GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS

RAJYA SABHA
UNSTARRED QUESTION NO. 228

TO BE ANSWERED ON THE 27TH NOVEMBER, 2024/ AGRAHAYANA 6, 1946 (SAKA)

CASES OF DIGITAL ARREST SCAMS

228 DR. SUDHANSHU TRIVEDI:

Will the Minister of HOME AFFAIRS be pleased to state:

(a) the measures being taken to deal with an alarming surge in digital arrest scams in the country;

(b) whether the Ministry, in coordination with Ministry of Electronics and Information Technology will take strict action to identify and arrest those impersonators posing as Government and law enforcement officials;

(c) the manner in which Ministry propose to deal with untraceable SIMs which allows scammers to defraud victims with a reduced risk of immediate detection; and

(d) the new initiatives to educate and alert users about potential scams through various social media portals and which fake law enforcement handles have been disabled?

ANSWER

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

(a) to (d) : '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 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 cybercrimes in the country, in a coordinated and comprehensive manner.**

ii. **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. Such international spoofed calls have been made by cyber-criminals in recent cases of fake digital arrests,**

FedEx scams, impersonation as government and police officials, etc. Directions have been issued to the TSPs for blocking of such incoming international spoofed calls.

iii. 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.

iv. Till 15.11.2024, more than 6.69 lakhs SIM cards and 1,32,000 IMEIs as reported by Police authorities have been blocked by Government of India.

v. Samanvaya Platform (Joint Management Information System) has been made operational from April 2022 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.

vi. A Suspect Registry of identifiers of cyber criminals has been launched by I4C on 10.09.2024 in collaboration with Banks/Financial Institutions.

vii. The Central Government has introduced a new feature titled as 'Report and Check Suspect' on https://cybercrime.gov.in. This facility provides citizens a search option to search I4C's repository of identifiers of cyber criminals through 'Suspect Search'.

viii. I4C proactively identifyand blockfake IDs used for Digital Arrest.

ix. 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.

x. 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.

xi. The 'National Cyber Crime Reporting Portal' (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.

xii. 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. 3431 Crore has been saved in more than 9.94 lakh complaints. A toll-free Helpline

number '1930' has been operationalized to get assistance in lodging online cyber complaints.

xiii. I4C has imparted cyber hygiene training to 7,330 officials of various Ministries/ Departments of Government of India.

xiv. I4C has imparted cyber hygiene training to more than 40,151 NCC cadets.

xv. 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, newspaper advertisement on digital arrest scam, announcement in Delhi metros on digital arrest and other modus operandi of cyber criminals, use of social media influencers to create special posts on digital arrest, digital displays on railway stations and airports across, etc.

*****