GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS

LOK SABHA
UNSTARRED QUESTION NO. 2576

TO BE ANSWERED ON THE 19TH DECEMBER, 2023/ AGRAHAYANA 28, 1945 (SAKA)

CYBER CRIME AWARENESS

2576. SHRI MARGANI BHARAT:

Will the Minister of HOME AFFAIRS be pleased to state:

(a) the details of any national campaigns or initiatives aimed at promoting cyber crime awareness among citizens;

(b) the measures taken by the Government to equip law enforcement agencies with the necessary skills and resources to effectively combat cyber crime and any recent training programmes implemented;

(c) the investments made in technology infrastructure and cyber security tools to strengthen the nation's overall cyber resilience; and

(d) whether any assessment has been conducted on the impact of these initiatives on the reduction of cyber crime incidents and if so, the details thereof?

ANSWER

MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS
(SHRI AJAY KUMAR MISHRA)

(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 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 their capacity building of their LEAs.

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) to deal with all types of cyber crime in the country, in a coordinated and comprehensive manner.

ii. 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 in 2023.

iii. 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) have provided its services to

State LEAs in around 8,840 cyber forensics like mobile forensics, memory forensics, CDR Analysis, etc. to help them in investigation of cases pertaining to cyber crimes.

iv. **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.**

v. **The 'Citizen Financial Cyber Fraud Reporting and Management System', under I4C, has been launched for immediate reporting of financial frauds and to stop siphoning off funds by the fraudsters. So far, financial amount of more than Rs. 1000 Crore have been saved in more than 4 lakh incidents. A toll-free Helpline number '1930' has been operationalized to get assistance in lodging online cyber incidents.**

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. along with**

certification. More than 72,800 Police Officers from States/UTs are registered and more than 50,000 Certificates issued through the portal.

vii. I4C has imparted cyber hygiene training to 5,600 officials of various Ministries/ Departments of Government of India.

viii. I4C has imparted cyber hygiene training to more than 17,000 NCC cadets.

ix. The Ministry of Home Affairs has provided financial assistance to the tune of Rs. 122.24 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. So far, cyber forensic-cum-training laboratories have been commissioned in 33 States/UTs. So far, more than 24,600 LEA personnel, judicial officers and prosecutors have been provided training on cyber crime awareness, investigation, forensics etc.

x. 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.

xi. 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, etc. The States/UTs have also been requested to carry out publicity to create mass awareness.

xii. The Ministry of Electronics and Information Technology conducts programmes to generate information security awareness. Books, videos and online materials about information security are developed for general users, children and parents, and are disseminated through portals such as www.infosecawareness.in and www.csk.gov.in

xiii. The Ministry of Electronics and Information Technology initiated the Cyber Surakshit Bharat (CSB) programme in public-private partnership to educate & enable the Chief Information Security Officers (CISOs) & broader IT community in Central/State Governments, Banks, PSUs and Government organizations to address the challenges of cyber security.

The training programmes are conducted in cities like Delhi, Gurgaon, Mumbai, Kolkata, Bangalore, Hyderabad, Chennai, Chandigarh, Bhopal, etc.

xiv. The Ministry of Electronics and Information Technology conducts online awareness level and advanced level training courses in cyber security for officials of Central Government Ministries/Departments to create awareness about cyber security in Government employees.

xv. The Indian Computer Emergency Response Team (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 42 training programmes have been conducted, covering 11,486 participants, during the years 2021 and 2022. In 2023, up to October, a total of 7007 officials from Government, critical sectors, public and private sector have been trained in 21 training programs in the area of cyber security.

xvi. CERT-In regularly disseminates information and shares security tips on cyber safety and security through its official social media handles and websites. CERT-In organised various events and activities for citizens during Safer Internet Day on 7.2.2023 and Cyber Security Awareness Month in October 2023, by posting security tips using posters and videos on social media platforms and websites.

CERT-In, in association with Centre for Development of Advanced Computing, conducted an online awareness campaign for citizens, covering topics such as general online safety, social media risks and safety, mobile related frauds and safety, secure digital payment practices, etc., through videos and quizzes on the My Gov platform.

xvii. CERT-In and the Reserve Bank of India (RBI) jointly carry out a cyber security awareness campaign on 'beware and be aware of financial frauds' through the Digital India Platform.

xviii. 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.

xix. 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.

xx. CERT-In has formulated a Cyber Crisis Management Plan for countering cyber attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.

xxi. CERT-In has empanelled 177 security auditing organisations to support and audit implementation of Information Security Best Practices.

xxii. Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 86 such drills have so far been conducted by CERT-In where 1159 organizations from different States and sectors participated.

xxiii. 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 42 training programmes have been conducted, covering 11,486 participants, during the years 2021 and 2022. In 2023, up to October, a total of 7007 officials from Government, critical sectors, public and private sector have been trained in 21 training programs in the area of cyber security.

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

*****