GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 2131
TO BE ANSWERED ON: 09.08.2024

CYBER ATTACKS ON THE COUNTRY

2131. SHRI SANJAY RAUT:

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

(a) whether it is a fact that Indian Threat Landscape Report by Singapore-based cyber security firm Cyfirma indicates that cyber attacks on the country has gone up by nearly 300 per cent in three years between 2021 and September, 2023;
(b) whether it is a fact that services companies, BPOs witnessed the highest attacks;
(c) whether it is a fact that targeted cyber attacks on Government agencies has gone up by460 percent and on Start-ups and MSMEs has gone up by 500 per cent; and
(d) if so, the manner in which Government is planning to contain this and protect the country's cyberspace?

ANSWER

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

(a) to (d): Government has taken following measures to enhance the cyber security posture and prevent cyber attacks:

(i) 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.

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.

(ii) 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.

(iii) 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.

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

(v) 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.

(vi) 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.

(vii) 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.

(viii) 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.

(ix) Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 92 such drills have so far been conducted by CERT-In where around 1,400 organizations from different States and sectors participated.

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

(xi) 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.

(xii) CERT-In regularly conducts trainings / workshops to train technical staff of Government, Public and Private sector organizations including StartUps and Micro, Small and Medium Enterprises (MSMEs) 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).

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

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

(xv) 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.

(xvi) 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.

****