GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS

LOK SABHA
UNSTARRED QUESTION NO. 2305

TO BE ANSWERED ON THE 10TH DECEMBER, 2024/ AGRAHAYANA 19, 1946 (SAKA)

AWARENESS CAMPAIGN ON CYBER CRIMES

2305. SHRI MANOJ TIWARI:

Will the Minister of HOME AFFAIRS be pleased to state:

(a) the measures being taken by the Government to prevent cyber crimes in the country, including initiatives to strengthen cybersecurity infrastructure and law enforcement capabilities;

(b) whether the Government has launched any public awareness campaigns to educate citizens about cyber crime prevention and safe internet practices and if so, the details thereof; and

(c) the steps being taken to improve coordination between different Government departments, State police and international agencies to tackle cross-border cyber crimes effectively?

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 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 initiatives to strengthen cybersecurity infrastructure and law enforcement capabilities 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 '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. **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'.**

v. 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.

vi. I4C proactively identify and blocked more than 1700 Skype IDs and 59,000 Whatsapp accounts used for Digital Arrest.

vii. 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.

viii. The Indian Computer Emergency Response Team (CERT-In) is operating an automated cyber threat exchange platform for proactively collecting, analysing and sharing tailored alerts with organisations across sectors for proactive threat mitigation actions by them.

ix. CERT-In has set up the National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats.

x. CERT-In operates the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) to detect malicious programs and provides free tools to remove the same, and also provides cyber security tips and best practices for citizens and organisations.

xi. Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 104 such drills have so far been conducted by CERT-In where around 1450 organizations from different States and sectors participated.

xii. CERT-In conducts regular training programmes for network / system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organisations regarding securing the IT infrastructure and mitigating cyber attacks. A total of 9,807 officials have been trained in 20 training programs in 2024 upto October.

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.

xiv. 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.

xv. 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.

xvi. 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.

xvii. 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.

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

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

xx. 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.

xxi. 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.

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

xxiii. The Central Bureau of Investigation (CBI) participates in various regional and international cyber crime cooperation initiatives led by Interpol, fostering collaboration with global LEAs to address cross-border cyber crime challenges.

xxiv. The CBI serves as the nodal point in India for data preservation requests, sending and receiving such requests through the G7 24/7 network to ensure the timely and secure exchange of cyber crime related data.

xxv. The National Central Bureau (NCB) in CBI acts as a central coordination agency, facilitating the collection and dissemination of cyber crime information through Interpol channels.

****