GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS

RAJYA SABHA
UNSTARRED QUESTION NO. 1523

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

RISE IN INSTANCES OF CYBER ARREST SCAMS

1523 SHRI TIRUCHI SIVA:

Will the Minister of HOME AFFAIRS be pleased to state:

(a) whether the Ministry intends to establish a mechanism for tracking cyber arrest incidents, given NCRB does not maintain specific data on digital arrest scams;

(b) the technological measures being implemented to identify and block spoofed international calls mimicking Indian mobile numbers and whether these have been effective in reducing cyber arrest scams; and

(c) the steps being taken to strengthen international coordination with communication and law enforcement agencies to address the cross-border nature of cyber arrest scams?

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 cyber 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 cyber 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.**

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 identify 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. 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.

xii. 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.

xiii. 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.

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

*****