GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS

LOK SABHA
UNSTARRED QUESTION NO. 2729

TO BE ANSWERED ON THE 16TH DECEMBER, 2025/ AGRAHAYANA 25, 1947 (SAKA)

CYBERCRIME INCIDENTS

2729. SHRI YADUVEER WADIYAR:

Will the Minister of HOME AFFAIRS be pleased to state:

(a) the number of cyber financial crime incidents reported in 2025 and the amount defrauded through such crimes across the country;

(b) the details of cybercrime cases reported in Karnataka, particularly those involving financial fraud and digital payment related offences, district-wise;

(c) the steps taken to enhance coordination among State police forces, I4C, CERT-In, and Central agencies to dismantle inter-state and international cybercriminal networks; and

(d) the measures proposed to strengthen cybercrime prevention, victim compensation and capacity-building in districts such as Mysuru that are increasingly vulnerable to digital fraud and emerging cyber threats?

ANSWER

MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS

(SHRI BANDI SANJAY KUMAR)

(a) to (d): The National Crime Records Bureau (NCRB) compiles and publishes the statistical data on crimes in its publication "Crime in India". The latest published report is for the year 2023.

'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 crime 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 applicable across India including Karnataka 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. Till 31.10.2025, financial amount of more than Rs. 7,130 Crore has been saved in more than 23.02 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 31.10.2025, more than 11.14 lakhs SIM cards and 2.96 lakhs IMEIs as reported by Police authorities have been blocked by Government of India.

vi. I4C, MHA is regularly organising 'State Connect', 'Thana Connect' and Peer learning session to share best practices, enhance capacity building, etc.

vii. Seven Joint Cyber Coordination Teams (JCCTs) have been constituted for Mewat, Jamtara, Ahmedabad, Hyderabad, Chandigarh, Vishakhapatnam, and Guwahati under I4C covering the whole country based upon cyber crime hotspots/ areas having multi jurisdictional issues by onboarding States/UTs to enhance the coordination framework among the Law Enforcement Agencies of the States/UTs.

viii. The state of the art 'National Cyber Forensic Laboratory (Investigation)' 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 31.10.2025, National Cyber Forensics Laboratory (Investigation), New Delhi has provided its services to State/UT LEAs in around 12,952 cases pertaining to cyber crimes.

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. More than 1,44,895 police officers/judicial officers from States/UTs are registered and more than 1,19,628 Certificates issued through the portal.

x. '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.

xi. A Suspect Registry of identifiers of cyber criminals has been launched by I4C on 10.09.2024 in collaboration with Banks/Financial Institutions. Till 31.10.2025, more than 18.43 lakh suspect identifier data received from Banks and 24.67 lakh Layer 1 mule accounts have been shared with the participating entities of Suspect Registry and declined transactions worth Rs. 8031.56 crores.

xii. 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 16,840 accused and 1,05,129 Cyber Investigation assistance request.

xiii. A Memorandum of Understanding (MoU) was signed on 17 January 2025 by I4C, MHA and the Department of Homeland Security, USA to strengthen cooperation and capacity building in cybercrime investigations.

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, Caller tune 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.

*****