GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
**LOK SABHA**
**UNSTARRED QUESTION NO. 2624**
TO BE ANSWERED ON: 11.12.2024

## AWARENESS ABOUT CYBER THREATS

**†2624. SHRI RAM PRASAD CHAUDHARY:**

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

(a) whether the Government is aware that cyber criminals are becoming increasingly sophisticated, leveraging deepfake technology, Artificial Intelligence (AI) and social engineering/websites to do unbelievable scams; and

(b) if so, the steps taken/being taken by the Government to raise awareness about cyber threats, promote safe online behaviour and equip organisations with the necessary tools to tackle emerging digital risks?

**ANSWER**

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

(a) and (b): The policies of the Government are aimed at ensuring an open, safe, trusted and accountable internet for its users. Government is fully cognizant and aware of various cyber security threats including those due to emerging technologies. To strengthen the nation's cybersecurity posture, the Government has taken several key initiatives to raise awareness about cyber threats and promote safe online behaviour, which, inter alia, includes:

i. The Indian Computer Emergency Response Team (CERT-In) is designated as the national agency for responding to cyber security incidents under the provisions of section 70B of the Information Technology Act, 2000.

ii. National Cyber Coordination Centre (NCCC) implemented by the CERT-In serves as the control room to scan the cyberspace in the country and detect cyber security threats. NCCC facilitates coordination among different agencies by sharing with them the metadata from cyberspace for taking actions to mitigate cyber security threats.

iii. 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.

iv. Cyber Swachhta Kendra (CSK) is a citizen-centric service provided by CERT-In, which extends the vision of Swachh Bharat to the Cyber Space. Cyber Swachhta Kendra is the Botnet Cleaning and Malware Analysis Centre and helps 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.

v. CERT-In, through Reserve Bank of India, 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.

vi. CERT-In has empanelled 155 security auditing organisations to support and audit implementation of Information Security Best Practices.

vii. Cyber security mock drills are conducted regularly to enable assessment of cyber security posture and preparedness of organisations and enhance resilience in Government and critical sectors.

viii. CERT-In conducts regular training programmes for network and system administrators and CISOs of government, public and private sector organisations regarding securing information technology infrastructure and mitigating cyber-attacks.

ix. The Computer Security Incident Response Team-Finance Sector (CSIRT-Fin) has been setup for responding to and containing and mitigating cyber security incidents reported from the financial sector under the umbrella and guidance of CERT-In.

x. CERT-In operates an automated cyber threat intelligence exchange platform for proactively collecting, analysing and sharing tailored alerts with organisations across sectors for proactive threat mitigation actions by them.

xi. CERT-In issued Cyber Security Directions in April 2022 under sub-section (6) of section 70B of Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet.

xii. CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities including social engineering, phishing and vishing campaigns using Artificial Intelligence and countermeasures to protect computers, networks and data on an ongoing basis. In this context, an advisory on safety measures to be taken to minimize the adversarial threats arising from Artificial Intelligence (AI) based applications was published in May 2023.

xiii. CERT-In 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.

xiv. CERT-In issued an advisory to various Ministries in November 2023 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.

xv. CERT-In has published an advisory in November 2024 on deepfake threats and measures that need to be followed to stay protected against deepfakes.

xvi. National Informatics Centre (NIC) provides Information Technology (IT) support to ministries, departments and agencies of the Central Government, State Governments and district administrators for various e-governance solutions and follows information security policies and practices in line with industry standards and practices, aimed at preventing cyber attacks and safeguarding data.

xvii. The Ministry of Electronics and Information Technology conducts programmes to generate information security awareness. Awareness material in the form of handbooks, short videos, posters, brochures, cartoon stories for children, advisories, etc. on various aspects of cyber hygiene & cyber security including deepfakes are disseminated through portals such as www.staysafeonline.in,www.infosecawareness.inand www.csk.gov.in.

xviii. The Ministry of Home Affairs (MHA) has set up the Indian Cyber Crime Coordination Centre(I4C) to deal with all types of cybercrime. The MHA has launched the National Cyber Crime Reporting Portal (https://cybercrime.gov.in) to enable the public to report all types of cyber crimes. A toll-free number 1930 is made operational for citizens to get assistance in lodging online complaints in their own language.

********