GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
STARRED QUESTION NO. *18
TO BE ANSWERED ON: 03.02.2023

MEASURES TO PREVENT CYBER ATTACKS

***18. SHRI M. SHANMUGAM:**

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

(a) whether Government has recently taken a few measures to prevent cyber attacks, including creation of inter-Departmental panel to coordinate with various agencies;

(b) if so, the details thereof;

(c) the number of cyber security incidents reported in the last three years, year-wise;

(d) whether those cases were tracked by Indian Computer Emergency Response Team(CERT-In) and necessary action taken, the details thereof; and

(e) whether any proactive measures have been taken for sharing alerts with organisations across the sectors, if so, the details thereof?

ANSWER

MINISTER FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI ASHWINI VAISHNAW)

(a) to (e): A statement is laid on the Table of the House.

STATEMENT REFERRED TO IN REPLY TO RAJYA SABHA STARRED QUESTION NO.*18 FOR 03.02.2023 REGARDING MEASURES TO PREVENT CYBER ATTACKS

……

(a) and (b): Measures to prevent cyber-attacks are taken on an ongoing basis. As per section 70B of the Information Technology Act, 2000, the Indian Computer Emergency Response Team (CERT-In) is the national agency for coordination of cyber incident response activities. Number of measures have been taken to prevent cyber-attacks, including in recent times. The same include the following:

(i) CERT-In, in April 2022, issued directions under section 70B for mandatory reporting of cyber incidents to CERT-In within six hours of such incidents being noticed or being brought to notice.

(ii) CERT-In, in December 2022, issued a special advisory on best practices to enhance the resilience of health sector entities, and has requested the Ministry of Health and Family Welfare to disseminate the same to all authorised medical care entities and service providers in the country.

(iii) Cyber security best practices have been issued in September 2022 for adherence by all government employees, including outsourced, contractual and temporary employees who work for Central Government's Ministries and Departments.

(iv) CERT-In has formulated a Cyber Crisis Management Plan for countering cyber-attacks and cyber-terrorism, for implementation by all Ministries and Departments of the Central Government, State Governments and their organisations and critical sectors.

(v) CERT-In has empanelled 150 security auditing organisations to support and audit implementation of Information Security Best Practices.

(vi) Chief Information Security Officers (CISOs) have been appointed in various Central Government Ministries and Departments as nodal officers for ensuring cyber hygiene and security aspects of their respective Ministry/Department. CISOs are sensitised regarding their roles and responsibilities and salient aspects of cyber security through skill enhancement programme.

(vii) CERT-In, on an ongoing basis, disseminates information and shares security tips on cyber safety and security through its official social media handles and websites. CERT-In has organised various events and activities for citizens during the Safe Internet Day on 8.2.2022 and the Cyber Security Awareness Month in October 2022, by posting security tips and videos on social media platforms and websites.

(viii) CERT-In, in association with the Centre for Development of Advanced Computing (C-DAC), has 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 MyGov platform.

(ix) CERT-In, on an ongoing basis, issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks.

(x) Security tips are published for users to secure their desktops and mobile phones and to prevent phishing attacks.

(xi) The Ministry of Home Affairs has created the National Counter Ransomware Taskforce, comprising of multiple stakeholders, to formulate strategies to effectively tackle ransomware threats and put in place proactive and responsive systems by stakeholders. The Taskforce comprises Working Groups on Cooperation and Diplomacy, Incident Response, Security Cluster, Awareness and Capacity Building.

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

(xiii) CERT-In regularly conducts training programmes for network and system administrators and CISOs of government and critical sector organisations, regarding securing the information technology infrastructure and mitigating cyber-attacks. A total of 42 training programmes were conducted, covering 11,486 participants, during the years 2021 and 2022.

(xiv) Cyber security mock drills are being conducted to enable assessment of cyber security posture and preparedness of organisations in the government and the critical sectors. 74 such drills have so far been conducted by CERT-In, in which 990 organisations from various States and sectors participated.

(c) and (d): As per the information reported to and tracked by CERT-In, a total of 11,58,208, 14,02,809 and 13,91,457 cyber security incidents were observed during the years 2020, 2021 and 2022 respectively. CERT-In receives inputs from its situational awareness systems and threat intelligence sources about malware infections and vulnerabilities in networks of entities across sectors and issues alerts to the organisations and sectoral Computer Security Incident Response Teams (CSIRTs) concerned for remedial measures. It also co-operates and works with, and coordinates incident response measures, with affected organisations, service providers and law enforcement agencies.

(e): The following measures have been taken for sharing alerts with organizations across sectors:

(i) CERT-In has set up the National Cyber Coordination Centre to generate situational awareness regarding existing and potential cyber security threats. It 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.

(ii) CERT-In operates the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) to detect malicious programs and offer free tools to remove the same, and to provide cyber security tips and best practices for citizens and organisations.

******