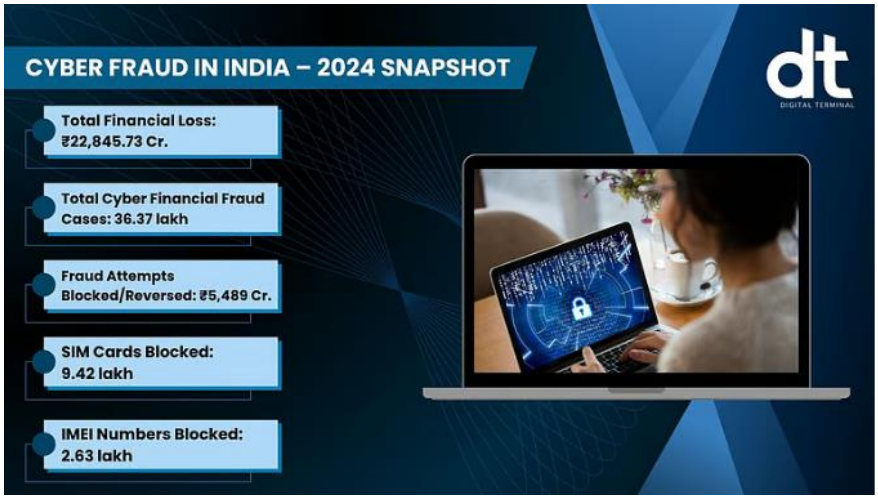
Cyber Frauds Cost India ₹22,845 Crore in 2024 as Digital Threats Escalate

Fraudsters today use sophisticated methods, including fake apps, social engineering, QR code traps, and impersonation tactics.

India is witnessing a sharp and alarming rise in cybercrime. According to new data shared by the Ministry of Home Affairs in Parliament, cyber fraud cases led to financial losses of over ₹22,845 crore in 2024 alone. This marks a 206% increase from ₹7,465 crore lost in the previous year.

The information was presented in a written reply to the Lok Sabha by Minister of State for Home Affairs, Bandi Sanjay Kumar. The figures are based on inputs collected from two official platforms — the National Cyber Crime Reporting Portal (NCRP) and the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS). Both systems are managed by the Indian Cyber Crime Coordination Centre (I4C) under the MHA.

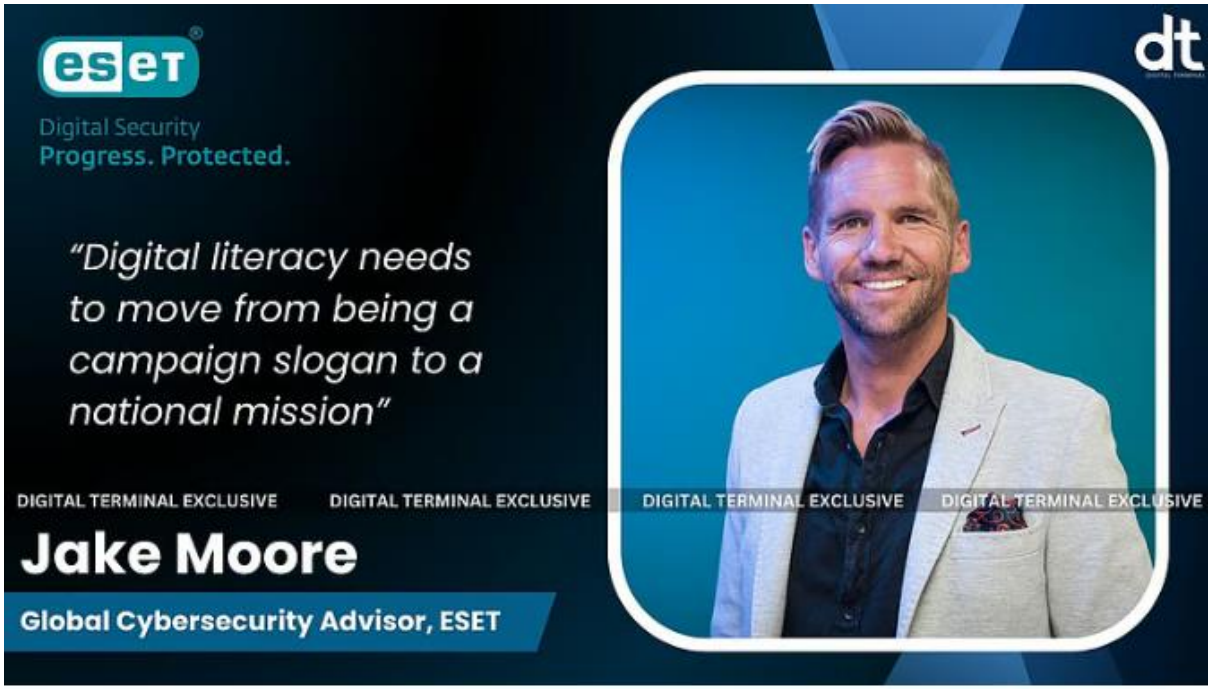
“The government is working closely with law enforcement agencies, financial institutions, and telecom service providers to disrupt cybercrime networks. Through the CFCFRMS platform, we have been able to save over ₹5,489 crore across 17.8 lakh complaints in 2024 alone. Additionally, a centralized Suspect Registry launched by I4C in collaboration with banks and financial institutions has helped flag more than 11 lakh suspicious identifiers and 24 lakh mule accounts, preventing fraud worth an estimated ₹4,631 crore,” said Minister Bandi Sanjay Kumar in his official statement to the Lok Sabha.



A Surge That Cannot Be Ignored

The total number of financial cybercrime cases reported in 2024 was 36.37 lakh, a significant rise from 20.6 lakh cases recorded in 2023. This surge shows how deeply digital fraud is now affecting citizens across India — from cities to small towns.

Cyber fraud in India is no longer limited to isolated phishing attempts or fake lottery calls. Fraudsters today use sophisticated methods, including fake apps, social engineering, QR code traps, and impersonation tactics. They often exploit gaps in digital awareness or take advantage of delays in reporting.



Speaking exclusively to Digital Terminal about the sharp surge in cyber fraud revealed by new government data, Jake Moore, Global Cybersecurity Advisor at ESET, stressed the urgent need for widespread digital awareness and stronger grassroots-level cybersecurity education to protect India's rapidly growing online population. He remarked, "Digital literacy needs to move from being a

campaign slogan to a national mission. The sophistication of scams today means that even the most cautious users are vulnerable.

In a world where trust can be manufactured with just a few data points, awareness is no longer optional. What makes this more urgent is India's digital scale. Millions of first-time users are coming online through vernacular apps, small-town smartphones, and regional social networks, without adequate exposure to basic cyber hygiene. That's where the real vulnerability lies. We need a culture of digital self-defence, not just in metros or enterprise offices, but across the full spectrum of users."

While talking exclusively to DT, Dr. Sanjay Katkar, Joint Managing Director at Quick Heal Technologies Ltd., strongly reacted to this concerning trend, stating, "The alarming ₹22,845 crore loss to cybercrime in 2024 highlights what we, at Quick Heal Technologies Limited, have been pointing out for so long that there is an urgent need for stronger and more evolved digital security measures. Users need to adopt multi-layered defense strategies, such as enabling multi-factor authentication for all banking transactions, regularly updating passwords with alphanumeric combinations, and avoiding sharing personal information even when contacted by seemingly legitimate sources. Never access banking sites from public computers or unsecured networks."

"Most importantly, remain vigilant against 'digital arrest' scams and phishing attempts. Always remember, no legitimate financial institution will request sensitive credentials via calls or emails. For an extra layer of security and complete peace of mind, we recommend using advanced cybersecurity solutions such as Quick Heal AntiFraud.AI to keep digital fraud at bay and protect your digital wellbeing," said Dr. Sanjay Katkar.

Tools Are Available, But Use Remains Low

To fight back, the government has made several tools available to the public. Citizens can report financial cybercrime through:

The 1930 emergency helpline for immediate fraud reporting.

The Cybercrime.gov.in portal to lodge official complaints.

The CFCFRMS system, introduced in 2021, was designed to stop or recover money when reported within the first few hours. But recovery is possible only if users act fast and report fraud immediately. Many victims are either unaware or hesitate, which limits the effectiveness of these tools.

Saving Lives, One Call at a Time

India's cybercrime helpline 1930 and the CFCFRMS platform have played a critical role in limiting losses. According to MHA data:

Over ₹5,489 crore was saved in 2024 by blocking or reversing fraudulent transactions.

Since the launch of the 1930 helpline, authorities have prevented losses exceeding ₹1,200 crore.

The systems now handle nearly 10,000 complaints per day, emphasizing the need for rapid public response.

The CFCFRMS portal, launched in April 2021, works on the "golden hour" principle and encouraging victims to report fraud immediately for better chances of recovery.

Enforcement and Tech-Driven Action

The government has also made significant strides in disrupting cybercrime operations:

Over 10,000 cybercriminals were arrested in 2024 through coordinated law enforcement efforts.

The I4C helped block over 9.4 lakh SIM cards and 2.6 lakh device IMEIs associated with fraud.

A centralized Suspect Registry, introduced in September 2024, flagged over 11 lakh suspicious identities and 24 lakh mule accounts, preventing an additional ₹4,631 crore in losses.

Speaking exclusively to Digital Terminal on the staggering financial impact of cybercrime and the concerning trends highlighted by the latest government report, Govind Rammurthy, CEO and Managing Director of eScan, emphasized how overdependence on digital ease is leaving users dangerously exposed. He said, "The ₹22,845 crore loss to cybercrime isn't just a number — it's the price we're paying for becoming too comfortable with digital convenience. UPI and smartphone apps have made everything accessible with a few taps. But this ease has made us careless. People now click 'approve' without thinking twice, and businesses rush to deploy new payment systems without proper security checks."

"What's worse is how these platforms have become playgrounds for fraudsters. Creating a fake loan app or investment scheme used to require significant effort and resources. Today, anyone can build a convincing app, buy targeted social media ads, and reach thousands of potential victims within hours. The same tools that help legitimate businesses now serve criminals just as effectively," stated Govind Rammurthy.

A Clear and Urgent Warning

India's digital economy is growing at a fast pace. But this growth must be matched with stronger cybersecurity infrastructure, digital literacy, and public-private collaboration. The loss of over ₹22,000 crore in just one year is not merely a statistic — it is a wake-up call.

As Minister Bandi Sanjay Kumar emphasized in Parliament, "Cybersecurity is a shared responsibility. Citizens must report fraud quickly. Institutions must remain vigilant. And the government will continue to invest in tools, enforcement, and awareness to secure our digital future."

ESET's Jake Moore also stressed the need for policy to keep up with evolving threats: "India has made great progress through initiatives like CFCFRMS, and new tools like the Suspect Registry and Pratibimb module. But governments and regulatory bodies must move faster. The IT Act and the upcoming Digital Personal Data Protection Rules offer a strong foundation, but the landscape is

evolving faster than policy. Cybersecurity must now move from the periphery to the core of every business decision and every boardroom agenda. Because in the end, the question is no longer if your organisation will face a cyber threat, but whether you'll be ready when it does."

"We need practical fixes, not more technology Band-Aids. So, lets start with basic education — teach people to recognize red flags like unrealistic returns or pressure tactics. Regulators must enforce stricter app store policies and conduct surprise audits of financial apps. Most importantly, we should add deliberate delays to large transactions, giving people time to reconsider. Sometimes the best security feature is simply making people wait and think before their act gets finalized. And this has to be done by government and large institutions, before it's too late, and not pass on the responsibility to common people, who have already gotten so used to (single-click) conveniences that it's impossible to snatch that away from their hands," concluded Govind Rammurthy.