GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 1937
TO BE ANSWERED ON: 05.12.2019

STEPS TAKEN TO IMPROVE THE SECURITY OF WEBSITES

1937. **SHRI A. VIJAYAKUMAR:**

Will the Minister of Electronics & Information Technology be pleased to state:-

(a) whether Government is aware that many of Government websites are vulnerable to hacking;

(b) whether Government would take steps to improve the security of websites, particularly Government websites;

(c) whether many incidents of data theft have occurred in the country; and

(d) if so, the action taken to protect Indian data?

ANSWER

MINISTER FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAVI SHANKAR PRASAD)

(a): As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In) a total number of 199, 172, 110 and 48 websites of Central Ministries/Departments and State Governments were hacked during the year 2016, 2017, 2018 and 2019 (till October) respectively.

(b), (c) and (d): With the innovation of technology and rise in usage of cyber space for businesses, the cyber-attacks are on the rise in the country as well as globally. Such cyber-attacks target organizations and users to gain unauthorized access to data. Government is aware of such instances.

In tune with the dynamic nature of Information Technology and emerging cyber threats, continuous efforts are required to be made by owners to protect data and networks by way of hardening and deploying appropriate security controls.

Government has taken following measures to enhance the cyber security posture and prevent cyber attacks:

(i) Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country, as per the provisions of section 70A of the Information Technology (IT) Act, 2000.

(ii) 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.

(iii) Security tips have been published for users to secure their Desktops, mobile/smart phones and preventing phishing attacks.

(iv) Government has issued guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.

(v) All the government websites and applications are to be audited with respect to cyber security prior to their hosting. The auditing of the websites and applications will be conducted on a regular basis after hosting also.

(vi) Government has empanelled 90 security auditing organisations to support and audit implementation of Information Security Best Practices.

(vii) Government has formulated 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.

(viii) Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 44 such drills have so far been conducted by CERT-In where 265 organisations from different States and sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS, etc participated.

(ix) 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. 19 trainings covering 515 participants conducted in the year 2019 till October.

(x) Government has launched 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.

(xi) Government has set up 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. Phase-I of NCCC has been made operational.

(xii) Ministry of Electronics & Information Technology (MeitY) is conducting programs 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 Portal "www.infosecawareness.in".

******