GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO.4127
TO BE ANSWERED ON: 18.03.2020

HACKING OF GOVERNMENT WEBSITES

4127. SHRI KRUPAL BALAJI TUMANE:

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

(a) the number of incidents of Government website hacking reported during each of the last three years, State/UT-wise;

(b) whether the Government has taken any steps to protect these websites from hacking in view of sensitive information present therein and if so, the details thereof; and

(c) whether the Government has set up any special cell to ascertain the details of hacked websites and the person responsible for it along with restoring the hacked websites and if so, the details thereof?

ANSWER
MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI SANJAY DHOTRE)

(a): As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In) a total number of 172, 110 and 54 websites of Central Ministries/Departments and State Governments were hacked during the year 2017, 2018 and 2019 respectively.

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

(i) CERT-In is regularly tracking the hacking of websites and alerts the website owners concerned to take actions to secure the websites to prevent recurrence. Restoration of the affected website is done after taking necessary remedial measures.

(ii) 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 will be conducted on a regular basis after hosting also.

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

(vi) Government has formulated guidelines for 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. 46 such drills have so far been conducted by CERT-In where 362organisations from different States and sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS, etc 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. 23 trainings covering 692 participants conducted in the year 2019.

(ix) 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.

(x) 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.

****