GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 1804
TO BE ANSWERED ON: 03.07.2019

HACKING OF WEBSITES

1804. SHRI GAJANAN KIRTIKAR: SHRI BIDYUT BARAN MAHATO: SHRI SUDHEER GUPTA :

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

(a) whether several cases of hacking of websites, belonging to important institutions like MHA etc. have been reported in the country;
(b) if so, the details thereof and the reaction of the Government thereto along with the corrective steps taken by the Government in this regard;
(c) whether the Government has earmarked any agency for quick response to such exigencies;
(d) if so, the details thereof and if not, the reasons therefor along with the other corrective measures being taken by the Government in this regard; and
(e) whether the Government has any action plan/proposes to formulate any action plan to counter such cases in near future and if so, the details thereof?

ANSWER

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

(a) to (e): As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In) a total number of 199, 172, 110 and 25 websites of Central Ministries/Departments and State Governments were hacked during the year 2016 , 2017, 2018 and 2019 (till May) respectively.

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.

****