GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 690
TO BE ANSWERED ON 08.02.2019

STRENGTHENING OF INTERNET SECURITY

690 SHRI HISHEY LACHUNGPA:

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

(a) the details of the number of cases of people being forged in regard to fraudulent usage of the debit/credit cards by pilferage of their passwords, etc., in last five years;

(b) whether any steps are being taken by Government to create awareness as well as further strengthen the security system to ensure maximum internet security to the people;

(c) if so, the details thereof; and

(d) if not, the reasons therefor?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI S. S. AHLUWALIA)

(a): This ministry does not have specific information about the above mentioned question. However, as per the details shared by Reserve Bank of India (RBI), data on 'ATM/Debit Card' and 'Credit Card' frauds reported by scheduled commercial banks and select financial institutions during the last three years and the current year (till September 30, 2018), is given in Annexure-I.

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

Annexure –I

Number of ATM/Debit Cards, Credit Cards Frauds reported by Schedule Commercial Banks and Select FIs during the last 3 years and the current year (Amount involved Rs. 1 lakh and above)

Area of Operation	2015-16	2016-17	2017-18	2018-19 (Upto 30 Sept 2018)
ATM/Debit Cards	563	724	911	507
Credit Cards	616	609	1102	357
Grand Total	1179	1333	2013	864

It may please be noted that as per rectification/updation made subsequent to first reporting by banks, the data may change.

Annexure –II

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. Regarding securing digital payments, 28 advisories have been issued for users and institutions.
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.
3. Government has issued guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.
4. Government has empanelled 76 security auditing organisations to support and audit implementation of Information Security Best Practices.
5. All organizations providing digital services have been mandated to report cyber security incidents to CERT-In expeditiously.
6. 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.
7. 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. 38such 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.
8. 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 conducted in the year 2018 (till November).
9. 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.
10. 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.
11. Information Security Education and Awareness (ISEA) Project Phase II was approved in the year 2014 with an objective of capacity building in the area of Information Security, training of Government personnel and creation of mass Information Security awareness targeted towards various user segments. The project aims to train more than 1 lakh candidates in various formal/non-formal courses and more than 13,000 Government officials by March 2020. In addition, the project envisages creation of mass awareness on Information Security through direct and indirect mode. So far, 39,495 candidates have been trained/under-going training in various formal/non-formal courses through 52 institutions; 6,035 Government officials have been trained in various short term courses of 2/3/5 days duration and 749 Government officials have been trained through e-learning courses in the area of Information Security. Besides this, 770 half day general awareness workshops on Information Security have been organized across the country for various user groups covering 84,671 participants. Information Security Awareness handbooks were distributed as a part of these workshops to disseminate information and tips on safe use of internet. Awareness material in the form of videos, posters, brochures, newsletter, etc. are also made available for download on the website www.isea.gov.in.

Annexure-III

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: -

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.

iii) 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.
iv) 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).

2. **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:

i) Customer induced options may be provided for fixing a cap on the value/mode of transactions /beneficiaries. In the event of customer wanting to exceed the cap, an additional authorization may be insisted upon.
ii) Limit on the number of beneficiaries that may be added in a day per account could be considered.
iii) A system of alert may be introduced when a beneficiary is added.
iv) Banks may put in place mechanism for velocity check on the number of transactions effected per day / per beneficiary and any suspicious operations should be subjected to alert within the bank and to the customer.

v) Introduction of AFA (preferably dynamic in nature) for payment transactions should be considered.
vi) The banks may consider implementation of digital signature for large value payments for all customers, to start with for RTGS transactions.
vii) Capturing of Internet Protocol (IP) address as an additional validation check should be considered.
viii) Sub-membership of banks to the centralized payment systems has made it possible for the customers of such sub-members to reap the benefits of the same. Banks accepting sub-members should ensure that the security measures put in place by the sub members are on par with the standards followed by them so as to ensure the safety and mitigate the reputation risk.
ix) Banks may explore the feasibility of implementing new technologies like adaptive authentication, etc. for fraud detection.

3. **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).

As per para 15.3 of MD on PPI issuers were instructed to put in place a framework to address the safety and security concerns, and for risk mitigation and fraud prevention as follows:

i) In case of wallets, PPI issuers shall ensure that if same login is provided for the PPI and other services offered by the PPI Issuer, then the same shall be clearly informed to the customer by SMS or email or post or by any other means. The option to logout from the website / mobile account shall be provided prominently.
ii) Issuers shall put in place appropriate mechanisms to restrict multiple invalid attempts to login / access to the PPI, inactivity, timeout features, etc.
iii) Issuers shall introduce a system where every successive payment transactions in wallet is authenticated by explicit customer consent.
iv) Cards (physical or virtual) shall necessarily have AFA as required for debit cards, except in case of PPIs issued under PPI-MTS.
v) Issuers shall provide customer induced options for fixing a cap on number of transactions and transaction value for different types of transactions / beneficiaries. Customers shall be allowed to change the caps, with additional authentication and validation.
vi) Issuers shall put in place a limit on the number of beneficiaries that may be added in a day per PPI.
vii) Issuers shall introduce a system of alert when a beneficiary is added.
viii) PPI issuers shall put in place suitable cooling period for funds transfer upon opening the PPI or loading / reloading of funds into the PPI or after adding a beneficiary so as to mitigate the fraudulent use of PPIs.
ix) Issuers shall put in place a mechanism to send alerts when transactions are done using the PPIs. In addition to the debit or credit amount intimation, the alert shall also indicate the balance available / remaining in the PPI after completion of the said transaction.
x) Issuers shall put in place mechanism for velocity check on the number of transactions effected in a PPI per day / per beneficiary.
xi) Issuers shall also put in place suitable mechanism to prevent, detect and restrict occurrence of fraudulent transactions including loading / reloading funds into the PPI.
xii) Issuers shall put in place suitable internal and external escalation mechanisms in case of suspicious operations, besides alerting the customer in case of such transactions.

4. **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. The transactions include–

i) Remote / Online payment transactions (transactions that do not require physical payment instruments to be presented at the point of transactions e.g. internet banking, mobile banking, CNP transactions, PPIs,
ii) Face-to-face / Proximity payment transactions (transactions which require the physical payment instrument such as a card or mobile phone to be present at the point of transaction e.g. ATM, POS, etc.)

The systems and procedures in banks must be designed to make customers feel safe about carrying out electronic banking transactions. To achieve this, banks must put in place:

i) appropriate systems and procedures to ensure safety and security of electronic banking transactions carried out by customers;

ii) robust and dynamic fraud detection and prevention mechanism;
iii) mechanism to assess the risks (for example, gaps in the bank's existing systems) resulting from unauthorized transactions and measure the liabilities arising out of such events;
iv) appropriate measure to mitigate the risks and protect themselves against the liabilities arising therefrom; and
v) a system of continually and repeatedly advising customers on how to protect themselves from electronic banking and payments related fraud.

5. **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. To achieve this, PPI issuers are directed to:

a. Ensure that their customers mandatorily register for SMS and email alerts.
b. Send alert for any payment transaction in the account to the customers. Transaction alert should have a contact number and / or e-mail id on which a customer can report unauthorised transactions or notify the objection.
c. Provide customers with 24x7 access via website / SMS / e-mail / a dedicated toll-free helpline for reporting unauthorised transactions that have taken place and / or loss or theft of the PPI.
d. Provide a direct link for lodging of complaints, with specific option to report unauthorised electronic payment transactionson mobile app / home page of their website / any other evolving acceptance mode.
e. Ensure that a complaint is resolved and liability of the customer, if any, established within such time, as may be specified in the PPI issuer's Board approved policy, but not exceeding 90 days from the date of receipt of the complaint.

6. For the purpose of creating awareness RBI is holding e-BAAT program at various locations wherein audience are sensitised about safe digital payments. Also, a campaign named "RBI Kehta Hai" is undertaken through print and electronic media to create awareness in this regard.

****