GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 762
TO BE ANSWERED ON: 07.02.2024

PREVENTION OF CYBER ATTACK

762. SHRI MANOJ TIWARI:
DR. NISHIKANT DUBEY:

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;
(b) if so, the details thereof;
(c) the number of cyber security incidents reported in the last three years, year-wise;
(d) whether said cases were tracked by Indian Computer Emergency Response Team (CERT-In) and necessary action taken, and if so, the details thereof; 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 RAJEEV CHANDRASEKHAR)

(a) and (b): The policies of the Government are aimed at ensuring an Open, Safe and Trusted and Accountable Internet for its users. Government is fully cognizant and aware of various cyber security threats and challenges and has taken following measures to enhance the cyber security posture and prevent cyber-attacks:

(i) Indian Computer Emergency Response Team (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 (MoHFW) to disseminate the same to all authorised medical care entities and service providers in the country.
(iii) 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.
(iv) The office of National Cyber Security Coordinator (NCSC) has been established to coordinate, oversee and in compliance of Cyber Security policies. The function of NCSC, inter alia, includes advise and ensure implementation of action plans for cyber security by nodal agencies in their areas of responsibility.
(v) To mitigate cybersecurity risks on telecom networks, the National Security Directive on Telecommunication Sector has been mandated with effect from 15 June 2021.
(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 issues alerts and advisories regarding latest cyber threats/vulnerabilities

and countermeasures to protect computers and networks on an ongoing basis.

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

(ix) 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.

(x) CERT-In has empanelled 177 security auditing organisations to support and audit implementation of Information Security Best Practices.

(xi) Cyber security mock drills are conducted to enable assessment of cyber security posture and preparedness of organisations in the Government and critical sectors. 87 such drills have so far been conducted by CERT-In where 1173 organizations from different States and sectors participated.

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

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

(c): As per the information reported to and tracked by CERT-In, a total of 14,02,809, 13,91,457 and 15,92,917 cyber security incidents were observed during the years 2021, 2022 and 2023 respectively.

(d): 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. CERT-In co-operates, works and coordinates incident response measures with affected organisations, service providers as well as law enforcement agencies.

(e): Government has taken following proactive measures for sharing alerts with organizations across the sectors:

(i) 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.

(ii) CERT-In has set up the National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities.

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

(iv) The analytic centre at National Critical Information Infrastructure Protection Center (NCIIPC) provides near real time threat intelligence and situational awareness based on which regular alerts and tailored advisories are sent to Critical Information Infrastructure/ Protected System entities.

****