GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
STARRED QUESTION NO. *320
TO BE ANSWERED ON: 31.03.2023

NATIONAL CYBER SECURITY STRATEGY

***320. SHRI K.C. VENUGOPAL:**

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

(a) the number of cyber attacks on Government websites every year since 2018;
(b) the number of cyber attacks on health institutions like public and private hospitals and insurance agencies, every year since 2018;
(c) whether the draft National Cyber Security Strategy will include measures for protection of Indian cybersecurity infrastructure to prevent large scale data breaches such as that of 3.8 crore DigiLocker accounts in 2020 and 110 crore Aadhar accounts in 2018;
(d) if so, details thereof, and if not, the reasons therefor; and
(e) measures Government plans to take under the Strategy to protect Indian Government websites in particular?

ANSWER

MINISTER OF ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI ASHWINI VAISHNAW)

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

STATEMENT REFERRED TO IN THE REPLY TO RAJYA SABHA STARRED QUESTION NO. *320 FOR 31.3.2023, REGARDING NATIONAL CYBER SECURITY STRATEGY

(a) and (b): Government is committed to ensure that Internet in India is Open, Safe and Trusted and Accountable for its users. With emergence of new technology and rise in the usage of Internet, the growing risk to digital data in the cyberspace is a global phenomenon, and Government is fully cognizant of such cyber risks.

The Indian Computer Emergency Response Team (CERT-In) is mandated to track and monitor cybersecurity incidents in India. The number of incidents of hacking of websites of Central Ministries/Departments and State Governments and of cyber incidents pertaining to health institutions, reported by CERT-In on the basis of incidents reported to and tracked by it, is as under:

Year	Website hacking incidents of Central Ministries/Departments and State Governments	Cybersecurity incidents pertaining to Health institutions
2018	110	665
2019	54	1,108
2020	59	2,889
2021	42	1,904
2022	50	2,712

(c) to (e): Government has undertaken the finalisation of a National Cyber Security Strategy to holistically looks at all issues of security in the national cyberspace, capture all cyber-threat concerns, detail the mechanism and roadmap for the protection of India’s digital assets, especially critical information infrastructure, and capacity building activities to deal with cyber-attacks.

The following steps have been taken for cybersecurity, protection of cybersecurity infrastructure to prevent data breaches and protecting Indian Government websites:

(i) On observing cyber security incidents, 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 as well as Law Enforcement Agencies.

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

(iii) 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.

(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) The Guidelines for Indian Government Websites address common policy issues and practical challenges faced by government organisations during the development and management of Indian Government websites and portals, and recommend policies and guidelines for the same. Government websites and applications are audited with respect to cybersecurity and compliance with the Government of India Guidelines for Websites prior to their hosting.

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

(vii) CERT-In conducts regular training programmes for network and system administrators and the Chief Information Security Officers 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.

(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.

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

(x) 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.

(xi) CERT-In regularly disseminates information and shares security tips on cyber safety and security through its official social media handles and websites. CERT-In organised various events and activities for citizens during Safer Internet Day on 7 February 2023 and Cyber Security Awareness Month in October 2022, by posting security tips using posters and videos on social media platforms and websites. CERT-In, in association with Centre for Development of Advanced Computing, 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.

(xii) The Ministry of Electronics and Information Technology conducts programmes to generate information security awareness. Specific books, videos and online materials are developed for children, parents and general users about information security, which are disseminated through portals such as www.infosecawareness.in and www.csk.gov.in.

*****