GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
STARRED QUESTION NO. *249
TO BE ANSWERED ON: 04.01.2019

HACKING OF DATA

***249 SHRI RIPUN BORA:**

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

(a) whether hacking of data and illegal money transfers have grown in the last three years in the country;

(b) if so, the breach of data and money siphoned off from different banks through stolen data reported since 2014; and

(c) the initiatives taken by Government for ensuring high security system thereof?

ANSWER

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

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

STATEMENT REFERRED TO IN REPLY TO RAJYA SABHA STARRED QUESTION NO. *249 FOR 04-01-2019 REGARDING HACKING OF DATA

……

(a) and (b): As per information provided by Reserve Bank of India (RBI), a total of 1191, 1372, 2059 and 921 cases of frauds involving ATM/Debit Cards, Credit Cards and Internet Banking Frauds (amount involved Rs 1 lakh and above) were reported during the years 2015-16, 2016-17, 2017-18 and 2018-19 (Upto 30 Sept 2018) respectively. The amount involved for frauds of Rs 1 lakh and above during the years 2015-16, 2016-17, 2017-18 and 2018-19 (Upto 30 Sept 2018) are Rs.40.2 crore, Rs.42.29 crore, Rs.109.56 crore and Rs.40.34 crore respectively.

(c) : In tune with the dynamic nature of Information Technology and emerging cyber threats, continuous efforts are required to be made by owners and users to protect networks and data by way of deploying appropriate security controls.

Government has taken several measures to enhance the cyber security of digital payment systems. These, *inter alia*, include:

(i) The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis to ensure safe usage of digital technologies. Regarding securing digital payments, 28 advisories have been issued for users and institutions.

(ii) All authorised entities/banks issuing Prepaid Payment Instruments (PPIs) in the country have been advised by CERT-In through Reserve Bank of India to carry out special audit by empanelled auditors of CERT-In and to take steps to comply with the findings of the audit report and ensure implementation of security best practices.

(iii) Government has issued guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.

(iv) Government has empanelled 76 security auditing organisations to support and audit implementation of Information Security Best Practices.

(v) All organizations providing digital services have been mandated to report cyber security incidents to CERT-In expeditiously.

(vi) 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.

(vii) Cyber security mock drills and exercises are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 38 such exercises have so far been conducted by CERT-In where organisations from different sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS etc participated. 3 exercises were conducted in coordination with Reserve bank of India in November 2018 for senior management and Chief Information Security Officers (CISOs) of banks.

(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

trainings covering 746 participants have been conducted in the year 2018 (till November).

(ix) 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.

(x) 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 been made operational.

****