GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 1948
TO BE ANSWERED ON 03.07.2019

CYBER CRIMES

1948 SHRI B.B. PATIL:
DR. NISHIKANT DUBEY:

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

(a) whether incidents of cyber crimes involving internet banking, banks cards and e-wallets are increasing day by day;
(b) if so, the details thereof and the action taken by the Government to strengthen the security and legal framework to deal with such cyber crimes;
(c) whether crores of rupees are misappropriated/siphoned off every year in the country through cyber crime, if so, the details thereof including the number of such cyber crimes reported during each of the last three years, state/UT-wise ;
(d) whether the police and other security agencies are well equipped and trained to deal with such cyber crimes; and
(e) if so, the details thereof and if not, the reasons therefor along with the action taken by the Government in this regard?

ANSWER

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

(a) and(c): Data on frauds committed in ATM/Debit Card/ Credit Card/Internet Banking category is provided in Annexure -I. The data of frauds (more than one lakh) in this category is provided in Table 1 based on the date of report. Data on such frauds for amounts involved less than Rs.1 lakh was started only in 2017 and therefore the same is shown in table 2 for only the last two years. The specific state/UT-wise data is not available.

(b): The steps taken by Government to create awareness as well as further strengthen the security system and legal framework have been mentioned in Annexure II. In addition, the steps taken by Reserve Bank of India (RBI) in respect of digital payments security have been mentioned in Annexure III.

(d) and (e): This Ministry, in collaboration with Data Security Council of India (DSCI), has set up Cyber Forensic Labs 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 cyberlaws and cyber crimes for judicial officers. Using these facilities, Police /LEA personnel have been trained for cyber crime detection.

In addition to this, National Crime Record Bureau (NCRB) has been organising training for Indian Police Officers and Foreign Police Officers to deal with the cyber crimes.

******

ANNEXURE - I

Table – 1

Year-wise data on frauds reported under "ATM/Debit Card/Credit Card/Internet Banking" by Scheduled Commercial Banks and selected FIs based on Date of Reporting for last 3 years (amount Involved Rs 1 lakh and above)		
Year	No. of Frauds	Amount Involved (Rs. In crores
2016-17	1372	42.29
2017-18	2059	109.56
2018-19	1866	71.38
Grand Total	**5297**	**223.23**

Table – 2

Year-wise data on frauds reported under "ATM/Debit Card/Credit Card/Internet Banking" by Scheduled Commercial Banks and selected FIs based on Date of Reporting for last 2 years (amount Involved below Rs 1 lakh)		
Year	No. of Frauds	Amount Involved (Rs. In crores
2017-18	32732	59.43
2018-19	50438	78.04
Grand Total	**83170**	**137.47**

1) It may be noted that fraud cases below Rs. 1 lakh were not reported to RBI prior to April 1, 2017. The data may change subject to rectification/updation made subsequent to first reporting by banks.
1) Data furnished in two separate sets, i.e. based on Date of Reporting and Date of Occurrence as reported by banks, to capture better picture of incidence of frauds
3) Frauds reported in a year could have occurred several years prior to year of reporting.

Source: RBI

Annexure II

Initiatives by the Government of India

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 hardening and deploying appropriate security controls.

1. 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.
2. All authorised entities/ banks issuing 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.
1. Government has issued guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.
2. Government has empanelled security auditing organizations to support and audit implementation of Information Security Best Practices.
3. All organizations providing digital services have been mandated to report cyber security incidents to CERT-In expeditiously.
4. 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.
5. 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 such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeSetc participated.

6. 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.

7. 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.
8. Government has initiated setting up of 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.
9. Under the Information Security Education and Awareness (ISEA) Project, candidates are trained in various formal/non-formal courses in Information Security.

Annexure-III

Steps taken by RBI

Department of Payment and Settlement Systems (DPSS), Reserve Bank of India (RBI) has issued circulars/ guidelines related to security and risk mitigation measures for securing digital / online payment transactions.

1. Securing Card Transactions

Various measures have been taken by RBI to secure card transactions and issued advisories: -

i) Banks have been advised to provide online alerts for all card transactions {Card Present (CP) and Card Not Present (CNP)}, vide, RBI circular dated March 29, 2011.

ii) RBI has also issued circulars dated September 22, 2011, February 28, 2013 and June 24, 2013 for securing electronic (online and e-banking) transactions advising banks to introduce additional security measures, as follows:
   a) All new debit and credit cards to be issued only for domestic usage unless international use is specifically sought by the customers. Such cards enabling international usage will have to essentially be EMV Chip and PIN enabled.
   b) Issuing banks should convert all existing MagStripe cards to EMV Chip card for all customers who have used their card internationally atleast once (for/ through e–commerce/ATM/POS).
   c) Banks should ensure that the terminals installed at the merchants for capturing card payments (including the double swipe terminals used) should be certified for PCI-DSS (Payment Card Industry-Data Security Standards) and PA-DSS (Payment Applications-Data Security Standards).
   d) Banks should ensure that all acquiring infrastructure that is currently operational on IP (Internet Protocol) based solutions are mandatorily made to go through PCI-DSS and PA-DSS certification. This should include acquirers, processors / aggregators and large merchants.

i) RBI has directed banks to mandatorily put in place an Additional Factor of Authentication (AFA) for all CNP transactions w.e.f. 01.05.2013 failing which the issuer bank shall reimburse the loss to customer without demur.

ii) All authorised card payment networks are permitted to offer card tokenisation services to any token requestor (i.e., third party app provider), subject to certain conditions. All extant instructions of RBI on safety and security of card transactions, Including the mandate for Additional Factor of Authentication (AFA) / PIN entry shall be applicable for tokenised card transactions also (DPSS.CO.PD No.1463/02.14.003/2018-19) dated January 08, 2019).

iii) The systems and procedures in banks must be designed to make customers feel safe about carrying out electronic banking transactions.
   a) **Securing Payments through Internet Banking / Electronic Payments**
   RBI has issued circular on 'Security and Risk Mitigation Measures for Electronic Payment Transactions' (DPSS.CO.PD No.1462 /02.14.003 /2012-13) dated February 28, 2013. Vide this circular, RBI has required banks to introduce following additional measures to secure electronic mode of payments like RTGS, NEFT and IMPS.
   b) **Prepaid Payment Instruments (PPIs):**
   RBI has issued 'Master Direction on Issuance and Operation of PPIs' (MD on PPIs) (DPSS.CO. PD. No.1164/02.14.006/2017-18) dated October 11, 2017 (updated as on December 29, 2017).
   c) **Limiting Customer Liability on Unauthorized Electronic Banking Transactions**
   RBI has issued circular no. DBR.No. Leg.BC.78/09.07.005/2017-18 dated July 06, 2017 limiting the liability of customers on unauthorized electronic banking transactions.

d) **Limiting Customer Liability in Unauthorized Electronic Banking Transactions in PPIs issued by Authorised Non-banks**

RBI has issued circular no. DPSS.CO.PD.No.1417/02.14.006/2018-19 dated January 04, 2019 limiting the liability of customers in unauthorized electronic banking transactions in PPIs issued by Authorised Non-banks.