Cybersecurity Vulnerabilities

India has experienced rapid digital transformation, driven by initiatives such as Digital India and the widespread adoption of the Unified Payments Interface (UPI). However, this digital expansion has also exposed the country to significant cybersecurity risks, including AI-driven fraud.

Some of the major Cybersecurity Vulnerabilities in India include;

- **Rise in AI-Powered Cyberattacks**

  A recent study indicates that 72% of Indian organizations have been targeted by AI-driven cyberattacks, including deepfake impersonation, phishing scams, and credential stuffing attacks (Free Press Journal, 2025; SME Futures, 2025).

- **Financial Fraud and Deepfake Scams**

  AI-enabled financial scams have reportedly caused losses exceeding ₹20,000 crore in 2024–25, with cybercriminals using deepfake videos to impersonate public figures and promote fake investment schemes (The Logical Indian, 2025).

- **Weak Cybersecurity Infrastructure**

  Despite progress in cybersecurity adoption, only 14% of Indian firms feel confident in defending against AI-based threats, while 36% say these threats surpass their existing detection tools (SME Futures, 2025).

- **Lack of AI-Specific Regulations**

  India’s legal framework, including the Information Technology Act of 2000, does not fully address the challenges posed by AI-generated fraud. The country lacks comprehensive laws focused on generative AI misuse and cross-border enforcement (LawArticle, 2025).

Technology Adoption Lifecycle & The Evolution of AI-Driven Scams

AI-driven scams evolve in tandem with the Technology Adoption Lifecycle.

- This process begins in fringe cybercrime circles before scaling into mainstream fraud tactics.
- As tools become easier to use, the early majority phase sees mass deployment of phishing bots and synthetic identity fraud.
- In the late majority phase, scams become widespread, prompting institutional countermeasures.

This progression mirrors the disruptive innovation model, where new AI-enabled fraud replaces conventional tactics. A prime example is how AI-generated investment scams have overtaken manual Ponzi schemes, thanks to their scalability and realism.

The fraud tactics have evolved significantly over the past decade (see annex A). Before 2018, scams relied on basic impersonation calls, generic phishing emails, and Ponzi schemes. However, from 2019 onward, AI has revolutionized financial fraud—deepfake videos now impersonate trusted figures, AI-generated phishing messages exploit personal data, and synthetic identities automate loan fraud. Scams have become hyper-realistic, scalable, and harder to detect, with AI enabling real-time deception through chatbots, cloned customer support, and fake e-commerce sites. The shift from human-led cons to AI-driven fraud underscores the urgent need for advanced detection tools and regulatory frameworks to combat these sophisticated threats. How Generative AI can be used or exploited to facilitate or enhance each scam can be seen in Annex B.

PATTERNS AND TRENDS OF GEN AI-DRIVEN ONLINE SCAMS IN INDIA

The Digital Surge and Its Dark Underside

India's rapid digital transformation, fueled by Digital India, UPI, and Aadhaar-based services, has inadvertently created new vulnerabilities for Generative AI-driven scams. Fraudsters now exploit AI to generate synthetic identities, bypassing traditional verification systems. AI-generated fake Aadhaar and PAN cards are being used to access financial services fraudulently, leading to unauthorized loans and identity theft (Economic Times, 2024). Additionally, deepfake technology enables real-time impersonation, allowing scammers to mimic bank officials or government representatives in video calls to deceive victims into transferring money. The Aadhaar-enabled Payment System (AePS) has seen a rise in fraud cases, with Aadhaar breaches in land records contributing to the surge in AePS fraud, exploiting fingerprint cloning and duplicate biometric records (Medianama, 2024).

The widespread adoption of UPI has also made AI-powered scams more sophisticated. Reports indicate that 55% of digital payment frauds in India are linked to UPI, with AI-driven phishing attacks targeting unsuspecting users (Business Standard, 2023). Fraudsters use AI-generated voice cloning to impersonate family members in distress, coercing victims into sending money. AI-powered chatbots further automate scam operations, responding dynamically to victims' queries and making fraudulent schemes appear more legitimate. As AI tools become more accessible, scams are evolving beyond simple phishing attempts into highly personalized fraud campaigns, making detection increasingly difficult. Without stronger AI-specific regulations, India's digital economy remains vulnerable to large-scale financial fraud.

Recent Statistics of Financial Losses and Reported Cases (2020-2025)

India has witnessed a dramatic surge in cybercrime over the past five years, driven by increased digital adoption and the proliferation of AI tools. According to the Future Crime Research Foundation (FCRF), online financial fraud accounted for 77.41% of all cybercrime cases reported between January 2020 and June 2023, making it the most dominant category of cybercrime in India[5].

Another major problem with this is that the rapid digitalisation of the economy also attracts this kind of scam and problems. Cybercrime cases themselves are not very old, Gen AI-related online scams are quite new in comparison. But there is a problem with the availability of data for this problem. Some data on cybercrime is available, but not segregated as Gen AI related financial scams. Though this is one type of Cybercrime, so data on cybercrime can definitely give us some idea about the increasing number of Gen AI-related financial scams.

Table 3.1 Number of Cybercrime Cases and Estimated Financial Loss Over the Period 2020-2024

Year	Reported Cybercrime Cases	Estimated Financial Loss (₹ crore)	Source
2020	50,035	1,785	Economic Times, 2024
2021	52,974	2,096	Statista, 2024
2022	65,893	3,192	Business Standard, 2024

[5] https://the420.in/fcrf-cybercrime-report-india-77-percent-online-financial-fraud/

2023	76,630	4,820	Times of India, 2024
2024 (est.)	89,000+	6,500+	Medianama, 2024

Between January and April 2024, India recorded over 740,000 cybercrime complaints, as reported by the Indian Cyber Crime Coordination Centre (I4C). This marks a significant increase compared to previous years, with cybercrime cases surging between 2019 and 2020 and continuing to rise steadily. Notably, approximately 85% of these complaints in 2024 were linked to online financial fraud, including investment scams, illegal lending apps, and phishing attacks (Statista, 2024).

Cross-Border Scam Activities and India's Exposure

India is increasingly vulnerable to transnational AI-driven scams, especially those involving cryptocurrency, investment fraud, and identity theft. These scams often originate from jurisdictions with weak enforcement and exploit global platforms like WhatsApp, Telegram, and fake websites.

- Cross-border UPI frauds and SIM swap attacks have been traced to Southeast Asia and Eastern Europe.
- AI-generated deepfakes are used to bypass KYC protocols, enabling money laundering and mule account creation
- According to CloudSEK, brand impersonation and cross-border phishing campaigns are among the top threats to Indian financial institutions.

India's regulatory and enforcement agencies, including CERT-In, RBI, and NCRB, are increasingly collaborating with global cybersecurity firms to track and mitigate these threats. However, the lack of harmonized international frameworks continues to hinder effective prosecution and recovery. India is a prime target for transnational AI fraud networks, with 70% of scam calls originating from Cambodia, Myanmar, and Laos[6].

Table 3.2 Transnational Scam Operations Targeting Indian Victims in Recent Times

Country	Scam Particulars	Primary Scam Types	Indian Victims	Source
Cambodia	100,000 scammers generating an estimated $12.8 billion in 2013	AI Voice Cloning, Fake Job Scams	More than 5,000	Voanews, Indiana-express
Myanmar	About 120,000 individuals being forced into scamming in Myanmar in the last year	Invest-ment Frauds, Romance Scams	549 Indians were freed from cybercrime centres in Myanmar-Thailand border	BBC, Hindu-stantimes
Laos	306 call centers or fraud units are identified in SEZs	UPI Fraud, Fake Customer Support	To date, 924 Indian nationals have been rescued	Laotian-times

[6] https://laotiantimes.com/2024/10/29/india-faces-rising-digital-scams-linked-to-laos-myanmar-cambodia/

China	Transnatio-nal Criminal networks from China dominate Southeast Asia's gambling and scam operations	Deepfake Video Scams, Loan Frauds	The NIA reports that many Indians were recruited via fraudulent job ads and compelled to work under coercive contracts	Usip, Indiato-day

Source: Author's compilation

Southeast Asia has become a major hub for transnational scam operations. As we can see from Table above that, in Cambodia alone, 100,000 scammers generated an estimated $12.8 billion in fraudulent activity, nearly half the country's GDP. Myanmar's scam networks, often linked to criminal syndicates, force over 120,000 individuals into scams such as crypto fraud and romance-investment scams, with 549 Indians rescued from cybercrime centres near the Thai border. Laos' Golden Triangle Special Economic Zone hosts 306 scam units, where Indian nationals are trafficked into forced cyber fraud-924 Indians have been rescued to date. Many times, China's networks dominate global gambling and online fraud, with $64 billion stolen annually, as syndicates exploit a $40-$80 billion market. Reports indicate many more scams remain unaccounted for, highlighting the urgent need for cross-border regulatory enforcement and digital fraud prevention strategies.

Case Studies

CBI's Operation Chakra-V (2025)

Operation Chakra-V, launched by the Central Bureau of Investigation (CBI) in 2025, marked a significant milestone in India's fight against cyber-enabled financial fraud. The operation targeted an international cybercrime syndicate that exploited AI-driven scams, including spoofed caller IDs, deepfake impersonation, and voice cloning to deceive victims, primarily in the United States and Canada. Investigators uncovered fraudulent operations linked to tech-support scams, impersonation of government officials, and cryptocurrency laundering schemes. During coordinated raids across three locations in India, CBI seized ₹2.8 crore in cryptocurrency, ₹22 lakh in cash, and multiple fake digital identities, disrupting a complex fraud network.

Beyond financial fraud, Operation Chakra-V highlighted the growing role of AI in cybercrime and the urgent need for AI-specific cybersecurity regulations. The operation also strengthened international cooperation, with CBI working alongside Interpol and the FBI to trace global money trails. Following the arrests, India's cyber enforcement agencies intensified efforts to strengthen digital forensic capabilities and fraud detection frameworks. With AI-powered scams evolving rapidly, Operation Chakra-V underscores the importance of proactive cyber-defense strategies in safeguarding India's digital economy.

AI-Generated Flipkart Scam (2023)

The AI-Generated Flipkart Scam in 2023 exemplifies the growing sophistication of AI-driven cyber fraud in India's digital economy. Fraudsters leveraged generative AI to clone Flipkart's website, creating a near-identical replica that deceived thousands of unsuspecting shoppers. By running fake discount campaigns, scammers lured over 30,000 victims into purchasing non-existent products, leading to an estimated ₹120 crore in financial losses. The scam exploited AI-generated phishing tactics, including automated customer service bots and deepfake promotional videos, making detection difficult until significant damage had been done.

This case highlights the urgent need for AI-specific cybersecurity regulations and enhanced fraud detection mechanisms. As AI tools become more accessible, cybercriminals are increasingly using synthetic identities, deepfake impersonation, and automated scam operations to bypass traditional security measures. The Flipkart scam underscores the importance of digital literacy, real-time fraud monitoring, and stricter e-commerce verification protocols to protect consumers from AI-enabled deception.

The Cambodia Cyber Scam Factories (2023)

In 2023, a major cyber scam operation in Cambodia exposed the forced involvement of Indian nationals in fraudulent online schemes. According to reports, over 5,000 Indians were coerced into working in scam centers, where they were made to conduct online fraud, including money laundering, crypto scams, and romance fraud. Victims were initially lured with fake job offers, only to find themselves trapped in illegal cyber operations upon arrival.

The Indian government intervened, successfully rescuing 250 citizens and working closely with Cambodian authorities to crack down on the scam networks. The case highlights the growing transnational nature of cyber fraud, where AI-driven deception tactics—such as deepfake impersonation and automated phishing—are increasingly used to exploit victims. It also underscores the urgent need for international cooperation and AI-specific cybersecurity regulations to prevent such large-scale fraud operations.

IMPLICATIONS OF ONLINE FRAUD AND SCAMS

Financial Impact on Individuals, SMEs, and the Economy

AI-driven online scams have inflicted significant financial damage across all segments of Indian society. According to a 2025 report by The Logical Indian[7], India is projected to lose over ₹20,000 crore to AI-enabled scams in a single year, with deepfake investment frauds and impersonation scams being the primary culprits. These scams often impersonate public figures like Finance Minister Nirmala Sitharaman or Google CEO Sundar Pichai to promote fake investment platforms, leading to widespread deception and monetary loss.

For individuals, especially those with limited digital literacy, the financial consequences can be devastating. Victims often lose life savings or emergency funds, with little recourse for recovery. Small and medium enterprises (SMEs) are also vulnerable, particularly to phishing attacks and synthetic identity fraud. A study by Experian and Forrester Consulting found that 64% of Indian financial institutions reported increased fraud losses in 2024, with synthetic identity fraud being the most prevalent[8].

At the macroeconomic level, the cumulative effect of these scams undermines investor confidence, increases cybersecurity costs, and diverts resources from productive sectors. These kind of Gen AI Online scams leads to business disruptions, intellectual property theft, and increased expenditure on fraud prevention, all of which hamper economic growth.

[7] https://thelogicalindian.com/india-faces-%E2%82%B920000-crore-cybercrime-threat-in-2025-amid-surge-in-ai-driven-deepfake-investment-scams/

[8] https://www.experian.in/2024/02/11/financial-frauds-rise-in-india-as-genai-gains-traction/

Psychological and Social Impact

The psychological toll of AI-driven scams is often overlooked but deeply consequential. Victims experience a range of emotional responses, including shock, anxiety, shame, and depression. A 2023 article in The Times of India[9] highlights how deepfake scams and voice cloning can cause lasting mental distress, especially when victims are manipulated into believing a loved one is in danger.

The emotional manipulation involved in AI scams—such as receiving a cloned voice call from a family member in distress—can lead to trauma and long-term distrust. Victims often suffer from self-blame, fear of future scams, and social withdrawal, particularly when the scam involves sextortion or impersonation. These effects are compounded in cases involving adolescents or the elderly, who may lack the tools or support systems to recover emotionally.

Digital Trust Erosion in Financial Institutions and E-Commerce Platforms

AI scams have significantly eroded public trust in digital platforms. These scams not only cause financial loss but also undermine the credibility of financial institutions and e-commerce platforms.

A survey by Finextra found that 63% of Indian consumers have either fallen victim to a scam or know someone who has, leading many to reduce their use of digital payment platforms[10]. This erosion of trust has broader implications: it slows down digital adoption, increases reliance on cash transactions, and hampers the growth of India's fintech ecosystem.

Consumer behaviour is also shifting. According to FICO's 2025 India Fraud Report, users are becoming more cautious, often avoiding online transactions or demanding additional verification steps. While this may enhance security, it also reduces the convenience and efficiency that digital platforms are designed to offer.

Government and Institutional Regulatory Responses

The surge in AI scams has forced policymakers to accelerate regulatory reforms. Some of the key actions include:

- **Digital Personal Data Protection Act (DPDP), 2023** – Introduces penalties for misuse of personal data in AI fraud but lacks specific provisions on deepfakes.
- **RBI's AI Fraud Prevention Guidelines (2024) –** Mandates banks to deploy AI-based deepfake detection and multi-factor authentication for high-risk transactions.
- **Interpol-India Collaboration** – Targeting offshore scam hubs in Cambodia and Myanmar, leading to 50+ arrests in 2024.

[9] https://timesofindia.indiatimes.com/life-style/health-fitness/health-news/the-deep-impacts-of-deepfakes-and-cyber-fraud-on-mental-health/articleshow/106145692.cms

[10] https://www.finextra.com/blogposting/27108/digital-arrest-a-new-frontier-in-cybercrime-and-its-ripple-effects-on-consumer-trust

Table 3.3 Sectoral Impact-Who Is Being Targeted?

Sector	Primary AI-Driven Threats	Impact
Banking & Fintech	Deepfake investment scams, synthetic identity fraud	Loss of consumer trust, regulatory fines
Retail & E-Commerce	Fake websites, chatbot impersonation	Brand damage, customer losses
Government Services	Deepfake impersonation of officials	Public misinformation, reputational harm
Telecom	Phishing via SMS/WhatsApp	SIM swap fraud, identity theft

Other than the individual level impact, AI-driven scams have significantly impacted critical industries, eroding trust, financial stability, and operational integrity. From the table 4 above, we can see that the banking and fintech sector faces rising fraud cases through deepfake investment scams and synthetic identity fraud, forcing tighter regulatory oversight. Retail and e-commerce platforms suffer brand damage and customer losses due to fake websites and chatbot impersonation, making digital trust harder to maintain. In government services, deepfake impersonation of officials fuels public misinformation, threatening policy credibility. Meanwhile, the telecom sector experiences phishing attacks via SMS and WhatsApp, leading to SIM swap fraud and identity theft, amplifying security concerns across digital transactions. These sectoral vulnerabilities demand AI-specific cybercrime laws, rules, regulations, and robust AI-driven fraud detection strategies and heightened consumer awareness initiatives.

KEY STAKEHOLDERS IN ADDRESSING AI-DRIVEN SCAMS IN INDIA

The rise in AI-driven scams has prompted not only government, but also other stakeholders to launch initiatives aimed at addressing scams. Below is an overview of the key actors and their efforts to address online fraud and scams in India.

Government Bodies

Government agencies play a pivotal role in regulating, preventing, and mitigating AI-driven scams.

Stakeholder	Key Responsibilities	Recent Actions (2023-24)
CERT-In (Indian Computer Emergency Response Team)	• National nodal agency for cybersecurity threats • Issues alerts on AI scams • Coordinates with ISPs to block fraudulent domains	• Launched AI-powered scam tracking system (2024) • Reported 12,000+ deepfake fraud cases in 2023
Ministry of Electronics & IT (MeitY)	• Formulates AI and cybersecurity policies • Regulates digital platforms	• Released AI Ethics Guidelines (2024) • Proposed ban on malicious deepfakes
Reserve Bank of India (RBI)	• Safeguards financial systems from AI fraud • Mandates fraud detection for banks	• Introduced AI-based UPI fraud detection (2024 • Reported ₹23,000 crore in AI banking scams (2023)
Securities and Exchange Board (SEBI)	• Prevents stock market fraud via AI • Monitors fake investment schemes	• Banned 350 AI-powered trading scams (2024)

Private Sector Participation

Private companies, especially in fintech and telecom, are crucial in detecting and preventing scams.

Sector	Key Players	Anti-Scam Measures
Fintech & Digital Payments	Paytm, PhonePe, NPCI	• AI-based transaction anomaly detection • Real-time fraud alerts via SMS/email
Telecom Providers	Jio, Airtel, Vodafone-Idea	• AI call monitoring to flag scam numbers • Blocked 10M+ spam calls monthly (TRAI, 2024)
E-Commerce & Social Media	Flipkart, Amazon, Meta	• Deepfake detection algorithms • Verified seller programs

Tech & AI Companies

Global tech giants and Indian startups are deploying AI to counter AI-driven fraud.

Company	Role in Scam Prevention	Key Initiatives
Google	• Detects phishing sites • Flags scam ads	• Deepfake watermarking in Google Search
Microsoft	• Azure AI for fraud detection • Secure digital identities	• AI voice clone detection for banks
Indian Startups (e.g., SigTuple, RazorpayX)	• AI-based KYC fraud prevention • Scam pattern recognition	• Reduced fraud by 40% in partner banks (2024)

Law Enforcement & Cybersecurity Firms

Cybercrime units and cybersecurity firms track and dismantle scam operations.

Agency/Firm	Function	Notable Cases (2023-24)
Indian Cyber Crime Coordination Centre (I4C)	• Tracks transnational scam networks • Trains police in AI fraud detection	• Busted Cambodia-based AI call center scamming Indians
Delhi/Mumbai Cyber Cells	• Investigates financial fraud • Recovers stolen funds	• Solved ₹5.7 crore AI voice scam (2023)
Cybersecurity Firms (e.g., Kaspersky, Quick Heal)	• Develop AI scam detection tools • Provide threat intelligence	• Blocked 5M+ phishing attempts in India (2024)

POLICY ASSESSMENT

Existing Laws & Regulations

India has several legal frameworks addressing cybersecurity and financial fraud, but they lack AI-specific provisions. The following laws and regulations play a role in mitigating online scams.

Information Technology (IT) Act, 2000 and Amendments

The IT Act, 2000 is India's primary legislation governing cybercrime and electronic commerce. It provides legal recognition for digital transactions and penalizes cyber fraud. However, the Act does not explicitly address AI-driven scams, deepfake fraud, or synthetic identity manipulation. Amendments have been made to strengthen cybersecurity, but AI-driven fraud detection remain absent.

RBI Guidelines on Financial Fraud

The Reserve Bank of India (RBI) has issued multiple guidelines to combat financial fraud, including:

- Master Directions on IT Governance (2023), which mandate banks and financial institutions to adopt AI-driven fraud detection systems.
- Cybersecurity Framework for Banks, requiring real-time monitoring of digital transactions.
- Guidelines on Digital Lending, aimed at preventing fraudulent loan applications using synthetic identities.

Despite these measures, AI-powered scams continue to exploit loopholes in digital banking security.

Consumer Protection Laws Relevant to Digital Transactions

The Consumer Protection Act, 2019 and the Digital Personal Data Protection Act, 2023 provide safeguards against fraudulent digital transactions. The Central Consumer Protection Authority (CCPA) oversees deceptive practices, but enforcement against AI-generated scams remains weak. AI-generated misinformation and fraudulent e-commerce platforms often bypass existing consumer protection mechanisms.

Challenges

Despite existing regulations, several challenges hinder effective enforcement against AI-driven scams.

a) **Broader definitions of scams to cover AI-driven**

India lacks dedicated AI-driven scams provisions in the existing law to regulate deepfake fraud, AI-generated phishing, and synthetic identity scams. While the IndiaAI Mission (2024) aims to develop ethical AI frameworks, it does not directly address AI-driven cybercrime. The absence of AI-specific liability frameworks makes it difficult to prosecute fraudsters using AI tools. There is a need to incorporate AI-driven scams in the under the current IT Act.

b) **Limited Cross-Border Enforcement Mechanisms**

AI-driven scams often originate from international cybercrime syndicates, making enforcement difficult. India's cybercrime laws do not have strong cross-border provisions, limiting cooperation with global agencies. The lack of extradition treaties for cybercriminals further complicates prosecution. A huge number of AI scam operations are run from Cambodia, Myanmar, and Laos, as mentioned earlier. Mutual Legal Assistance Treaties (MLATs) with these countries are often slow, allowing scam networks to evade shutdowns.

c) **Inadequate Digital Literacy Among Users**

A major challenge in combating AI scams is low digital literacy. Only 38 percent of households in the country are digitally literate. Additionally, only 31 percent of the rural population uses the internet as compared to 67 percent of the urban population[11]. Many users are unaware of AI-driven fraud tactics, making them vulnerable to scams. Public awareness campaigns on AI fraud detection are needed to bridge this gap.

India's policy landscape for addressing AI-driven scams is evolving but remains fragmented and reactive. Strengthening IT Act by including AI-driven scams provisions, enhancing cross-border enforcement, and improving digital literacy are crucial steps toward mitigating AI-enabled fraud. The government must integrate AI governance frameworks into cybersecurity laws to ensure a proactive approach to fraud prevention.

Table 3.4. Comparative Policy Analysis of India and its Asia-Pacific Peers

Policy Aspect	India	China (Interim AI Measures, 2023)	Japan (AI Governance Guidelines, 2024)	Singapore (AI Verify Framework)	Australia (AI Ethics Principles)
AI Scam Definition	No explicit classification	Strict AI content labelling, bans unauthorized deepfakes	Ethical AI guidelines, voluntary compliance	AI risk-based classification	Ethical AI guidelines, no legal mandate
Cross-Border Cooperation	Limited MLAT effectiveness	Cybersecurity cooperation with ASEAN	International AI safety partnerships	ASEAN cybersecurity cooperation	International AI safety partner-ships
Public Awareness	Ad-hoc campaigns (e.g., Cyber Jaagrookta Diwas)	AI literacy in schools, public misinformation monitoring	AI ethics education on in universities	AI literacy initiatives	AI ethics education in universities

BEST POLICY PRACTICES FOR GENAI ONLINE SCAM PREVENTION

AI Transparency and Content Labelling

European Union – AI Act & Digital Services Act (DSA)

The EU mandates labelling of AI-generated content, bans high-risk applications like unauthorized deepfakes, and requires platforms to verify advertisers. Non-compliance can result in fines up to 6% of global revenue.

China – Interim Measures for Generative AI (2023)

Requires synthetic content to be labelled, prohibits impersonation without consent, and mandates that AI-generated content must not endanger national security or social stability.

Cross-Border Intelligence Sharing

Interpol & Europol Joint Task Forces

Facilitate real-time data exchange on transnational scams, including AI-enabled fraud. These platforms support coordinated takedowns and intelligence-led investigations.

[11] https://idronline.org/article/inequality/indias-digital-divide-from-bad-to-worse/

ASEAN Cybersecurity Cooperation

Southeast Asian nations collaborate on cross-border scam prevention, sharing threat intelligence and harmonizing digital fraud response protocols.

Public Awareness and Digital Literacy

Japan – AI Ethics in Education

Integrates AI literacy and scam awareness into school curricula and public campaigns to build early digital resilience.

Australia – eSafety Commissioner Initiatives

Runs national campaigns on deepfake awareness, scam reporting, and content takedown protocols, modelled on the Online Safety Act.

Private Sector and Regulatory Collaboration

United States – FTC & NIST AI Risk Management Framework

The U.S. Federal Trade Commission (FTC) uses AI to analyze consumer complaints and detect scam patterns. The NIST AI Risk Management Framework promotes red-teaming and stress-testing of AI systems to reduce vulnerabilities.

Google's Global Scam Policy Recommendations

Advocates for cross-sector collaboration, real-time scam intelligence sharing, and proactive takedown of malicious content. Google's pilot in Singapore blocked nearly 900,000 high-risk app installations.

AI-Specific Legal Frameworks

Singapore – Model AI Governance Framework & Anti-Scam Command (ASCom)

Combines real-time scam detection, mandatory SMS sender ID registration, and public-private coordination. Phishing losses dropped by 37% in 2023.

UK – Online Fraud Charter (2023)

Requires banks, telecoms, and tech firms to share fraud data within 24 hours, improving scam response time and consumer protection.

POLICY RECOMMENDATIONS

- **AI Scam Registry & Shared Intelligence Grid**

  Create a centralized fraud intelligence platform that banks, fintech firms, telecoms, e-commerce companies, and law enforcement can access. Patterned after the UK's National Fraud Database, it would enable real-time sharing of scam indicators like deepfake voiceprints, scam URLs, and synthetic identity hashes.

- **AI Media Provenance & Content Labeling Mandate**

  Introduce legislation requiring mandatory watermarking and cryptographic labeling of AI-generated images, videos, and voices. This will bolster public trust and help platforms automatically flag deceptive content before dissemination.

- **Sector-Specific AI Risk Certification for Platforms**

  Inspired by the U.S. NIST Framework, mandate that high-risk sectors (e.g., banking, telecom, digital advertising) undergo annual AI fraud risk audits, including red-teaming, explainability testing, and consumer impact simulations. CERT-In and RBI could co-lead certification.

- **AI Scam Literacy in Government Portals & Education**

  Integrate regional-language chatbot explainers about AI scams into key portals like MyGov, DigiLocker, and PMGDISHA. Simultaneously, embed scam resilience modules into CBSE/NCERT digital literacy curriculum.

- **National Rapid Takedown Protocol**

  Enact a cross-sector protocol requiring platforms to takedown verified scam content (e.g., deepfake investment ads) within 6 to12 hours of verified flagging by I4C, CERT-In, or RBI. This protocol can emulate Australia’s eSafety takedown standard.

- **National Scam Simulation Challenge**

  Launch an annual innovation challenge for universities, startups, and police academies to prototype:
  - Deepfake detection models
  - Real-time scam alert apps
  - Local-language scam literacy games

  Winners could receive funding and regulatory fast-tracking for national deployment, catalyzing homegrown, scalable scam-tech solutions.

- **Establish a Cross-Border Generative AI Scam Intelligence Taskforce (GEN-SAFE*)***

  India should initiate or co-lead a multilateral taskforce called GEN-SAFE (Generative AI Scam and Fraud Exchange) in collaboration with ASEAN, Interpol, and select G20 digital economy members.

- **Public-Private Collaboration Frameworks**

  A National AI Scam Registry should be created as a unified database of scam signatures, integrating with banking systems, e-commerce platforms, and telecom providers.

- **Consumer Empowerment Initiatives**

  The government can launch a ScamScan app with UPI verification, deepfake detection, and one-click police reporting. A digital literacy offensive must make "AI Spotting" modules mandatory in schools and Digital India centers, while expanding the MyGov "FRAUD AI" chatbot that already served 2.1 million users in 12 languages during its pilot phase.

ANNEXES

Annex A. Evolution of Financial Scams in India – From Traditional to AI-Driven

Category	Traditional Financial Scams (Pre-2018)	AI-Driven Online Scams (2019–2025)	Key Changes
Impersonation Scams	Fake calls from bank officials or police demanding KYC updates or legal payments.	Deepfake videos and voice cloning of public figures (e.g., Finance Minister, Sundar Pichai) promoting fake investment platforms.	Shift from human-led deception to AI-generated hyper-realistic impersonation.
Phishing Attacks	Generic emails or SMS with suspicious links.	AI-generated personalized phishing emails and WhatsApp messages using NLP and behavioural data.	Enhanced targeting and believability due to AI's ability to mimic tone and context.
Investment Scams	Ponzi schemes, chit funds, or fake stock tips.	AI-generated fake websites and social media ads with deepfake endorsements for crypto or government bonds.	Use of generative AI to simulate legitimacy and scale outreach.
Loan & Credit Scams	Fake loan offers via SMS or calls.	AI-created synthetic identities used to apply for loans or open mule accounts.	Automation of identity fraud using AI-generated documents and profiles.
Customer Support Fraud	Fake helpline numbers or spoofed IVR systems.	AI chatbots mimicking bank or e-commerce support to extract OTPs and credentials.	Real-time AI interaction increases success rate of deception.
E-Commerce Fraud	Non-delivery of goods from fake websites.	AI-generated scam websites mimicking trusted brands with cloned UI and fake reviews.	AI enables rapid creation of convincing fraudulent storefronts.
Romance & Sextortion Scams	Fake dating profiles using stolen photos.	AI chatbots and deepfake avatars used to build emotional trust and extort money.	Emotional manipulation scaled through generative AI and voice cloning.
Cross-Border Fraud	Email lottery scams or Nigerian prince frauds.	Transnational AI scams using multilingual phishing, crypto laundering, and global mule networks.	AI enables cross-border scalability and evasion of local enforcement.

Annex B. Misuse of AI for Online Scams in India

Type of Scams	Cases in India	Source
Phishing scams	Indians receive an average of 12 fake messages per day, many impersonating banks or government agencies	The Hindu – AI-powered phishing surge in India
Investment fraud	Deepfake videos of Finance Minister Nirmala Sitharaman and Google CEO Sundar Pichai were	NDTV – False Endorsements, Real Losses

	used to promote fake crypto platforms like "InvestGPT."	
Fake job offers	A Chennai woman was targeted by an AI chatbot posing as a recruiter from "Flypside Global Services," offering a fake job via WhatsApp	PyLessons – Bot-Driven Job Scams
Loan app scams	RBI flagged over 1,200 fake loan apps in Q1 2025; victims were harassed and extorted after borrowing. Generative AI created fake content and deepfaked video 'loan officers' also being used for this kind of scams.	OneTouch Finance – Fake Loan App List
Deepfake scams	A 73-year-old man in Kerala lost ₹40,000 after a scammer used a deepfake video call to impersonate his former colleague. The scammer used AI-enabled deepfake technology to create a video call in which the impersonator's face and voice matched the victim's former colleague. This is the first reported case of a deepfake scam	Hindustan Times – Kerala Deepfake Scam
Online shopping fraud	In 2024, Indians lost over ₹11,000 crore to online fraud, including fake e-commerce sites using AI-generated product images and reviews	ET CIO – AI in Fintech Fraud Prevention
OTP and UPI scams	A Mumbai resident lost ₹95,000 in 3 minutes after sharing an OTP with a scammer posing as a bank official	Sprouts News – UPI Verification Scam
Romance scams	A Bengaluru woman lost ₹5.4 lakh to a scammer posing as an army officer on Tinder, who used emotional manipulation and AI-generated content	Media India – AI & Romance Scams
Fake digital arrest threats	A Mumbai professional was coerced into paying ₹50,000 after a scammer impersonated an income tax officer and threatened "digital arrest."	Union Bank of India – Digital Arrest Case
TRAI (Telecom Regulatory Authority of India) Impersonation Scam	An elderly woman in Chandigarh lost ₹2.5 crore after scammers impersonated TRAI and CBI officials, threatening to disconnect her phone number	Indian Express – TRAI Impersonation Scam

REFERENCES

Belanger, A. (2023, March 6). *Thousands scammed by AI voices mimicking loved ones in emergencies*. Ars Technica. https://arstechnica.com/tech-policy/2023/03/rising-scams-use-ai-to-mimic-voices-of-loved-ones-in-financial-distress/

Europol. (2025). *EU Serious and Organised Crime Threat Assessment (EU-SOCTA) 2025*. European Union Agency for Law Enforcement Cooperation. Retrieved from https://www.europol.europa.eu/publications-events/main-reports/socta-report

INTERPOL. (2023, December 8). *INTERPOL operation reveals further insights into 'globalization' of cyber scam centres*. Retrieved from https://www.interpol.int/en/News-and-Events/News/2023/INTERPOL-operation-reveals-further-insights-into-globalization-of-cyber-scam-centres

South China Morning Post. (2024, February 4). *'Everyone looked real': Multinational firm's Hong Kong office loses HK$200 million after scammers stage deepfake video meeting*. Retrieved from https://www.scmp.com/news/hong-kong/law-and-crime/article/3250851/everyone-looked-real-multinational-firms-hong-kong-office-loses-hk200-million-after-scammers-stage

CERT-In. (2024, March 8). *Advisory on threats posed by deepfakes powered by artificial intelligence and related countermeasures (CIAD-2024-0060)*. Indian Computer Emergency Response Team. https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2024-0060

CNBC TV18. (2024, June 5). *UPI fraud cases rise 85% in FY24 to 13.4 lakh: Parliament reply*. https://www.cnbctv18.com/business/finance/upi-fraud-cases-rise-85-pc-in-fy24-increase-parliament-reply-data-19514295.htm

Free Press Journal. (2023, October 24). *CERT-In issues advisory on AI-powered deepfakes, warns citizens of scammers using realistic tactics for financial fraud*. https://www.freepressjournal.in/mumbai/cert-in-issues-advisory-on-ai-powered-deepfakes-warns-citizens-of-scammers-using-realistic-tactics-for-financial-fraud

India Foundation. (2025, April 15). *Fortifying the digital frontier: Protecting India's cyber interests*. https://indiafoundation.in/articles-and-commentaries/fortifying-the-digital-frontier-protecting-indias-cyber-interests/

Chitranshi, S. (2023, September 7). The deepfake conundrum: Can the Digital Personal Data Protection Act, 2023 deal with misuse of generative AI? *Indian Journal of Law and Technolog*y (IJLT). https://www.ijlt.in/post/the-deepfake-conundrum-can-the-digital-personal-data-protection-act-2023-deal-with-misuse-of-ge

The Hindu. (2024, April 16). *From IT bots to AI deepfakes: The evolution of election-related misinformation in India*. https://www.thehindu.com/elections/lok-sabha/from-it-bots-to-ai-deepfakes-the-evolution-of-election-related-misinformation-in-india/article68015342.ece

Times of India. (2024, March 17). *Fooled by your own kid? Chilling rise of AI voice cloning scams*. https://timesofindia.indiatimes.com/india/fooled-by-your-own-kid-chilling-rise-of-ai-voice-cloning-scams/articleshow/108569446.cms

Times of India. (2024, January 4). *India saw 129 cybercrimes per lakh population in 2023*. Retrieved from https://timesofindia.indiatimes.com/india/india-saw-129-cybercrimes-per-lakh-population-in-2023/articleshow/106524847.cms

Free Press Journal. (2025, June 9). *Cybercrime alert: 72% Indian organisations targeted; AI becomes new weapon enabling stealthier attacks*. https://www.freepressjournal.in/business/cybercrime-alert-72-indian-organisations-targeted-ai-becomes-new-weapon-enabling-stealthier-attacks

India Foundation. (2025, May 1). *Fortifying the digital frontier: Protecting India's cyber interests*. https://indiafoundation.in/articles-and-commentaries/fortifying-the-digital-frontier-protecting-indias-cyber-interests

LawArticle. (2025, June 11). *Emerging cybercrime and the AI impact*. https://lawarticle.in/emerging-cybercrime-and-the-ai-impact

SME Futures. (2025, June 9). *72% Indian firms hit by AI-powered cyberattacks in past year: Report*. https://smefutures.com/72-indian-firms-hit-by-ai-powered-cyberattacks-in-past-year-report

The Logical Indian. (2025, June 5). *India faces ₹20,000 crore cybercrime threat in 2025 amid surge in AI-driven deepfake investment scams*. https://thelogicalindian.com/india-faces-%E2%82%B920000-crore-cybercrime-threat-in-2025-amid-surge-in-ai-driven-deepfake-investment-scams

Economic Times. (2024, May 10). *How AI-generated Aadhaar and PAN card frauds are rising*. Retrieved from https://economictimes.indiatimes.com

Business Standard. (2023, May 16). *UPI-related scams account for 55% of total digital payments frauds in India*. Retrieved from https://www.business-standard.com/finance/news/upi-related-scams-account-for-55-of-total-digital-payments-frauds-in-india-123051600333_1.html

Medianama. (2024, July 7). *Aadhaar breaches in land records behind AePS fraud surge*. Retrieved from https://www.medianama.com/2024/07/223-aadhaar-breaches-in-land-records-behind-aeps-fraud-surge/#:~:text=AePS'%20contribution%20to%20financial%20fraud,fingerprint%20and%20a%20duplicate%20one

Statista. (2024). *Cybercrime cases reported to I4C India (2019–2024)*. Retrieved from https://www.statista.com/statistics/1499739/india-cyber-crime-cases-reported-to-i4c/

Safer Internet Lab

saferinternetlab.org

Jl. Tanah Abang III no 23-27
Gambir, Jakarta Pusat. 10160

Find Us On

CSIS Indonesia | Safer Internet Lab