## GOVERNMENT OF INDIA
## MINISTRY OF HOME AFFAIRS

## RAJYA SABHA
## UNSTARRED QUESTION NO. 1197

**TO BE ANSWERED ON THE 30TH JULY, 2025/ SRAVANA 8, 1947 (SAKA)**

**STRATEGIES TO PREVENT CYBER CRIMES**

1197 #     MS. INDU BALA GOSWAMI:
          SHRI NEERAJ SHEKHAR:

Will the Minister of Home Affairs be pleased to state:

(a) whether Government has formulated any strategy to curb cyber crimes;

(b) if so, the details thereof;

(c) whether any policy has been formulated  for  prompt  action  in  case  of cyber crime;

(d) the steps taken by Government to enhance capacity building of police / investigative agencies  across  the  country  to  deal with increasing cyber crimes; and

 (e) if so, the details thereof?

### ANSWER

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

(a) to (e):  '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.

With a view to strategically curb cyber crimes and take prompt action, the Ministry of Home Affairs has taken a policy decision to set up the 'Indian Cyber Crime Coordination Centre' (I4C) as an attached office on 01.07.2024 to deal with all types of cyber crimes in the country, in a coordinated and comprehensive manner.

To further, 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 '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.

ii. 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.

iii. 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.

iv. 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.

v. The Ministry of Home Affairs has provided financial assistance under the 'Cyber Crime Prevention against Women and Children (CCPWC)' Scheme, to the States/UTs for their capacity building such as setting up of cyber forensic-cum-training laboratories, hiring of junior cyber consultants and training of LEAs' personnel, public prosecutors and judicial officers. Cyber forensic-cum-training laboratories have been commissioned in 33 States/UTs and more than 24,600 LEA personnel, judicial officers and prosecutors have been provided training on cyber crime awareness, investigation, forensics etc.

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

vii. 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.

viii. 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.

ix. 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 10,599 accused, 26,096 linkages and 63,019 Cyber Investigation assistance request.

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

3) Caller Tune Campaign: I4C is 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.

4) 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.

5) 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.

*****