

**GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS**

**LOK SABHA
UNSTARRED QUESTION NO. 1431**

TO BE ANSWERED ON THE 28TH JULY, 2026/ SHRAVANA 6, 1948 (SAKA)

CYBER CRIME MITIGATION CENTRE

**1431. SHRI SUDHEER GUPTA:
 SHRI PRADEEP KUMAR SINGH:
 SHRI DULU MAHATO:
 SHRI YOGENDER CHANDOLIA:
 SHRI DINESHBHAI MAKWANA:
 SHRI BIDYUT BARAN MAHATO:
 DR. BHOLA SINGH:
 SHRI DEEPENDER SINGH HOODA:
 SHRI MURASOLI S:
 SHRI MUKESHKUMAR CHANDRAKAANT DALAL:
 SHRI SHIVMANGAL SINGH TOMAR:
 SHRI VISHWESHWAR HEGDE KAGERI:
 SHRI DHAIRYASHEEL SAMBHAJIRAO MANE:
 SHRI AMAR SHARADRAO KALE:
 SHRI DEVUSINH CHAUHAN:
 SHRI SHANKAR LALWANI:
 SMT. MAHIMA KUMARI MEWAR:
 SMT. KAMALJEET SEHRAWAT:
 SMT. SHOBHANABEN MAHENDRASINH BARAIYA:
 SHRI JAGDAMBIKA PAL:
 SHRI JYOTIRMAY SINGH MAHATO:
 SHRI KRISHNA PRASAD TENNETI:
 SHRI SURESH KUMAR KASHYAP:
 SMT. D K ARUNA:
 SHRI ARUN GOVIL:
 SHRI BHARATSINHJI SHANKARJI DABHI:
 DR. NISHIKANT DUBEY:**

Will the Minister of HOME AFFAIRS be pleased to state:

- (a) the achievements made so far by the Indian Cybercrime Coordination Centre (I4C) in curbing cyber financial fraud;**
- (b) whether the steps taken by the said Centre in curbing cyber financial fraud have been reviewed;**

(c) if so, the amount saved and the details of the complaints received through the Citizen Financial Cyber Fraud Reporting and Management System;

(d) the number of SIM (Subscriber Identity Module) cards and IMEIs (International Mobile Equipment Identity) blocked so far through the Suspect Registry and the number of mule accounts/bank accounts identified thereunder;

(e) the outcomes of the Cyber Fraud Mitigation Centre and the 'Pratibimb' module including the details and the number of arrests as well as the achievements made so far; and

(f) the steps taken for the capacity building of the law enforcement agencies under the National Cybercrime Training Centre (NCTC) ?

ANSWER

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

(a) to (f) : '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 fraud 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 including cyber financial fraud 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.**
- 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, till 30.06.2026, financial amount of more than Rs. 11,158 Crore has been saved in more than 32.80 lakh complaints. 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. **Till 30.06.2026, more than 15.75 lakhs SIM cards and 5.77 lakhs IMEIs as reported by Police authorities have been blocked by Government of India.**
- vi. **A Suspect Registry of identifiers of cyber criminals has been launched by I4C on 10.09.2024 in collaboration with Banks/Financial Institutions. Till 30.06.2026, more than 30.48 lakh suspect identifier data received from Banks and 32.08 lakh Layer 1 mule accounts have been shared with the participating entities of Suspect Registry and declined transactions worth Rs. 25,698 crores.**
- vii. **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 lead to arrest of more than 29,837 accused and more than 2,33,593 Cyber Investigation assistance request.**
- viii. **'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.

- ix. 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. Till 30.06.2026, more than 1,63,344 police officers/judicial officers from States/UTs are registered and more than 1,61,957 Certificates issued through the portal.**
- x. Cyber Commando programme was launched by the Hon'ble Home Minister on 10.09.2024 to establish a Special Wing of Cyber Commandos equipped with specialized training to counter cybersecurity threats in the country. The programme envisions the creation of a dedicated, skilled workforce capable of securing critical information infrastructure and supporting national cybersecurity efforts. 281 cyber commandos successfully completed training.**
- xi. I4C, MHA is regularly organising 'State Connect', 'Thana Connect' 'Bank Connect' and Peer learning session to share best practices, enhance capacity building, etc.**
- xii. The state of the art National-Digital Investigation Support Centre (previously known as National Cyber Forensic Laboratory**

(Investigation) {NCFL(I)}} has been established, as a part of the I4C, at New Delhi (on 18.02.2019) and at Assam (on 29.08.2025) to provide early stage cyber forensic assistance to Investigating Officers (IOs) of State/UT Police. Till 30.06.2026, National-Digital Investigation Support Centre, New Delhi has provided its services to State/UT LEAs in more than 14,064 cases pertaining to cyber crimes.

- xiii. To further strengthen operational efficiency and ensure uniformity in handling cybercrime complaints, the Ministry has issued a comprehensive Standard Operating Procedure (SOP) for NCRP-CFCFRMS. The SOP lays down a standardized framework for complaint processing, bank coordination, grievance redressal, removal of lien markings, and restoration of defrauded funds to rightful claimants based on complaints received through the NCRP. Money Restoration Module for expeditious restoration of defrauded money to the victims and Grievance Redressal Module for timely attending to the grievances relating to freezing of the bank accounts and lien marking of the amount, have been made functional from April, 2026.**

To further spread awareness on cyber crime, the Central Government has taken steps which, inter-alia, include; caller tune campaign, 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, engaged MyGov for publicity in multiple mediums, organizing Cyber Safety and Security Awareness weeks in association with States/UTs, digital displays on metro stations, railway stations and airports across, etc.
