GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA

STARRED QUESTION NO:349
ANSWERED ON:17.12.2014
DATA PROTECTION AND PRIVACY
Karandlaje Km. Shobha;Patel Shri Dilip

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

(a) whether UN has urged India to strengthen its data protection and privacy;

(b) if so, the details thereof and the steps being taken by the Government in this regard;

(c) whether the Government is aware of instances of data theft using malwares;

(d) if so, the details thereof and the steps taken/proposed to be taken in this regard; and

(e) whether the Government proposes to enact a legislation for data privacy, strict cyber disclosure norms and curtail security breaches and if so, the details thereof?

Answer

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

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

STATEMENT REFERRED TO IN REPLY TO LOK SABHA STARRED QUESTION NO.349 FOR 17.12.2014 REGARDING DATA PROTECTION AND PRIVACY.

(a) and (b): No, Sir. However, United Nations (UN) has adopted resolutions numbered A/ HRC/DEC/25/11-UN Human Rights Council and A/c.3/69/L.26 − UN General Assembly, on right to Privacy in the digital age. There is no provision in the said resolutions to urge states which includes India as a UN member to strengthen data protection and privacy. The emphasis of discussions on this topic have been around safeguarding the right to privacy.

(c): 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). However, no user has specifically reported theft of data. Some of the latest malware targeting computer systems and mobile devices include FakeInst, Android Opfake, Dyreza, Regin, Backoff POS, ZeroAccess and ZeuS.

(d): Government has taken following steps for protecting Indian cyber space from malware attacks :

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 is working in coordination with Reserve Bank of India and banks to track and disable phishing websites.

iii) CERT-In, Department of Electronics & Information Technology (DEITY), has initiated action with active participation of Service Providers and Industry to set up a 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.

iv) The Government has circulated Computer Security Policy and Guidelines to all the Ministries/Departments on taking steps to prevent, detect and mitigate cyber attacks for securing information and prevention of data theft.

v) CERT-In is conducting mock cyber security drills to enable assessment of preparation of organizations including Banks and financial institutions to withstand cyber attacks.

vi) Department of Electronics & Information Technology (DEITY) regularly conduct programs to generate information security awareness. Specific book, videos and online materials are developed for children, parents and general users about information security which are disseminated through Portals like "secureyourpc.in" and "www.secureyourelectronics.in".

(e): Section 43, Section 43A 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. Indian Computer Emergency Response Team (CERT-In) has also empanelled auditors to facilitate body corporate to audit their information technology infrastructure and implementation of security best practices.

In addition, Government has initiated consultation for drafting a legislation that will provide protection to individuals in case their privacy is breached through unlawful means.