GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 1210
TO BE ANSWERED ON: 10.03.2017

HACKING OF AIRPORT WEBSITES

1210 SHRI RAJEEV CHANDRASEKHAR:

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

(a) whether it is a fact that a server containing 148 domains of Indian airport websites including Cochin and Trivandrum was hacked by Pakistani cyber criminals, if so, the details thereof; and
(b) whether data on the server was stolen and domains compromised; and
(c) the details of steps taken/proposed to be taken by Government in this regard and its preparedness to deal with such cyber attacks?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI P.P. CHAUDHARY)

(a): The official websites of Kochi and Thiruvananthapuram International airports were not hacked. It has been reported that some private websites in the name of Kochi airport and Thiruvananthapuram airport were hacked in December 2016. These hacked websites are registered and hosted in USA.

(b) and (c): As the official websites Kochi and Thiruvananthapuram International airports were not hacked, no official data of these websites were stolen.

Government has taken the following steps to prevent cyber attacks and secure the websites:

i) All government websites and applications are required to be audited with respect to cyber security prior to their hosting. The auditing of the websites and applications is being conducted on a regular basis after hosting also. The Indian Computer Emergency Response Team (CERT-In) has empanelled 32 security auditing organisations to support and audit implementation of Information Security Best Practices.
ii) NIC which hosts the government websites is continuously engaged in upgrading and improving the security posture of its hosting infrastructure.
iii) 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. CERT-In also issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis.
iv) Government has formulated a Cyber Crisis Management Plan (CCMP) for countering cyber attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.
v) Comprehensive Cyber Security Mock Drills are being regularly held to assess preparedness of organizations to withstand cyber attacks. So far, 11 such drills have been conducted with participation from 110 organizations.

vi) CERT-In has published guidelines for securing IT infrastructure, which are available on its website (www.certin.org.in) and are used by Central Ministries/Departments and State Governments to secure their IT Infrastructure.

****