GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS

RAJYA SABHA
UNSTARRED QUESTION NO. 3100

TO BE ANSWERED ON THE 20TH AUGUST, 2025/ SRAVANA 29, 1947 (SAKA)

RISE OF AI-DRIVEN CYBERCRIME AND MEASURES TO CURB FINANCIAL LOSSES

3100 MS. SUSHMITA DEV:

Will the Minister of HOME AFFAIRS be pleased to state:

(a) whether Government is aware of the recent State of AI-Powered Cybercrime: Threat & Mitigation Report 2025, which highlights that ₹22,812 crore were lost due to digital frauds in 2024, much of it driven by Artificial Intelligence (AI) tools and techniquess;

(b) the total number of cybercrime complaints and financial losses due to AI-driven cybercrimes registered across the country in 2024 and how it compares with previous years; and

(c) the specific steps taken by Government to develop and deploy AI-based threat detection and monitoring tools and integrate cybersecurity awareness and digital safety education in schools and workplaces?

ANSWER

**MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS
(SHRI BANDI SANJAY KUMAR)**

(a) to (c): The National Crime Records Bureau (NCRB) compiles and publishes the statistical data on crimes in its publication "Crime in India". Specific data regarding Artificial Intelligence (AI) driven cyber crimes is not maintained separately by NCRB.

‘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 cyber crimes 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.

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

i. **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 cyber crimes in the country, in a coordinated and comprehensive manner.**

ii. **The ‘National Cyber Crime Reporting Portal’ (NCRP) (https://cybercrime.gov.in) has been launched, as a part of the I4C, to enable public to report incidents pertaining to all types of cyber crimes, with special focus on cyber crimes against women and children. Cyber crime 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.

iii. 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. As per CFCFRMS operated by I4C, financial amount of more than Rs. 5,489 Crore has been saved in more than 17.82 lakh complaints so far. A toll-free Helpline number ‘1930’ has been operationalized to get assistance in lodging online cyber complaints.

iv. 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.

v. So far, more than 9.42 lakhs SIM cards and 2,63,348 IMEIs as reported by Police authorities have been blocked by Government of India.

vi. The Ministry of Home Affairs has formed CyMAC (Cyber Multi Agency Centre) under the MAC (Multi Agency Centre) platform on 22.01.2025

with the objective to effectively address cybersecurity threats, cyber espionage, misuse of emerging technologies and similar concerns against national security.

vii. **In partnership with India AI, I4C launched the India AI Cyber Guard AI Hackathon to develop an AI-powered system for the automatic classification of cybercrime incidents. This initiative aims to improve the efficiency and responsiveness of Law Enforcement Agencies (LEAs).**

viii. **The Central Government has developed an indigenous Artificial Intelligence (AI) and big data analytic tool ASTR to identify suspected mobile connections taken by same person in different names. So far, more than 82 lakhs such connections have been disconnected after failing reverification process.**

ix. **The state of the art 'National Cyber Forensic Laboratory (Investigation)' has been established, as a part of the I4C, at New Delhi to provide early stage cyber forensic assistance to Investigating Officers (IOs) of State/UT Police. So far, National Cyber Forensics Laboratory (Investigation) has provided its services to State/UT LEAs in around 12,460 cases pertaining to cyber crimes.**

x. **The Massive Open Online Courses (MOOC) platform, namely 'CyTrain' portal has been developed under I4C, for capacity building of police officers/judicial officers through online course on critical aspects of cyber crime investigation, forensics, prosecution etc. More than 1,05,796 Police Officers from States/UTs are registered and more than 82,704 Certificates issued through the portal.**

xi. **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. It has led to arrest of 12,987 accused, 1,51,984 linkages and 70,584 Cyber Investigation assistance request so far.**

xii. **'Sahyog' Portal has been launched to expedite the process of sending notices to IT intermediaries by the Appropriate Government or its agency under clause (b) of sub-section (3) of section 79 of the IT Act,** 2000 to facilitate the removal or disabling of access to any information, data or communication link being used to commit an unlawful act.

xiii. The Central Government has taken various initiatives to create cyber crime awareness which, inter-alia, include:-

1) The Hon'ble Prime Minister spoke about digital arrests during the episode "Mann Ki Baat" on 27.10.2024 and apprised the citizens of India.

2) I4C in collaboration with CBSE organized awareness campaigns on cybercrime through which more than 25,000 teachers and students were educated.

3) I4C imparted cyberhygiene training to more than 2 lakh NCC, NSS & NYKS Students across the country.

4) A 1930 Cyber Walkathon was organized by I4C in collaboration with Mount Olympus School in Sector 79, Gurugram, Haryana on 22.12.2024. More than 1500 persons, including students, parents, and police officers, participated in this event.

5) The Reserve Bank of India (RBI) also undertakes initiatives to integrate cybersecurity awareness and digital safety education regarding creation of customer awareness. A booklet on

'BE(A)WARE' and 'Raju and the Forty Thieves' covering the modus operandi of frauds and the way to escape/avoid getting trapped by fraudsters has been issued by RBI and placed on its website for use of public.

6) **A special programme was organized by Akashvani, New Delhi on Digital Arrest on 28.10.2024.**

7) **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.**

8) **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 and participated in Raahgiri Function at Connaught Place, New Delhi on 27.10.2024.

9) 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, 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.

******