

**GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA**

UNSTARRED QUESTION NO:2382

ANSWERED ON:11.03.2015

HACKING OF WEBSITES

Sawaikar Shri Advocate Narendra Keshav, Shekhawat Shri Gajendra Singh

Will the Minister of COMMUNICATIONS AND INFORMATION TECHNOLOGY be pleased to state:

- (a) whether the websites of the Government of India have been hacked, if so, the details thereof;
- (b) whether there are any incidents of hacking of websites of any State Government/ Ministries/ Department of Government of India during the last three years and the current year, if so, the details thereof; and
- (c) the action taken and/ or the action that Government proposes to take to check recurrence of such incidents?

Answer

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

(a) and (b): The Government websites host information for public dissemination. No sensitive information is hosted on Government websites. As per the guidelines of the Government, the Computer systems with sensitive information are isolated from Internet.

As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In) a total number of 371, 189, 155 & 13 Government websites hosted under 'gov.in' & 'nic.in' domains were hacked by various hacker groups during the year 2012, 2013, 2014 and 2015 (January) respectively. This include 252, 135, 92 and 6 nos. of websites of State Governments hosted on 'gov.in' and 'nic.in' in the year 2012, 2013, 2014 and 2015 (January) respectively.

(c): The website owners of all the hacked websites were informed by CERT-In to immediately remove the hacked pages from the web servers and conduct thorough security audit of the hacked websites and associated IT infrastructure to identify and address the vulnerabilities to secure the websites to avoid such kind of incidents.

Government has also taken other actions to check recurrence of such incidents and secure the websites from hacking, these include:

i) All Central Government Ministries / Departments and State / Union Territory Governments have been advised to conduct security auditing of entire Information Technology infrastructure. All the new government websites and applications are to be audited with respect to cyber security prior to their hosting. The auditing of the websites and applications is to be conducted on a regular basis after hosting also. Indian Computer Emergency Response Team (CERT-In) provides necessary expertise to audit IT infrastructure of critical and other ICT sectors.

ii) It has been mandated that all government websites are to be hosted on infrastructure of National Informatics Centre (NIC), Education and Research Network (ERNET) or any other secure infrastructure service provider in the country.

iii) National Informatics Centre (NIC) which hosts the government websites is continuously engaged in upgrading and improving the security posture of its hosting infrastructure.

iv) National Informatics Centre (NIC) has been directed not to host web sites, which are not audited with respect to cyber security.

v) All major websites are being monitored regularly to detect malicious activities. A 24x7 security monitoring centre is operational in NIC for responding to security incidents. The security events generated from various security solutions on NIC Network (NICNET) are monitored round the clock for taking remedial measures.

vi) 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 the websites, which are available on its website (www.cert-in.org.in). CERT-In also conducts regular training programmes to make the system administrators aware about secure hosting of the websites.