

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION No. 674
TO BE ANSWERED ON 22.07.2026

CYBER FRAUDS

674. DR. D RAVI KUMAR:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

- (a) the details of cyber frauds and online financial scams increased during the last three years;
- (b) whether the Government has taken any measures to contain cyber frauds and online financial scams and if so, the details thereof;
- (c) the details of cyber crime complaints received and resolved during the year 2025-26; and
- (d) the details of measures taken by the Government to strengthen cyber security awareness and protect citizens from digital fraud?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI JITIN PRASADA)

(a) to (d): The policies of Government of India are aimed at ensuring open, safe, trusted and accountable cyberspace for users in the country. The Government is cognizant of the risks and harms arising from the misuse of digital technologies including Cyber Frauds. The Barathiya Nyaya Sanhita, 2023, The Bharatiya Nagarik Suraksha Sanhita, 2023, The Information Technology Act, 2000, The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 and other related laws together established a framework to address cyber frauds.

The Information Technology Act, 2000 (“IT Act”):

- Section 66C prescribes an imprisonment of up-to three years and fine which may extend to rupees one lakh for identity theft;
- Section 66D prescribes an imprisonment of up-to three years and fine which may extend to rupees one lakh for cheating by personation by using computer resource;
- Section 66 prescribes a punishment of upto three years or with fine which may extend to five lakh rupees or with both for computer related offences;
- Section 43 prescribes penalty and compensation for damage to computer, computer system etc.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021:

- The IT Rules cast specific obligations on intermediaries to make reasonable efforts to ensure that users of their computer resources do not host, display, upload, modify, publish, transmit, store, update or share any information that deceives or misleads, impersonates another person or that violates any law for the time being in force.

- Intermediaries are required to remove any unlawful content within three hours of the receipt of an order of a court of competent jurisdiction or on receipt of a reasoned intimation by the Appropriate Government or its authorized agency.

Bharatiya Nyaya Sanhita (BNS), 2023

- The BNS, 2023 addresses the offences involving Organized Crime (Section 111), Cheating by Personation (Section 319), Forgery (Section 336 / 337), etc., and other cyber-enabled frauds.

To monitor and to strengthen the mechanism to deal with cybercrimes in a comprehensive and coordinated manner, the Central Government has taken steps which, inter-alia, include the following:

- The Ministry of Home Affairs has set up the 'Indian Cyber Crime Coordination Centre' ("I4C") as an attached office to deal with all types of cybercrimes in the country, in a coordinated and comprehensive manner.
- The 'National Cyber Crime Reporting Portal' ("NCRP") has been launched, as a part of the I4C, to enable public to report incidents pertaining to all types of cybercrimes, with special focus on cybercrimes against women and children. The portal is accessible at <https://cybercrime.gov.in>. Cybercrime incidents reported on this portal, their conversion into FIRs and subsequent action thereon are handled by the State/UT Law Enforcement Agencies concerned as per the provisions of the law.
- The 'Citizen Financial Cyber Fraud Reporting and Management System' (CFCFRMS), under I4C, has been launched in year 2021 for immediate reporting of financial frauds and to stop siphoning off funds by the fraudsters. A toll-free Helpline number '1930' has been operationalized to get assistance in lodging online cyber complaints.
- A State of the Art, Cyber Fraud Mitigation Centre (CFMC) has been established at I4C where representatives of major banks, Financial Intermediaries, Payment Aggregators, Telecom Service Providers, IT Intermediaries and representatives of States/UTs Law Enforcement Agency are working together for immediate action and seamless cooperation to tackle cybercrime.
- Samanvaya Platform has been made operational to serve as an Management Information System (MIS) platform, data repository and a coordination platform for LEAs for cybercrime data sharing and analytics. It provides analytics-based interstate linkages of crimes and criminals, involved in cybercrime complaints in various States/UTs. The module 'Pratibimb' maps locations of criminals and crime infrastructure on a map to give visibility to jurisdictional officers. The module also facilitates seeking and receiving of techno-legal assistance by Law Enforcement Agencies from I4C and other SMEs.

The Central Government has taken various initiatives to create public awareness and expeditious grievance redressal in order to protect citizens from cyber financial fraud which, inter-alia, include: -

- MeitY is implementing a project on 'Information Security Education and Awareness (ISEA)' for generating human resources in Information Security and creating general awareness on various aspects of cyber hygiene & cyber security among the masses. So far, 6,650 awareness workshops have been conducted across the country covering 11.37 lakh+ participants, including school/colleges students, teachers, law enforcement, government personnel, and general public. Further, multilingual awareness material in the form of handbooks, short videos, posters,

- brochures, cartoon stories for children, etc. published and disseminated through print, electronic, social media and www.isea.gov.in & <https://staysafeonline.in/>.
- Indian Computer Emergency Response Team (CERT-In) regularly shares safety and security tips and awareness posters, info-graphics and videos on its official websites and social media handles. It is aimed at sensitizing internet users on cyber security attacks and frauds including online safety measures for children.
 - National cyber security month has been observed in October each year. Safer Internet Day is also celebrated in February to sensitise users regarding online safety. This year it was observed on 10.02.2026.
 - Caller Tune Campaign: I4C in collaboration with the Department of Telecommunications (DoT) has launched a caller tune campaign with effect from 19.12.2024 for raising awareness about cybercrime and promoting the Cybercrime Helpline Number 1930 & NCRP portal. The caller tunes were also being broadcast in English, Hindi and 10 regional languages by Telecom Service Providers (TSPs). Six versions of caller tunes were played which cover various modus-operandi, namely, Digital Arrest, Investment Scam, Malware, Fake Loan App, Fake Social Media Advertisements.
 - The Central Government has launched a comprehensive awareness programme on digital arrest scams which, inter-alia, include; newspaper advertisement, announcement in Delhi Metros, use of social media influencers to create special posts, campaign through Prasar Bharti and electronic media, special programme on Aakashvani.
 - In partnership with DD News, I4C conducted a cybercrime awareness campaign running through Weekly Show Cyber-Alert starting from 19th July 2025 for 52 Weeks.
 - To further spread awareness on cyber crime, the Central Government has taken steps which, inter-alia, include; dissemination of messages through SMS, I4C social media account i.e. X (formerly Twitter) (@CyberDost), Facebook (CyberDostI4C), Instagram (CyberDostI4C), Telegram(cyberdosti4c), SMS campaign, TV campaign, Radio campaign, School Campaign, advertisement in cinema halls, celebrity endorsement, IPL campaign, campaign during Kumbh Mela 2025 & Suraj Kund Mela 2025, engaged MyGov for publicity in multiple mediums, organizing Cyber Safety and Security Awareness weeks in association with States/UTs, publishing of Handbook for Adolescents/Students, digital displays on railway stations and airports across, etc.

‘Police’ and ‘Public Order’ are State subjects as per the Seventh Schedule of the Constitution of India. The States/UTs are primarily responsible for the prevention, detection, investigation and prosecution of crimes including cybercrime through their Law Enforcement Agencies (LEAs). The Central Government supplements the initiatives of the States/UTs through advisories and financial assistance under various schemes for capacity building of their LEAs. The National Crime Records Bureau (NCRB) compiles and publishes the statistical data on crimes in its publication “Crime in India”. The latest published report may be accessed on : <https://www.ncrb.gov.in>
