

3. Cybercrime Trends in India- Science & Technology

Cybercrime saw 24% spike in 2025. Indians lost Rs 22,495 crore, mainly in investment scams

In 2025, investment frauds accounted for over 75% of the total ₹22,495 crore lost to cybercrime in India, driven by sophisticated scams like digital arrests and fake trading platforms. Despite a marginal dip in total financial loss due to early interventions, the overall number of cybercrime cases surged, highlighting the growing threat of phishing, ransomware, and identity theft.

Investment Frauds & Cybercrime Trends in India (2025)

Introduction Data from the Ministry of Home Affairs highlights a critical shift in the digital threat landscape for 2025. While the total financial loss saw a marginal decline, the volume of cases surged, with investment frauds emerging as the dominant threat, contributing to over 75% of the total money lost by Indians.

1. Key Cybercrime Trends (2025 Data)

Financial Loss vs. Case Volume-

Total Loss- Indians lost ₹22,495 crore in 2025, a marginal decline from ₹22,845 crore in 2024.

Case Volume- Despite the slight dip in monetary loss, the *number* of cybercrime cases increased significantly.

Dominance of Investment Scams-

Financial Impact- Investment frauds accounted for 76% of the total money lost.

Nature of Scams- These include Ponzi schemes, fake stock trading platforms, and cryptocurrency frauds.

FIR Trends- FIRs declined to 55,484 (2025) from 66,370 (2024), attributed to effective early fund-blocking interventions.

Distribution of Frauds (Financial Loss vs. Cases Reported)-

By Financial Loss- Investment Fraud (76%), Digital Arrest Scams (9%), Sextortion (4%).

By Number of Cases- Investment Fraud (35%), Sextortion (19%), Digital Arrest Scams (6%).

2. Understanding Cybercrime

Definition- Any unlawful act using a computer, communication device, or network to commit or facilitate a crime (e.g., Hacking, Identity Theft, Cyberstalking).

Constitutional Status- Cybercrime is a State subject under the Seventh Schedule of the Indian Constitution.

Key Techniques-

1. Phishing- Attackers impersonate legitimate entities (via email/SMS) to steal sensitive info like passwords or OTPs.
2. Ransomware- Malicious software that encrypts a victim's data, demanding payment for restoration.

3. Major Reasons for Rising Cybercrime

Financial Gain- The primary driver, often involving theft of credit card/bank details or ransom demands.

Fact- UPI frauds were the most prevalent online financial frauds (Jan 2020–June 2023) per the Future Crime Research Foundation (IIT-Kanpur).

Espionage- Theft of confidential/proprietary info for competitive advantage or reputation damage.

Political/Ideological Motives- Targeting organizations to advance specific agendas.

1. Example- Cambridge Analytica scandal (2018) involved leaking data of 419 million users (including Indians) to influence political outcomes.

Personal Motives- Harassment, defamation, or revenge.

Opportunism- Exploiting security vulnerabilities.

1. Example- Anonymous Sudan (cybercrime group) attacked Microsoft in June 2023, disrupting Outlook and Azure services.

4. Manifestations of Cybercrime in Real Life

Cyber Bullying– Harassment inflicted through electronic devices.

Cyber Stalking– Repeated electronic attempts to contact or follow a person despite clear disinterest.

Cyber Grooming– Building online relationships with minors to trick them into sexual acts.

Sexting– Transmission of sexually explicit digital images/messages.

SIM Swap Scam– Fraudulently obtaining a new SIM card for a registered number to bypass OTP security.

Cyberterrorism– Premeditated, politically motivated attacks on information systems to intimidate populations or damage critical infrastructure.

Example– ISIS targeting military/government websites for propaganda.

5. Challenges Associated with Cybercrime in India

Rapid Technological Advancements– Adoption of **IoT and Cloud computing** expands the attack surface.

1. Emerging Threat– Deep Fakes and AI-generated voice/video are making impersonation easier.

Sophisticated Attacks– Use of advanced techniques like Zero-day exploits (attacks on unknown security flaws) and Social Engineering.

Cyber Warfare & State–Sponsored Attacks– Increasing vulnerability of critical infrastructure to foreign espionage.

1. Example– Malware (Dtrack) attack on Kudankulam Nuclear Power Plant (2019), attributed to the Lazarus group (linked to North Korea).

Lack of Awareness– Poor cyber hygiene among individuals and businesses makes them susceptible.

Inadequate Legal Framework– Gaps remain in the *effective enforcement* of existing laws.

6. Global Conventions to Tackle Cybercrime

Interpol Cybercrime Global Strategy (2022–2025)– Focuses on reducing global impact and supporting member countries.

Potential UN Cybercrime Treaty– Currently under negotiation; if adopted, it will be the first binding UN instrument on cyber issues.

Budapest Convention– The first international treaty on crimes committed via the Internet and other computer networks, focusing on copyright infringement, computer-related fraud, child pornography and violations of network security. India is NOT a signatory to this convention.

7. Government Measures in India

Indian Cyber Crime Coordination Centre (I4C)– The nodal point for coordinating efforts against cybercrime.

1. Impact– Facilitated the sharing of 18.43 lakh suspect identifiers, blocking fraudulent transactions worth **₹8,031.56 crore**.

National Cyber Forensic Laboratory (NCFL)– Provides early-stage forensic assistance (online/offline) to Investigating Officers.

Citizen Financial Cyber Fraud Reporting Portal– Enables real-time reporting to block funds.

1. Impact– Saved over **₹7,130 crore** across 23.02 lakh complaints.

Dedicated Infrastructure– India now has **459 dedicated cybercrime police stations** (up from 169 in 2020), with **Uttar Pradesh** leading (75 stations).

National Cyber Security Policy (NCSP)– Aims to strengthen the country's cybersecurity posture.

8. Way Forward

Advanced Cybersecurity Framework– Organizations must adopt best practices, security protocols, and invest in technologies to protect critical systems.

Cyber Hygiene– Promote regular software updates, strong password management, and secure online behaviour.

International Cooperation– Strengthen collaboration to share threat intelligence and coordinate investigations for cross-border crimes.

Source- <https://theprint.in/india/cybercrime-saw-24-spike-in-2025-indians-lost-rs-22495-crore-mainly-in-investment-scams/2859930/>

