GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 3814
TO BE ANSWERED ON 18.12.2024

CASES OF DIGITAL ARREST SCAMS

3814. SHRI ARVIND DHARMAPURI:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

(a) the total number of cases of digital arrest scams and related cybercrimes registered during the last three years, State/UT-wise;
(b) the details of the resolution rate of such cases along with the funds allocated for addressing them; and
(c) the steps taken by the Government to create awareness among vulnerable groups about digital arrest scams and improve cybersecurity measures?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI JITIN PRASADA)

(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.

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 2022. Specific data regarding digital arrest scams is not maintained separately by NCRB.

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 Bharatiya Nyaya Sanhita, 2023 ("BNS") penalizes the commission of any continuing unlawful activity including economic offence, cybercrimes, by any person or a group of persons, either as a member of an organised crime syndicate or on behalf of such syndicate. The punishment is minimum of 5 years (non-bailable) which may extend to imprisonment for life and fine not less than 5 lakh rupees and fine not less than 10 lakh rupees in case death of any is caused. It may be noted that the BNS which deals with false charge of offence made with intent to injure may also be applicable in cases where fraudsters use digital devices to falsely accuse victims of certain offences. The punishment may extend to five years, or with fine which may extend to two lakh rupees (non-bailable offence).Furthermore, several other sections under the BNS may also be attracted in case of cheating, cheating by personation, forgery, etc. Many criminal provisions especially cybercrimes under the newly enacted BNS have been made non-bailable.
ii. In addition to the punishment under the BNS, the Information Technology Act, 2000 ("IT Act") defines various cybercrimes such as tampering with computer source documents, computer related offences, identity theft, cheating by personation by using computer resource, and so on. There are 18 sections which provide various form of cyber offences, out of which 12 such offences are bailable. These provisions of

punishment for identity theft and cheating by personation by using computer resource may effectively tackle with the menace of digital arrests where fraudsters make use of digital devices to extort money from citizens who may fall in such traps of fraudulent calls where the caller impersonates a LEA or a government officer in India.

iii. 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.

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. I4C proactively identified and blocked more than 1700 Skype IDs and 59,000 WhatsApp accounts used for Digital Arrest.

vi. 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.

vii. 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.

viii. 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.

ix. 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.

x. 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.

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

xii. 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.

xiii. 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'.

xiv. 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.

xv. 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.

xvi. 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.

****