GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 2461
TO BE ANSWERED ON: 15.03.2023

CYBER HACKING

2461. SHRIMATI VANGA GEETHA VISWANATH:

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

(a) whether hackers from other countries have targeted Indian Government organisations and private reputed companies;
(b) if so, the details thereof alongwith the monetary losses incurred due to these attacks from hackers;
(c) the details of the number of cases and action undertaken on culprits since 2021;
(d) the details of major hacking incidents which occurred in India since 2021;and
(e) the steps taken by the Government to curb such cyber hacking?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAJEEV CHANDRASEKHAR)

(a) and (b): Government is cognizant and aware of various cybersecurity threats and is committed to ensure that the Internet in India is Open, Safe and Trusted and Accountable for its users.

There have been attempts from time to time to launch cyber-attacks in the Indian cyberspace from systems within and outside the country. It has been observed that the attackers compromise computer systems located in different parts of the world and use masquerading techniques and hidden servers to hide the identity of actual systems from which they launch the attacks.

Threat actors continue to modernise attack methodologies and exploit known vulnerabilities, compromised credentials of remote access services and phishing campaigns for gaining access to the infrastructure of organisations across sectors.
With innovation in technology and rise in usage in the cyberspace and digital infrastructure for businesses and services, cyber-attacks pose a threat to confidentiality, integrity and availability of data and services, which may have indirect or direct impact on the economy of businesses and service providers. Such economic impact is specific to the impacted entity, and depends on the extent to which its data, assets and services are affected by such attacks.

(c) and (d): As per information reported to and tracked by the Indian Computer Emergency Response Team (CERT-In),during the years 2021 and 2022,14,02,809 and 13,91,457 cybersecurity incidents respectively were observed, including 42 and 50 incidents respectively of hacking of websites belonging to the Central Government and the State Governments. CERT-In notifies the affected organisations, along with remedial actions to be taken, and coordinates incident response measures with affected organisations, service providers, respective sector regulators and law enforcement agencies.

(e): A number of measures have been taken to enhance India's cybersecurity posture and to curb such incidents. These include the following:

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

(ii) On observing an incident, CERT-In notifies the affected organisations along with remedial actions to be taken, and coordinates incident response measures with affected organisations, service providers, respective sector regulators and law enforcement agencies.

(iii) Regular training programmes for network and system administrators and the Chief Information Security Officers of government and critical sector organisations are conducted by CERT-In, for 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.

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

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

(vi) The National Cyber Coordination Centre has been set up to generate situational awareness regarding existing and potential cyber security threats. CERT-In shares the tailored alerts with organisations across sectors for proactive threat mitigation actions by them.

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

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

****