GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 1848
TO BE ANSWERED ON: 03.07.2019

CYBER SECURITY BREACHES

1848. DR. SANJAY JAISWAL:

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

(a) whether there has been a rise in the number of cyber security breaches in the country in the past few years;
(b) if so, the details thereof along with the steps taken/being taken by the Government in this regard; and
(c) the steps taken/being taken by the Government to strengthen cyber security in the country?

ANSWER

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

(a) to (c): As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In) a total number of 53117, 208456 and 105849 cyber security incidents including phishing, network scanning and probing, virus / malicious code and website hacking are reported during the year 2017, 2018 and 2019 (till May) respectively.

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

Government has taken several steps to prevent cyber security incidents and enhancing cyber security in the country. These, *inter alia,* include:

(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 and countermeasures on regular basis. CERT-In has published guidelines for securing IT infrastructure, which are available on its website (www.cert-in.org.in).
(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 to be audited with respect to cyber security prior to their hosting. The auditing of the websites and applications are conducted on a regular basis after hosting also.

(v) Government has empanelled 84 security auditing organisations to support and audit implementation of Information Security Best Practices.

(vi) All organizations providing digital services have been mandated to report cyber security incidents to CERT-In expeditiously.

(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 and exercises are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 43 such exercises have so far been conducted by CERT-In where organisations from different sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS sectors 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. 24 trainings covering 845 participants conducted in the year 2018.

(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.

****