GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO.1443
TO BE ANSWERED ON: 04.07.2019

CYBER ATTACKS ON BANKING AND CASHLESS NETWORKS

1443. SHRI PARIMAL NATHWANI:

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

(a) the number of cases of cyber attacks on banking and other cashless networks that have been reported during the last three years;
(b) the steps Government has taken to curb cyber-crimes, hacking of bank transactions of credit cards and to organise campaigns for building and regaining confidence of citizens;
(c) whether Government has proposed sufficient/additional budgetary provisions to provide technological support to curb cyber crimes; and
(d) if so, the details thereof?

ANSWER

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

(a): As per information reported to the Indian Computer Emergency Response Team (CERT-In), 14, 6 and 2 financial fraud incidents affecting ATMs, Cards, Point-of-sale (PoS) systems and Unified Payment Interface (UPI) have been reported during the year 2017, 2018 and 2019 (upto May) respectively.

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

(a) Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country, as per the provisions of section 70A of the Information Technology (IT) Act, 2000.
(i) 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 on a priority basis and to take immediate steps thereafter to comply with the findings of the audit report and ensure implementation of security best practices.
(ii) The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis. CERT-In has published guidelines for securing IT infrastructure, which are available on its website (www.cert-in.org.in).
(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 84 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 Cyber 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.

(viii) 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. 43 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 sectors participated.

(ix) 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. 24 trainings covering 845 participants conducted in the year 2018.

(x) 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.

(xi) 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.

(i) Ministry of Home Affairs (MHA) has constituted an Inter-Ministerial Committee on Phone Fraud (IMCPF) having members of all stakeholder organisations, namely, Ministry of Electronics & Information Technology (MeitY), Department of Financial Services, Department of Telecommunications, Reserve Bank of India and law enforcement agencies, to address the problem. FCORD - (FICN Coordination Agency) has been designated as Central Nodal Agency for this purpose.

(ii) MHA has issued an advisory dated 12.02.2018 on "Steps to check Phone Frauds". It has also issued an advisory on 13.01.2018 on "Cyber Crime Prevention and Control".

(c) and (d): Cyber security is a continuous process and Government allocates necessary budget to address this. MeitY had a budget of Rs. 70 crores, Rs. 100 crore and Rs. 110 crore during the years 2016-17, 2017-18 and 2018-19 respectively for cyber security. Also MeitY has directed all Central Government Ministries/Departments, State Government/UTs and Critical Sectors to earmark 10% of their annual IT budget to implement cyber security.

Further, MHA is implementing Indian cyber Crime Coordination Centre (14C) Scheme at an estimated cost of Rs. 415.86 crore which aims at providing a platform to deal with all types of cybercrime in a coordinated and comprehensive manner.

******