GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 410
TO BE ANSWERED ON: 24.07.2024

CYBER FRAUDS

410. SHRI K C VENUGOPAL:

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

(a) whether the Government is aware of the rising incidents of cyber frauds;
(b) if so, the details thereof;
(c) whether the Government have taken any specific initiatives or policies to mitigate fraud risks;
(d) whether the current redressal mechanism for victims of cyber frauds effective;
(e) if so, the details thereof;
(f) whether the Government has established collaborations with the law enforcement and private sector entities to combat cyber frauds; and
(g) if so, the details thereof?

ANSWER

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

(a) to (g):As per Ministry of Home Affairs (MHA), the 'Citizen Financial Cyber Fraud Reporting and Management System' was launched for immediate reporting of financial frauds and to stop siphoning off fund by the fraudsters. So far, financial amount of more than Rs. 2,400Crore has been saved in more than 7.6 lakh complaints.

'Police' and 'Public Order' are State subjects as per the Seventh Schedule of the Constitution of India. States/UTs are primarily responsible for the prevention, detection, investigation and prosecution of crimes including cyber frauds 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.

Government has taken following measures to enhance awareness among organisations and users for safe usage of digital technologies and prevent cyber frauds:

(i) The Government has established the Indian Cyber Crime Coordination Centre (14C) under Ministry of Home Affairs (MHA) to provide a framework and eco-system for LEAs to deal with cyber crimes in a comprehensive and coordinated manner. The Government has launched the National Cyber Crime Reporting Portal (https://cybercrime.gov.in) to enable the public to report all types of cyber crimes, with special focus on incidents reported on this portal are routed automatically to the respective State/UT law enforcement agency for further handling as per the provisions of law.

(ii) The 'Citizen Financial Cyber Fraud Reporting and Management System' was launched for immediate reporting of financial frauds and to stop siphoning off fund by the fraudsters. A toll-free Helpline number '1930' is operationalized to provide assistance in lodging online cyber complaints.

(iii) To strengthen the mechanism to deal with cyber crimes in a comprehensive and coordinated manner, the Central Government has taken steps for spreading awareness about cyber crimes; issuance of alerts/advisories; capacity building/training of law enforcement personnel/ prosecutors/ judicial officers; improving cyber forensic facilities, etc.

(iv) The Ministry of Home Affairs has taken many steps to spread awareness on cyber crime that inter-alia include; issuance of alerts/advisories, dissemination of messages through SMS, I4C social media account i.e Twitter handle (@Cyberdost), Facebook(CyberDostI4C), Instagram (cyberdostI4c), Telegram (cyberdostI4c), Radio campaign, engaged MyGov for publicity in multiple media, publishing of Handbook for Adolescents/Students, organizing of Cyber Safety and Security Awareness week, in association with policy department in different States/UTs etc. The Ministry of Home Affairs has issued advisory to all the State/UT Governments to carry out publicity of National Cyber Crime Reporting Portal (https://cybercrime.gov.in) and Toll-free helpline number '1930' to create mass awareness.

(v) The Indian Computer Emergency Response Team (CERT-In)issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers, mobile phones, networks and data on an ongoing basis.

(vi) CERT-In works in coordination with service providers, regulators and Law Enforcement Agencies (LEAs) to track and disable phishing websites and facilitate investigation of fraudulent activities.

(vii) CERT-In has issued an advisory to various Ministries outlining the measures to be taken for strengthening the cyber security by all entities that are processing the digital personal data or information including sensitive personal data or information.

(viii) CERT-In, through RBI, has advised all authorised entities and banks issuing pre-paid payment instruments (wallets) in the country to carry out special audit by CERT-In-empanelled auditors, close the non-compliances identified in the audit report and ensure implementation of security best practices.

(ix) CERT-In has empanelled 176 security auditing organisations to support and audit implementation of Information Security Best Practices.

(x) CERT-In has issued guidelines on information security practices for government entities in June 2023 covering domains such as data security, network security, identity and access management, application security, third-party outsourcing, hardening procedures, security monitoring, incident management and security auditing.

(xi) CERT-In operates 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.

(xii) 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.

(xiii) 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.

(xiv) Cybersecurity mock drills are conducted to enable assessment of cyber security posture and preparedness of organisations in the Government and critical sectors. 92 such drills have so far been conducted by CERT-In where around 1400 organizations from different States and sectors participated.

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

(xvi) CERT-In provides leadership for the Computer Security Incident Response Team-Finance Sector (CSIRT-Fin) operations under its umbrella for responding to and containing and mitigating cyber security incidents reported from the financial sector.

(xvii) CERT-In regularly conducts trainings / workshops to train officials of Government, Public and Private sector organizations across all sectors on focused topics of Cyber

Security. During 2024, till June, CERT-In has conducted 9 trainings on various specialized topics of cyber security covering 4,166 participants including system/Network Administrators and Chief Information Security Officers (CISOs).

(xviii) CERT-In, National Institute of Securities Markets and the Centre for Development of Advanced Computing (C-DAC) conducts a self-paced 60-hour certification Cyber Security Foundation Course for professionals in the financial sector.

(xix) Security tips have been published for users to secure their desktops and mobile phones and to prevent phishing attacks.

(xx) CERT-In regularly carry out various activities for awareness and citizen sensitization with respect to cyber-attacks and cyber frauds.

(xxi) 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.

(xxii) 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.

****