GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
STARRED QUESTION NO *197
TO BE ANSWERED ON: 05.01.2018

DEALING WITH CYBER CRIMES

***197. DR. T. SUBBARAMI REDDY:**

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

(a) whether there are growing incidents of cyber crimes, including financial frauds, using bank cards and e-wallets;

(b) if so, the response of Government thereto;

(c) the measures taken to strengthen surveillance and legal framework to deal with cyber crimes; and

(d) whether police force has been adequately trained to deal with cyber crimes, if so, the details thereof?

ANSWER

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

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

STATEMENT REFERRED TO IN REPLY TO RAJYA SABHA STARRED QUESTION NO.*197 FOR 05.01.2018 REGARDING DEALING WITH CYBER CRIMES

……..

(a): As per the data maintained by National Crime Records Bureau (NCRB), a total of 9622, 11592 and 12,317 cyber crime cases were registered during the years 2014, 2015 and 2016 respectively. This includes cases registered under the Information Technology (IT) Act, 2000 and related sections of Indian Penal Code and Special & Local Laws involving computer as medium/ target. As per incidents reported to the Indian Computer Emergency Response Team (CERT-In), 79 phishing incidents affecting 22 financial organisations and 13 incidents affecting ATMs, Point of Sales (POS) systems and Unified Payment Interface (UPI) have been reported during November 2016 to November 2017. Further, Reserve Bank of India (RBI) has registered a total of 13083, 16468, 13653 and 12520 cases of frauds involving credit cards, ATM / debit cards and internet banking during the year 2014-15, 2015-16, 2016-17 and quarter April-September 2017 respectively.

(b) and (c): Government has taken a number of legal, technical and administrative measures to prevent incidents of cyber crimes, including financial frauds, using bank cards and e-wallets. These *inter alia,* include:

(i) Enactment of the Information Technology (IT) Act, 2000 which has adequate provisions for dealing with prevalent cyber crimes.
(ii) Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) as per the provisions of Section 70A of the Information Technology (IT) Act, 2000 for protection of critical information infrastructure in the country.
(iii)The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis. CERT-In has issued 27 advisories since Nov 27, 2016 for security safeguards covering Point of Sale (POS), Micro ATMs, electronic Wallets, online banking, smart phones, unified payment interface, Unstructured Supplementary Service Data (USSD), RuPay, SIM cards, wireless access points / routers, mobile banking, cloud and Aadhaar Enabled Payment System (AEPS). Advisory has also been sent by CERT-In to RBI, National Payment Corporation of India (NPCI) and Payment Card Industry Organizations covering precautions to be taken to avoid similar attacks as those that occurred recently with credit / debit cards. CERT-In has published guidelines for securing IT infrastructure, which are available on its website (www.certin.org.in).
(iv) Government has initiated setting up of National Cyber Coordination Centre (NCCC) in CERT-In 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.
(v) 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 for banks as well as common users.

(vi)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. Regular workshops are conducted for Ministries, Departments, States & Union Territories and critical organizations to sensitize them about the cyber security threat landscape and enabling them to prepare and implement the Cyber Crisis Management Plan.

(vii)Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 15 such drills have so far been conducted by CERT-In where 148 organisations from different states and sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS, etc have participated.

(viii) Law and Order being a State subject, the implementation is with the State Government.

(ix) Ministry of Home Affairs has issued National Information Security Policy and Guidelines (NISPG) to Government organizations to ensure safety of data and minimize cyber threats.

(x) With respect to the banking sector, RBI reviews the cyber security developments and threats on an ongoing basis and necessary measures are taken to strengthen the cyber resilience of banks. In order to focus more attention on IT related matters, Reserve Bank of India (RBI) has taken various action which includes:

a. RBI has set up a Cyber Security and IT Examination (CSITE) cell within its Department of Banking Supervision in 2015.
b. 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.
c. RBI carries out IT Examination of banks separately from the regular financial examination of banks from last year. This report has a special focus on cyber security. The reports have been issued to the banks for remedial action.
d. RBI has also set up Cyber Crisis Management Group to address any major incidents reported including suggesting ways to respond and recover to/ from the incidents.
e. Department of Banking Supervision under RBI also conducts cyber security preparedness testing among banks on the basis of hypothetical scenarios with the help of CERT-In.
f. An inter-disciplinary Standing Committee on Cyber Security has been constituted which, inter alia, reviews the threats inherent in the existing/emerging technology and suggests appropriate policy interventions to strengthen cyber security and resilience.
g. RBI has set up an IT Subsidiary, which, inter alia focuses on cyber security within RBI as well as in regulated entities.
h. On October 11, 2017 Master Directions on Issuance and Operation of Prepaid Payment Instruments were issued by RBI.
i. RBI has issued circular on 09th December 2016 in Security and Risk mitigation measure for all authorised entities / banks issuing Prepaid Payment Instrument (PPI) in the country.

j. In addition, RBI issues Circulars/advisories to all Commercial Banks on phishing attacks and preventive / detective measures to tackle phishing attacks.

k. To Secure Card Present Transactions (both at ATM and POS delivery channels), RBI has taken a number of measures including migration of debit/credit card from magnetic strip to EMV chips and PIN based cards.

l. RBI has mandated additional factor of authentication for all card not present (CNP) transactions.

(d) : Government has taken a series of steps to train and develop Cyber Crime investigators. The steps include:

i) Ministry of Home Affairs has issued an Advisory to the State Governments and Union Territory Administrations to build adequate technical capacity in handling cyber crime including trained manpower for detection, registration, investigation and prosecution of cyber crimes. Also, under the Cyber Crime Investigation programme, Ministry of Home Affairs is supporting the establishment of Cyber Crime Police Stations (CCPS) and Cyber Crime Investigations and Forensic Training Facilities (CCIFTF) in each State / Union Territory of India under Police Modernization Scheme. Action also has been taken to set up a National Centre of Excellence exclusively devoted to render Cyber Forensic services and to act as National Research and Training Centre on Cyber Forensics.

ii) Ministry of Home Affairs is implementing the 'Cyber Crime Prevention against Women and Children (CCPWC)' scheme from NIRBHAYA funds of the Ministry of Women & Child Development in the period 2017-2020, which inter alia, aims at setting up an online cyber-crime reporting platform, cyber forensic training cum laboratories in States/UTs, R&D facilities and capacity building in law enforcement against cyber-crime. The main objective of the scheme is to facilitate handling of issues related to cyber-crime against women and children.

iii) A major programme has been undertaken on development of cyber forensics tools, setting up of infrastructure for investigation and training of the users, particularly police and judicial officers in use of this tool to collect and analyze the digital evidence and present them in Courts.

iv) Indian Computer Emergency Response Team (CERT-In) and Centre for Development of Advanced Computing (CDAC) are involved in providing basic and advanced training to Law Enforcement Agencies, Forensic labs and judiciary on the procedures and methodology of collecting, analyzing and presenting digital evidence.

v) MeitY has setup Cyber Forensics Training Lab at CBI Academy Ghaziabad. Also In collaboration with Data Security Council of India (DSCI), Cyber Forensic Labs have been set up at Mumbai, Bengaluru, Pune and Kolkata for awareness creation and training programmes on Cyber Crime investigation. National Law School, Bangalore and NALSAR University of Law, Hyderabad are also engaged in conducting several awareness and training programmes on Cyber Laws and Cyber crimes for judicial officers. Mumbai, Pune, Bangalore and Kolkata and in north-eastern States at respective Police headquarters to train LEA officials (Police) in cyber crime detection, seizing and imaging of digital evidence. Using these facilities, more than 28000 Police /LEA personnel have been trained.

vi) 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.

vii) Government organised Cyber Crime Awareness workshops in 17 cities (Ahmadabad, Chandigarh, Bhopal, Lucknow, Jaipur, Patna, Shimla, Shillong, Dehradun, Thrissur, Bhubaneswar, Ranchi, Nagpur, Srinagar, Raipur, Goa and Mangalore.

****