GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 5316
TO BE ANSWERED ON: 28.03.2018

CYBER ATTACK

5316. SHRI DUSHYANT CHAUTALA

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

(a) whether the Indian Computer Emergency Response Team (CERT-In) has issued an alert about spread of a new malicious software being circulated through spam messages that can potentially lock computers and demand ransom for restoring access to users;

(b) if so, the total amount of damages that have been reported through this malware ; and

(c) the steps taken by the Government to prevent cyber attacks in future?

ANSWER
MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI K. J. ALPHONS)

(a) and (b): The Indian Computer Emergency Response Team (CERT-In) is regularly publishing Alerts and Advisories about the malware threats. CERT-In issued an alert regarding spread of variants of ransomware called "Locky" through spam mail messages. Locky ransomware is a type of malicious software that infects a computer and restricts users' access to affected files by encrypting them until a ransom is paid to unlock it. Countermeasures to prevent the infection were suggested in the said alert published on websites of CERT-In and Cyber Swachhta Kendra. No damage has been reported to CERT-In.

(c): Government has taken following measures to prevent cyber attacks and enhance cyber security in the country:

(i) The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect systems and mobile devices.
(ii) Security tips are published for users to secure their Desktops and mobile/smart phones.
(iii) 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.
(iv) 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.
(v) Cyber security exercises are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 25 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.
(vi) Government has issued general guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.
(vii) Government has empanelled 67 security auditing organisations to support and audit implementation of Information Security Best Practices.
(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. 22 training programs covering 610 participants were conducted during the year 2017.

(ix) 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 already been made operational.

*****