CURBING CYBER FRAUDS IN DIGITAL INDIA

Published On: 08-10-2025

“I dream of a Digital India where cyber security becomes an integral part of our national security”- Prime Minister Narendra Modi

Key Takeaways

- Over86% of householdsare nowconnected to theinternet.
- Cybersecurity incidentsin India rosefrom 10.29 lakh in 2022 to 22.68 lakh in 2024.
- Union Budget 2025-2026allocated?782 crorefor cybersecurity projects.
- Over9.42 lakh SIM cardsand2,63,348 IMEIslinked to cyber frauds have been blocked.
- A dedicatedhelpline 1930offers immediatecybersecurity assistance.

Introduction

India’s cyberspace is busier than ever, carrying crores of transactions and interactions every day. Over86% of households are now connected to the internet, reflecting the remarkable progress under theDigital India initiative. The expanding digital landscape has enabled citizens to access digital services at their fingertips. At the same time, it has also widened the attack surface for cyber frauds, making cybersecurity a national priority.

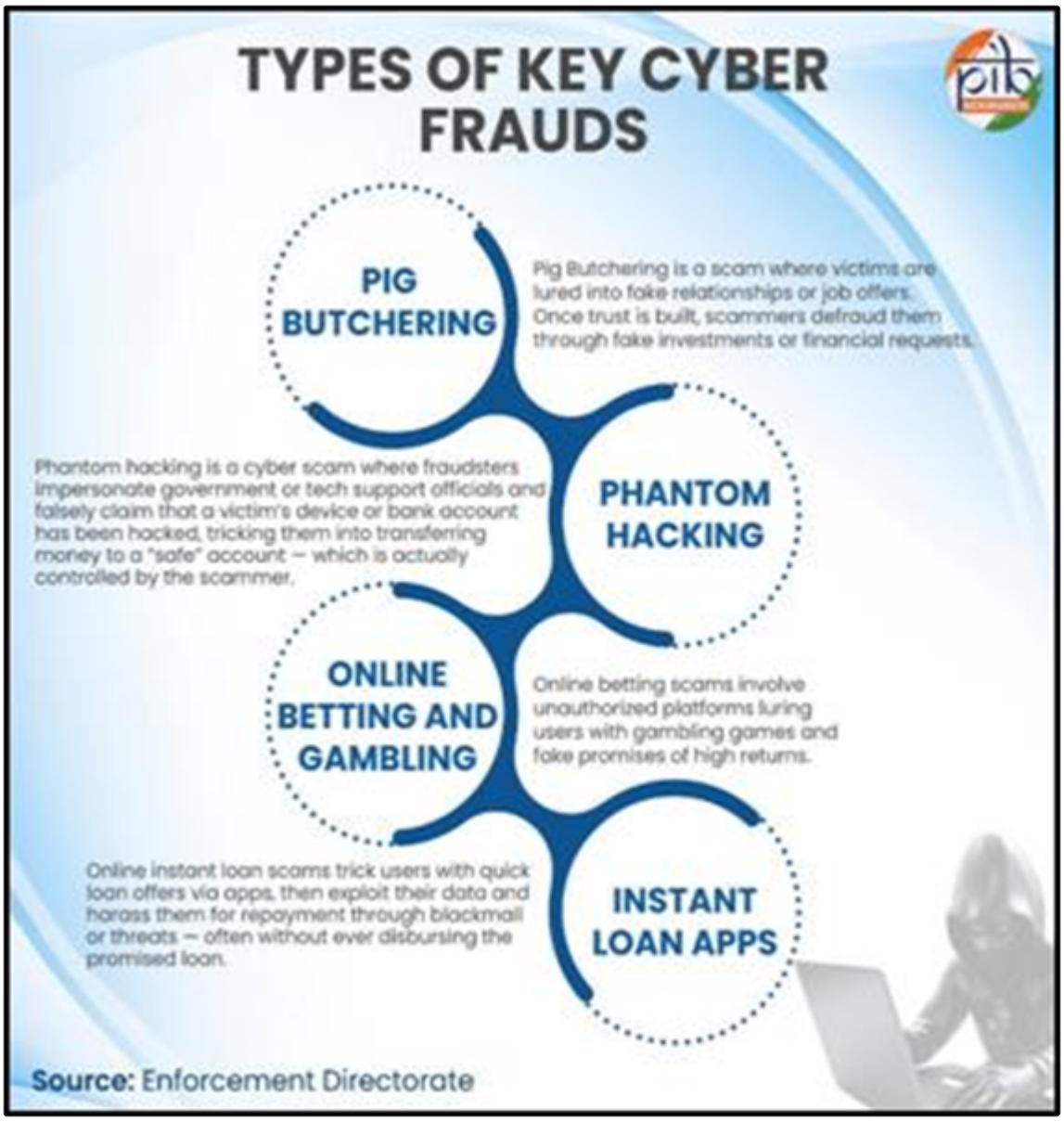
Cyber frauds refer to deceptive activities carried out through digital platforms such asunauthorized access, data theft, or online scams, which are often intended to cause financial loss to victims.

The surge in cybersecurity incidents from10.29 lakh in 2022 to 22.68 lakh in 2024reflects the growing scale and complexity of digital threats in India. At the same time, the financial toll is becoming more pronounced, with cyber frauds amounting to?36.45 lakhreported on the National Cyber Crime Reporting Portal (NCRP) as of 28 February 2025While the numbers point to increasing challenges, they also highlight remarkable progress in the nation’s detection and reporting mechanisms

Tracing Cyber Fraud Patterns

The evolving landscape of cyber frauds shows that frauds are not confined to a single method but take diverse forms, often adapting to new technologies and user behaviour. Mapping these patterns is crucial to enable

preventive measures. The staggering financial impact across the world is underscoring fraudsters' global reach and the involvement of organized crime, often linked to fraud factories in Southeast Asia



Emerging Cyber Threats

- Techniques like spoofing, where criminals act like trusted sources, are showing up in multiple fraud reports. Likewise, cases ofdeepfakes leveraging AI (Artificial Intelligence) and phishing, where individuals are lured into revealing sensitive information through deceptive emails or messages, are also on the rise— amplifying the overall impact of scams
- Unified Payments Interface (UPI), India's most preferred digital payment mode, has also been targeted by fraudsters using compromised mobile numbers. To address this issue, theDepartment of Telecommunications (DoT)launched theFinancial Fraud Risk Indicator (FRI),which classifies suspicious numbers as Medium, High, or Very High-risk.
- Illicit digital ventures have also emerged in the form ofonline betting apps, luring users into depositing funds in their online wallet to play such games with fake promises of large returns, generatingover ?400 croresin criminal proceeds.
- Strengthening India's fight against cyber frauds, thePromotion and Regulation of Online Gaming Bill, 2025was passed on21stAugust 2025This legislation is designed toencourage e-sports and social online gameswhile imposing acomplete ban on online money gaming, including their promotion, advertisements,

and financial transactions.

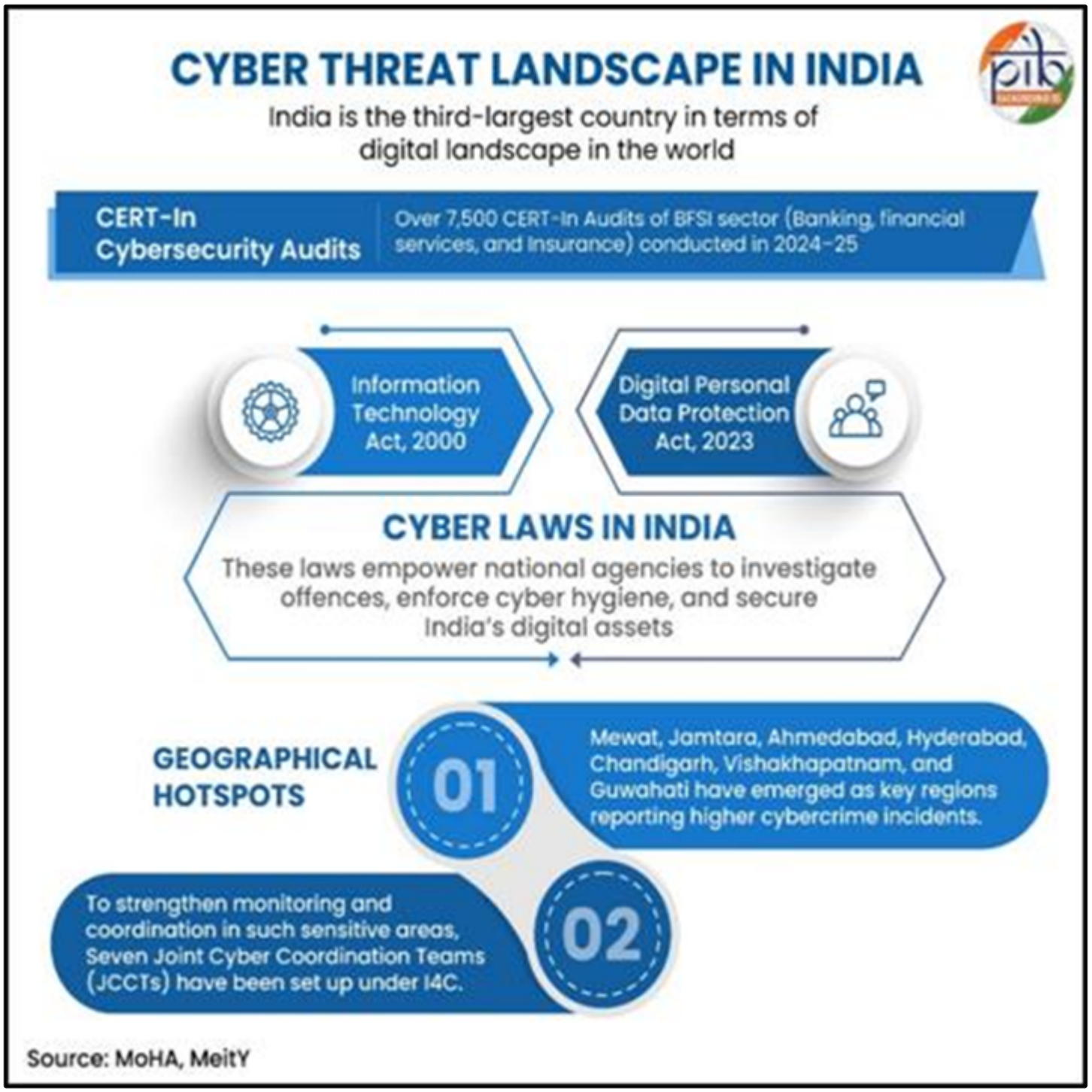
INDIA’S CYBERSECURITY FRAMEWORK

The Government of India has implemented strong Defence mechanisms aimed at safeguarding its vast online community. Indians are increasingly integrating the internet into their daily lives, relying on it for essential needs such as business transactions, education, financial activities, and accessing government services digitally. Over1,05,796 police officersare now registered on theCyTrain portal, with more than82,704 certificatesissued, equipping frontline personnel with essential cybercrime investigation skills.

1. Cyber Laws Securing Cyber Space

Recognizing the critical importance of a secure digital environment, India’s Cybersecurity framework is underpinned by key legislations, notably:

- Information Technology Act, 2000serves as the bedrock of India’s cyber law framework. It addresses offences like identity theft, impersonation, cheating by personation through computer resources, and dissemination of obscene or harmful material. These provisions are vital in prosecuting fraudsters who exploit digital platforms for financial gain, while also empowering authorities to block malicious websites and fraudulent applications.
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021ensure accountability of social media intermediaries, digital platforms, and online marketplaces. It addresses emerging misuse of technologies, including AI and mandate the removal of unlawful content from platforms.
- Digital Personal Data Protection Act, 2023: requires that all personal data be handled lawfully and with user consent, making India’s digital landscape safer and more accountable for everyone. The Act places strict obligations on data fiduciaries to ensure security safeguards, thereby reducing the risks of unauthorised access or misuse. So far, more than9.42 lakh SIM cardsand2,63,348 IMEIs(International Mobile Equipment Identity) linked to fraudulent activities have been blocked



2. Responding to Cyber Incidents

Indian Computer Emergency Response Team(CERT-In) is the national agency for responding to cybersecurity incidents. It monitors cyber threats, detect vulnerabilities, and issue necessary advisories. Upon identification of incidents such as data breaches, phishing campaigns, or malware intrusions, CERT-In disseminates alerts and prescribes remedial measures to affected organisations. This proactive mechanism ensures timely containment of risks and enhances resilience across government, industry, and critical service providers. As of March 2025, CERT-In facilitated109 cybersecurity mock drills, engaging1,438 organizationsfrom different states and sectors to assess cyber readiness and build resilience.

3. Protecting Critical Infrastructure

National Critical Information Infrastructure Protection Centre (NCIIPC), designated under Section 70A of the Information Technology Act, 2000, is the national nodal agency for the protection of critical information infrastructure in India. It works in close coordination with stakeholders in sectors such as banking, telecom, power, and transportation, which are vital to national security and public safety. Through continuous monitoring, risk assessment, and issuance of sector-specific guidelines, NCIIPC strengthens defensive capabilities and mitigates threats that could otherwise compromise essential services.

4. Strengthening Law Enforcement Capacity

TheIndian Cybercrime Coordination Centre (I4C), established under the Ministry of Home Affairs, provides a comprehensive framework to enable Law Enforcement Agencies (LEAs) to deal with cybercrimes in an organised and coordinated manner. It supports capacity-building through specialised training programmes, research, and development of technical tools. It also facilitates real-time information sharing and coordinated investigations, enabling effective action against cybercriminal networks, including those engaged in financial frauds and other organised cyber offences. So far,I4Chas proactively blocked3,962 Skype IDsand83,668 WhatsApp accountslinked to cyber frauds.

5. Cybersecurity Initiatives: Governance in Action

In an effort to bolster India’s cyber defences, the Union Budget 2025 has allocated?782 crore for cybersecurity projects. This significant move highlights government’s heightened focus on cyber threats that pose risk to the national security. Through theCitizen Financial Cyber Fraud Reporting and Management System (CFCFRMS), financial institutions have been able to save more than?5,489 crorein over17.82 lakh complaints.

6. National Cyber Crime Reporting Portal

To strengthen citizen participation in the fight against cybercrime, the Government has operationalised the National Cyber Crime Reporting Portal (www.cybercrime.gov.in). The portal enables citizens to report complaints relating to various categories of cybercrime, with a special focus on offences targeting women and childrenA dedicated cybercrime helpline number 1930provides immediate assistance to victims of online financial frauds by facilitating prompt reporting and, where possible, freezing of fraudulent transactions. Together, these initiatives serve as an accessible and responsive grievance redressal mechanism for citizens.

7. National Mission on Interdisciplinary Cyber-Physical Systems (NM-ICPS)

NM-ICPS plays a pivotal role in combating cyber frauds by promoting advanced research and innovation in cybersecurity, artificial intelligence, etc. By supporting the development of tools, platforms, and methodologies for threat detection, the mission strengthens India’s ability to identify and prevent cyber frauds targeting individuals, businesses, and critical infrastructure. Collaboration between academic institutions, industry, and government under NM-ICPS also accelerates solutions to emerging and sophisticated cyber threats, including financial frauds, phishing, and identity-based crimes.

8. Cyber Crime Prevention Against Women and Children (CCPWC) Scheme

The CCPWC scheme addresses cyber frauds targeting vulnerable sections, particularly women and children. With financial support of?132.93 crore,the scheme has established cyber forensic-cum-training laboratories across 33 States and Union Territories. These laboratories have trained over24,600 personnelin cybercrime investigation, digital forensics, and preventive measures. Through enhanced awareness, early detection, and rapid response capabilities, CCPWC strengthens the capacity of law enforcement to prevent online frauds, scams, and exploitation of women and children, ensuring a safer digital environment.

9. Cyber Crisis Management Plan (CCMP)

To strengthen preparedness against cyber-attacks and cyber-terrorism, the Government has initiatedCCMPfor all government bodies. The plan serves as a strategic framework to ensure coordinated recovery from any cyber crisis. So far,205 workshopshave been conducted across the country to build capacity and awareness under this framework.

10. Samanvaya Platform

The Samanvaya Platform strengthens cyber fraud investigations by providing analytics-based interstate linkages of criminals and crimes. Its‘Pratibimb’module maps locations of criminals and crime infrastructure, giving officers actionable visibility. So far, it has led to the arrest of12,987 accused,1,51,984 criminal linkages, and 70,584 cyber investigationassistance requests, helping dismantle organised cyber fraud networks efficiently.

11. Sahyog Portal

Sahyog Portal provides a centralized platform for addressing unlawful online content. It enables the automated issuance of removal notices to intermediaries, ensuring swift action against harmful material circulating in cyberspace. It brings together all authorised agencies across India onto a single interface, thereby strengthening the government’s ability to respond effectively to unlawful content in a timely manner.

CYBERSECURITY EXERCISES

The Bharat National Cybersecurity Exercise 2025was conducted from21stJuly to 01stAugust,reaffirming India’s commitment to strengthening its cyber resilienceThe exercise brought together over600 participants, including cybersecurity professionals, regulators, and policymakers. The highlight of this exercise wasSTRATEX, a simulated national cyber breach designed to test real-time inter-agency coordination and decision-making.

Cybersecurity in focus at India Mobile Congress 2025

At the 9th India Mobile Congress,Cybersecurity will be one of the key focus areas, highlighting India’s efforts to protect digital networks and emerging technologies from cyber threatsIMC 2025, themed*“Innovate to Transform”* will be inaugurated by Prime Minister Shri Narendra Modi from October 8–11 at Yashobhoomi, New Delhi.

IMC 2025 will featuresix global summits, including theCybersecurity SummitandBharat 6G Symposium, highlighting India's growing leadership in next-generation digital technologies. Key focus areas include6G, cybersecurity, satellite communications, AI, IoT,andtelecom manufacturing.

The event is expected to draw over1.5 lakh visitors,7,000+ international delegates,400+ exhibitors, and showcase more than1,600 cutting-edge use cases. With100+ sessionsand800+ speakers, IMC 2025 will serve as a premier platform for global collaboration and innovation.

As India celebrates its rapid5G rollout, with1.2 billion mobile subscribersand970 million internet users, the focus on secure, inclusive, and scalable digital ecosystems reinforces the country’s position as a global hub fortrusted and transformative digital infrastructure.

Forward Path: Cyber Awareness

To strengthen public awareness on cyber-crimes, the Government has taken a multi-platform outreach strategy.

- The Government has launched citizen-centric outreach campaigns throughradio, newspapers, and metro announcements, to caution people about cyber frauds.
- TheNational Cyber Coordination Centre (NCCC) has been set up by CERT-Into generate necessary situational awareness of existing and potential cyber security threats.
- Engaging the public by conductingCyber Safety and Security Awareness WeeksthroughMyGov platform.
- AHandbook for Adolescents and Studentsis published to guide young people on cyber safety and security.
- Use ofsocial mediato spread cyber awareness and safe practices to prevent cybercrime

Conclusion

India is at the crossroads of digital transformation and cyber threats, where it has become both an iron pillar of progress and a magnet for cyber fraudsters. Realising the vision of Digital India, the government's multi-layered cyber response team is facilitating fraud prevention and disrupting thousands of scam operations. Advanced forensics, big data analytics, and indigenous tools have bolstered national cyber resilience. Yet, securing India's cyberspace is a shared responsibility where the government and citizens must act together in this combat against cyber frauds.