GOVERNMENT OF INDIA
MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY
(DEPARTMENT OF ELECTRONICS & INFORMATION TECHNOLOGY)
LOK SABHA
UNSTARRED QUESTION NO. 172
TO BE ANSWERED ON: 24.02.2016

PROTECTION OF DATA

172 SHRI C.S. PUTTA RAJU:

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

(a) whether the Government has taken any steps to protect the data pertaining to individuals and their privacy in the country in view of increasing data thefts using malware;

(b) if so, the details thereof; and

(c) if not, the reasons therefor ?

ANSWER

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

(a) and (b): With the innovation of technology and rise in usage of cyber space for businesses, the cyber attacks such as spam, spoofing, phishing and malicious software or malware are also on the rise. Such cyber attacks target users to trick them to divulge information such as online credentials and steal data from computers. Incidents of malware infections in Indian cyber space are reported to and tracked by the Indian Computer Emergency Response Team (CERT-In). Some of the latest malware targeting computer systems and mobile devices include Capahaw, Dorkbot, corebot, Golroted, Kilim, Android.Badaccents, Cridex Trojan, Android Opfake, Dyreza, ZeroAccess, ZeuS etc.

Government has taken the following steps to prevent malware attacks and data theft:

i. Alerts and advisories about the malware threats are being issued regularly by the Indian Computer Emergency Response Team (CERT-In). Measures to be taken to detect infected systems, tools to dis-infect the same and prevent further propagation are also being advised regularly to organizations and published on website "www.cert-in.org.in" for all users.

ii. CERT-In, Department of Electronics & Information Technology (DEITY) has initiated action with active participation of Service Providers and Industry to set up a Botnet Cleaning and Malware Analysis centre for detection of computer systems infected by

malware and to notify, enable cleaning and securing systems of end users to prevent further malware infections.

iii. CERT-In is working in coordination with Reserve Bank of India (RBI) and banks to track and disable phishing websites.

iv. To create awareness about possible frauds by using email and SMS, advisories are being issued by Banks, Telecom Service Providers and Police Authorities from time to time to the users.

v. Banks are creating user awareness for general public against phishing, lottery scams, internet banking, Credit/Debit cards and other frauds.

vi. The Information Technology Act, 2000, provides legal framework to address various types of prevalent cyber crimes and security breaches of information technology infrastructure. Section 43, Section 43A Section 66, Section 66B, Section 66C, Section 66D and Section 72A of the Information Technology Act, 2000 provides comprehensive legal framework for privacy and Security of data in digital form. Sections 43 and 43A of the Act provides for compensation to be paid to the victim in case of unauthorized access of information and leakage of sensitive personal information respectively. Section 43A also mandates that body corporate, who collect personal data or information must provide privacy policy for handling of or dealing in personal information including sensitive personal data or information on their websites. They are also required to implement reasonable security practices and procedures to protect the information.

vii. Department of Electronics & Information Technology (DEITY) is conducting programs to generate information security awareness. Specific books, videos and online materials are developed for children, parents and general users about information security which are disseminated through Portals like"www.infosecawareness.in", "www.secureyourelectronics.in" and "www.cert-in.org.in".

(c): Does not arise.

****