GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 245
TO BE ANSWERED ON: 03.02.2017

LEGISLATION FOR PROTECTION OF DATA AND PRIVACY

245 SHRI RAJEEV SHUKLA:

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

(a) whether Government is aware of increasing cyber crimes involving breach of privacy and cheating, if so, the action taken in this regard; and

(b) whether there is any proposal to bring legislation regarding data protection and privacy in the digital domain, if so, the details thereof?

ANSWER

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

(a): With the growth of technology and rise in usage of cyber space for businesses, the cyber crimes involving breach of privacy and cheating (such as phishing and identity theft, etc.) continue to occur in the country like elsewhere in the world. Cyber attacks such as phishing target users to trick them to divulge information such as online credentials.

(i). RBI has registered a total of 9500, 13083, 16468, and 8689 cases of frauds involving credit cards, ATM / debit cards and internet banking during the year 2013-14, 2014-15, 2015-16 and 2016-17(upto December 2016), respectively.

(ii). As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In) a total number of 1122, 534 and 757 phishing incidents were handled during the year, 2014, 2015 and 2016 respectively.

(iii). As per the data maintained by National Crime Records Bureau (NCRB), a total of 16 and 20 cases were registered under breach of confidentiality/privacy during the year 2014 and 2015, respectively and 1115 and 2255 cases were registered under Cheating involving computer as medium/target during the year 2014 and 2015, respectively.

Government has taken various steps in the form of legal framework, awareness, training, and implementation of best practices to address these issues. The steps include:

(i). The Information Technology (IT) Act, 2000 provides a comprehensive legal framework to address the issues connected with cyber crime, cyber attacks and security breaches of information technology infrastructure.

(ii). In order to focus more attention on IT related matters, Reserve Bank of India has set up a Cyber Security and IT Examination (CSITE) Cell within its Department of Banking

Supervision in 2015. The Bank has issued a comprehensive circular on Cyber Security Framework in Banks on June 2, 2016 covering best practices pertaining to various aspects of cyber security. The circular requires banks to have among other things, a cyber-security policy, cyber crisis management plan, a gap assessment vis-à-vis the baseline requirements

indicated in the circular, monitoring certain risk indicators in the area, report unusual cyber security incidents within 2 to 6 hours, ensure board involvement in the matter and robust vendor risk management. The progress of banks in scaling up their cyber security preparedness is monitored.

(iii). RBI has been carrying out IT Examination of banks separately from the regular financial examination of banks. This report has a special focus on cyber security. The reports have been issued to the banks for remedial action. RBI has also set up Cyber Crisis Management Group to address any major incidents reported including suggesting ways to respond to and recover from the incidents. Department of Banking Supervision under RBI also conducts cyber security preparedness testing among banks on the basis of hypothetical scenarios with the help of The Indian Computer Emergency Response Team (CERT-In). RBI also has set up an IT subsidiary, which would focus, among other things, on cyber security within RBI as well as in regulated entities. The subsidiary is in the process of recruiting the experts.

(iv). CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and mobile phones on regular basis. Security tips have been published for users to secure their Desktops, mobile/smart phones and preventing phishing attacks. Advisories have also been issued regarding safeguards for users and institutions to secure digital payments.

(v). Ministry of Electronics & Information Technology (MeitY) 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.secureelectronics.in" and "www.cert-in.org.in".

(vi). Government has established Botnet Cleaning and Malware Analysis Centre to detect and clean infected systems in the country. The project is initiated in coordination with the Internet Service Providers and Industry.

(vii). Government has formulated a set of investigation manuals with procedures for Search, Seizure Analysis and Presentation of digital evidence in courts. The manuals have been circulated to Law Enforcement Agencies in all States.

(viii).Currently 24 security auditing organizations are empanelled to support and audit implementation of Information Security Best Practices.

(b): The IT Act, 2000 provides legal framework for data protection and privacy in the digital domain. Section 43, section 43A, section 72 and section 72A of the IT Act, 2000 provides for privacy and security of data in digital form. Further, the Government is in the process of drafting a legislation that will provide protection to individuals in case their privacy is breached through unlawful means, which is at consultation stage at present.

****