GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
STARRED QUESTION NO.*31
TO BE ANSWERED ON: 12.12.2018

WEBSITE HACKING

***31 SHRI HARISH CHANDRA ALIAS HARISH DWIVEDI:**

Will the Minister of Electronics & 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 system from hacking; and
(d) if so, the details thereof?

ANSWER

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

(a) to (d): A Statement is laid on the Table of the House.

STATEMENT REFERRED TO IN REPLY TO LOK SABHA STARRED QUESTION NO. *31 FOR 12-12-2018 REGARDING WEBSITE HACKING

……..

(a) and (b): As per information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), 33147, 30067 and 15779 Indian websites were hacked during the years 2016, 2017 and 2018 (upto November) respectively.

(c) and (d): 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 following measures to enhance the cyber security and prevent cyber attacks:

(i) 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.certin.org.in).

(ii) 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.

(iii) Cyber security exercises are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 38 such exercises have so far been conducted by CERT-In, wherein organisations from different sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS etc participated.

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

(v) New 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.

(vi) Government has empanelled 76 security auditing organisations to support and audit implementation of Information Security Best Practices.

(vii) 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.

******