GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION. NO. 3822
TO BE ANSWERED ON: 18.12.2024

PREVENTION OF CYBER ATTACK

3822. SHRI TANUJ PUNIA:

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

(a) whether the Government has recently taken a few measures to prevent cyber attacks including creation of inter-departmental panel to coordinate with various agencies and if so, the details thereof;
(b) the number of cyber security incidents reported during each of the last three years;
(c) whether said cases were tracked by Indian Computer Emergency Response Team;
(d) if so, the details thereof and the necessary action taken in this regard; and
(e) whether any proactive measures have been taken for sharing alerts with organisations across the sectors and if so, the details thereof?

ANSWER

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

(a): The Government is committed to ensure that the Internet in India is Open, Safe, Trusted and Accountable for its users. The Government is fully cognizant and aware of various cyber security threats and challenges and has taken following measures to prevent cyber-attacks which, inter alia, includes:

(i) National Cyber Security Coordinator (NCSC) under the National Security Council Secretariat (NSCS) to ensure coordination amongst different agencies.
(ii) Under the provisions of section 70A of the Information Technology (IT) Act, 2000, the Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country.
(iii) Under the provisions of section 70B of the Information Technology Act, 2000, the Indian Computer Emergency Response Team (CERT-In) is designated as the national agency for responding to cyber security incidents.
(iv) Ministry of Home Affairs (MHA) has created Indian Cybercrime Coordination Centre (I4C) to deal with cybercrimes in a coordinated and effective manner.
(v) 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 to CERT-In within six hours of such incidents being noticed or being brought to notice for Safe & Trusted Internet.
(vi) 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.
(i) 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.

(ii) CERT-In conducts regular training programmes for network and system administrators and Chief Information Security Officers of government, public and private sector organisations regarding securing information technology infrastructure and mitigating cyber-attacks. A total of 9,807 officials have been trained in 20 training programs in 2024 (upto October).

(iii) 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.

(iv) Cyber security mock drills are being conducted to enable assessment of cyber security posture and preparedness of organisations in the Government and critical sectors. 104 such drills have so far been conducted by CERT-In where 1420 organizations from different States and sectors participated.

(v) 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.

(a) to (e): As per the information reported to and tracked by CERT-In, the total number of cyber security incidents in the last three years are given below:

Year	Number of cyber security incidents
2021	14,02,809
2022	13,91,457
2023	15,92,917

The following measures have been taken for sharing alerts with organisations across sectors:

i. 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.

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. 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.

iv. National Informatics Centre (NIC) has deployed advanced security tools including Threat Intelligence Platform to identify the security issues associated with Government network.

v. NCIIPC provides threat intelligence, situational awareness, alerts & advisories and information on vulnerabilities to organisations having Critical Information Infrastructure (CIIs)/ Protected Systems (PSs) for taking preventive measures from cyber attacks and cyber terrorism.

vi. CERT-In collaborates with industry to exchange information on latest cyber threats, best practices and conduct joint capacity building programs.

vii. 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.in and www.csk.gov.in.

****