GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS

RAJYA SABHA
UNSTARRED QUESTION NO. 1505

TO BE ANSWERED ON THE 12TH MARCH, 2025/ PHALGUNA 21, 1946 (SAKA)

COMBATING DIGITAL ARREST, BLACKMAIL, AND CYBER IMPERSONATION OF LAW ENFORCEMENT AGENCIES

1505. SHRI SUJEET KUMAR:

Will the Minister of Home Affairs be pleased to state:

(a) the number of reported incidents of 'Digital Arrest' and blackmail recorded through the National Cyber Crime Reporting Portal (NCRP) in the last three years;

(b) the specific measures being taken by Government to prevent cybercriminals from impersonating law enforcement agencies such as the CBI, RBI, and NCB; and

(c) the role of the Indian Cyber Crime Coordination Centre (I4C) in tracking and dismantling cross-border cybercrime syndicates and the extent of its collaboration with other agencies in this regard?

ANSWER

MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS

(SHRI BANDI SANJAY KUMAR)

(a) to (c) : '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 and digital arrest scams 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 digital arrest scams 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. The number of incidents of digital arrest scams and related cyber crimes reported on 'National Cyber Crime Reporting Portal' for the last three years are as below:**

S. No.	Year	No. of incidents	De-frauded amount (In crore)
1	2022	39925	91.14
2	2023	60676	339.03
3	2024	123672	1935.51
4	2025 (till 28.02.2025)	17718	210.21

iii. The 'Citizen Financial Cyber Fraud Reporting and Management System', under I4C, has been launched in year 2021 for immediate reporting of financial frauds and to stop siphoning off funds by the fraudsters. So far, financial amount of more than Rs. 4,386 Crore has been saved in more than 13.36 lakh complaints. A toll-free Helpline number '1930' has been operationalized to get assistance in lodging online cyber complaints.

iv. 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 and participated in Raahgiri Function at Connaught Place, New Delhi on 27.11.2024.

v. 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.

vi. I4C in collaboration with the Department of Telecommunications (DoT) has launched a caller tune campaign for raising awareness about cybercrime and promoting the Cyber Crime Helpline Number 1930 & NCRP. The caller tune is also being broadcasts in regional languages, delivered 7-8 times a day by Telecom Service Providers (TSPs).

vii. I4C proactively identified and blocked more than 3,962 Skype IDs and 83,668 Whatsapp accounts used for Digital Arrest.

viii. The Central Government has published a Press Release on Alert against incidents of 'Blackmail' and 'Digital Arrest' by Cyber Criminals Impersonating State/UT Police, NCB, CBI, RBI and other Law Enforcement Agencies.

ix. The Central Government and Telecom Service Providers (TSPs) have devised a system to identify and block incoming international spoofed calls displaying Indian mobile numbers appear to be originating within India. Directions have been issued to the TSPs for blocking of such incoming international spoofed calls.

x. Till 28.02.2025, more than 7.81 lakhs SIM cards and 2,08,469 IMEIs as reported by Police authorities have been blocked by Government of India.

xi. To 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), Radio campaign, 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.

xii. A State of the Art Centre, 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.

xiii. 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 on boarding States/UTs to enhance the coordination framework among the Law Enforcement Agencies of the States/UTs. Seven workshops were organized for JCCTs at Hyderabad, Ahmedabad, Guwahati, Vishakhapatnam, Lucknow, Ranchi and Chandigarh.

xiv. 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 6,046 accused, 17,185 linkages and 36,296 Cyber Investigation assistance request.

xv. The Ministry of External Affairs also holds bilateral cyber dialogue with various countries from time to time. The Indian Cyber Crime Coordination Centre (I4C), Ministry of Home Affairs, being a nodal agency for cyber crime in the country is actively participate in such cyber dialogues.

xvi. The National Central Bureau (NCB) in the Central Bureau of Investigation (CBI) acted as effective interface between Indian LEAs and foreign LEAs and facilitates regular exchange of information through INTERPOL channels. Recently BHARATPOL portal has been launched to further streamline the communication between NCB, CBI and Indian LEAs in the matters of international assistance and coordination.

xvii. The CBI is nodal agency for G-7 24/7 network. G7 24/7 is secure channel for making data preservation requestes in cases related to cyber crime.

******