GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 1215
TO BE ANSWERED ON: 10.03.2017

SAFETY MEASURES FOR AVOIDING DATA THEFT

1215 SHRI MAHESH PODDAR

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

(a) whether along with promoting the usage of digital technology by the users Government is also promoting the safety measures of the digital technology to avoid data theft and its safety issues through cyber crime; and

(b) if so, the details thereof?

ANSWER

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

(a) and (b): Yes, Sir. 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. There are provisions in the Act for data theft and security of data in digital form. Further, Information Technology (Intermediary Guidelines) Rules, 2011 notified under Section 79 provides for grievance redressal mechanism.

ii. 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”.

iii. All authorised entities/banks issuing Prepaid Payment Instruments (PPIs) in the country have been advised by Indian Computer Emergency Response Team through the Reserve Bank of India to carry out audit by the empanelled auditors of Indian Computer Emergency Response Team (CERT-In) on a priority basis and take immediate steps thereafter to comply with the findings of the audit report and ensure implementation of security best practices.

iv. All organizations providing digital payment services have been mandated to report cyber security incidents to CERT-In expeditiously.

v. Government has formulated Cyber Crisis Management Plan for countering cyber attacks for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.

vi. Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. Till date, 11 such drills have been conducted by the Indian Computer Emergency Response Team (CERT-In) involving 110 organisations from different sectors including Finance sector. The last drill was conducted on 30th September 2016 in coordination with Reserve Bank of India for Finance Sector.

vii. The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and mobile phones on regular basis. 21 advisories have also been issued regarding safeguards for users and institutions to secure digital payments.

viii. Government has established Botnet Cleaning and Malware Analysis Centre. The centre is providing detection of malicious programs and free tools to remove the same for banks as well as common users.

ix. RBI issued a comprehensive circular on June 2, 2016 related to Cyber Security Framework in Banks. The circular covered covers best practices pertaining to various aspects of cyber security. Banks were advised to improve and maintain customer awareness and education with regard to cyber security risks.

x. In order to focus more attention on IT related matters, Reserve Bank has set up a Cyber Security and IT Examination (CSITE) Cell within its Department of Banking Supervision in 2015.

xi. RBI has also set up an IT Subsidiary, which would focus, among other things, on cyber security within RBI as well as in regulated entities.

xii. An inter-disciplinary Standing Committee on Cyber Security as indicated in the Statement on Developmental and Regulatory Policies issued along with the Sixth Bi-monthly Monetary Policy Statement, 2016-17 announced on February 8, 2017 has been constituted by RBI. The Committee would, inter alia, review the threats inherent in the existing/emerging technology and suggest appropriate policy interventions to strengthen cyber security and resilience.

****