GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS

LOK SABHA
UNSTARRED QUESTION NO. 1283

TO BE ANSWERED ON THE 3RD DECEMBER, 2024/ AGRAHAYANA 12, 1946 (SAKA)

CYBER FRAUD AND DIGITAL HARASSMENT

1283. SHRI VIJAYAKUMAR *ALIAS* VIJAY VASANTH:
SHRI MANICKAM TAGORE B:

Will the Minister of HOME AFFAIRS be pleased to state:

(a) the measures taken by the Government to prevent such instances of cyber fraud and digital harassment along with the support services provided by the Government to the victims of cyber fraud and digital harassment;

(b) whether the law enforcement agencies are equipped to handle such cases;

(c) if so, the status of existing laws and regulations regarding cyber fraud;

(d) the data on the number of reported cases of cyber fraud during the past year;

(e) the measures taken by the Government to educate the citizens on identifying and avoiding such scams;

(f) whether the Government is considering for establishing a dedicated agency to tackle cybercrime and if so, the details thereof; and

(g) the timeline for implementing effective solutions to prevent such digital arrest ordeals?

ANSWER

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

(a) to (g) : '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. Cyber Crimes cases are handled under the provisions of the Information Technology Act, 2000, the Bhartiya Nyaya Sanhita, 2023 and Protection of Children from Sexual Offences Act, 2012 (POCSO Act). 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. The NCRB maintained information regarding certain categories of fraud for cyber crime such as credit/debit cards, ATMs, online banking frauds, OTP frauds and others. As per the data published by the NCRB, details of cases registered under fraud for cyber crimes (involving communication devices as medium/target) for the period of 2022 is as under:

Cases Registered under Fraud for Cyber Crimes	Credit/Debit cards	ATMs	Online Banking frauds	OTP frauds	Others	Total
	1665	1690	6491	2910	4714	17470

To 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 Ministry of Home Affairs has set up the 'Indian Cyber Crime Coordination Centre' (I4C)as an attached office to deal with all types of cybercrime in the country, in a coordinated and comprehensive manner.**

ii. **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.**

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. 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.**

iv. 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.

v. 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 11,203 cases pertaining to cyber crimes.

vi. 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 98,698 Police Officers from States/UTs are registered and more than 75,591 Certificates issued through the portal.

vii. National Cyber Forensic Laboratory (Evidence) has been set up at Hyderabad. Establishment of this laboratory provides the necessary

forensic support in cases of evidence related to cyber crime, preserving the evidence and its analysis in line with the provisions of IT Act and Evidence Act; and reduced turnaround time.

viii. The Ministry of Home Affairs has provided financial assistance to the tune of Rs. 131.60 crores 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.

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

x. I4C has imparted cyber hygiene training to more than 40,151 and 53,022 NCC cadets and NSS cadets respectively.

xi. 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.

xii. 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.

xiii. 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.

*****