GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION. NO. 2466
TO BE ANSWERED ON: 16.03.2022

WEBSITE HACKING

2466. SHRI RAMCHARAN BOHRA:

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

(a) whether the Government is aware of several cases of website hacking;
(b) if so, the details thereof during the last three years;
(c) whether the Government has taken any steps to secure the computer systems from hacking; and
(d) if so, the details thereof?

ANSWER

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

(a) and (b): Yes, Sir. The Government is committed to ensure that the Internet in India is Open, Safe & Trusted and Accountable for all users. Indian Computer Emergency Response Team (CERT-In) is mandated to track and monitor cyber security incidents in India. CERT-In has reported that a total number of 24768, 26121 and 28897 Indian websites were hacked during the year 2019, 2020 and 2021respectively.

(c) and(d): Government is fully cognizant and aware of various cyber security threats; and has taken following measures to enhance the cyber security posture and prevent cyber-attacks:

i. The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on regular basis.
ii. CERT-In is operating 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.
iii. Government has issued guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.
iv. All the government websites and applications are audited with respect to cyber security prior to their hosting. The auditing of the websites and applications is conducted on a regular basis after hosting also.
v. CERT-In has empanelled 96 security auditing organisations to support and audit implementation of Information Security Best Practices.

vi. CERT-In has formulated a Cyber Crisis Management Plan for countering cyber attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.

vii. Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 64 such drills have so far been conducted by CERT-In where 820 organizations from different States and sectors participated.

viii. CERT-In conducts regular training programmes for network / system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organisations regarding securing the IT infrastructure and mitigating cyber attacks. 15 and 19 training programs were conducted covering 708 and 5169 participants during the year 2020 and 2021 respectively.

ix. CERT-In is operating the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre is providing detection of malicious programs and free tools to remove the same.

x. CERT-In has set up the National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats. Phase-I of NCCC is operational.

xi. CERT-In also co-operates, works and coordinates incident response measures with international CERTs, overseas organisations and service providers as well as Law Enforcement Agencies.

xii. The analytic centre at National Critical Information Infrastructure Protection Centre (NCIIPC) provides near real time threat intelligence and situation awareness based on which regular alerts and advisories are sent to Critical Information Infrastructure / Protected System entities to avert cyber-attacks.

xiii. Ministry of Home Affairs (MHA) has issued National Information Security Policy and Guidelines (NISPG) to the Central Ministries as well as the State Governments/Union Territories in order to prevent information security breaches/Cyber intrusions in ICT infrastructure.

****