GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO 2507
TO BE ANSWERED ON 16.03.2018

SECURITY AND SAFETY IN DIGITAL TRANSACTIONS

2507 DR. R. LAKSHMANAN:

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

(a) whether any complaints regarding breach of security and safety while doing digital transactions have been brought to the notice of Government;
(b) if so, the details thereof;
(c) the details of the steps taken by Government to enhance the safety and security while doing digital transactions; and
(d) the details of the steps taken by Government to create awareness among the bank customers in this regard?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI K.J. ALPHONS)

(a) and (b): In terms of RBI Circular no. DBS.CO/CSITE/BC.11/33.01.001/2015-16 dated June 2, 2016 on “Cyber Security Framework in Banks” (available at https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT41893F697BC1D57443BB76AFC7AB56272EB.PDF), banks have been advised, inter-alia to report all unusual cyber security incidents to RBI within 2 - 6 hours of detection.

Though not all such unusual incidents reported would be involving a breach of security, as per information received from RBI, incidents of phishing/vishing, OTP compromise, fraud by compromise of user credentials, compromise of mobile phone numbers of customers (only for the period from April 2017 to December 2017) as reported by banks is given below :

S.No.	Cyber Attacks	Quarter ending June –2017 (in nos.)	Quarter ending Sept – 2017 (in nos.)	Quarter ending Dec – 2017 (in nos.)
1	Vishing Attack	8995	11482	19873
2	Phishing Attack	5524	5938	6207
3	Credentials OTP compromises	859	1416	1977
4	Frauds by compromise of user credentials	597	1771	1002
5	Compromise of mobile nos. of customers	153	146	1163
Total Cyber Attacks		16128	20753	30222

In addition, RBI also received 2 complaints regarding ATM cloning and E wallet scam involving bank accounts in bank branches of public and private sector banks. Details of the complaints are given below:

1. Complaint regarding ATM / Debit Card cloning: A complaint was received in January 2017 wherein it was alleged that banks were involved in cloning of ATM /Debit cards. The complainant urged RBI to take action against errant banks. The complaint was taken up with SBI and Yes Bank.

2. E wallet scam involving 1020 bank accounts in 351 bank branches of public and private sector banks (13 banks): In the complaint received in November 2017, it was alleged that about 1020 bank accounts in different banks were used by the fraudsters to receive the money from victim's bank accounts by way of phishing.

(c) and (d): Reserve Bank of India (RBI) issues the regulations related to cyber security guidelines and periodically reviews the cyber security developments and threats on an ongoing basis and necessary measures are taken to strengthen the cyber resilience of banks. Reserve Bank of India (RBI) is taking adequate measures for **Risk Mitigation for Online Payments**.

Some of the measures taken by RBI are as follows-

1. A comprehensive circular on Cyber Security Framework in Banks issued on June 2, 2016 (DBS.CO/CSITE/BC.11/33.01.001/2015-16) covers best practices pertaining to various aspects of cyber security

2. RBI has also set up a Cyber Crisis Management Group to address any major incidents reported including suggesting ways to respond. Based on market intelligence and incidents reported by the banks, advisories are issued to the banks for sensitizing them about various threats and ensure prompt preventive/corrective action.

3. Department of Banking Supervision under RBI, with the help of Indian – Computer Emergency Response Team (CERT-In), conducts cyber security preparedness testing among banks on the basis of hypothetical scenarios.

4. RBI issues Circulars/advisories to all Commercial Banks on phishing attacks and preventive / detective measures to tackle phishing attacks. Banks have also been following the same with their users.

5. RBI has set up a Cyber Security and IT Examination (CSITE) cell in 2015
And carries out Information Technology (IT) Examination of banks separately from the regular financial examination of the banks to assess their cyber resilience. The examination, inter-alia, evaluates the processes implemented by banks for security checks like Vulnerability Assessment (VA) / Penetration Testing (PT) etc. and their follow up action.

6. An inter-disciplinary Standing Committee on Cyber Security at RBI, reviews the threats inherent in the existing/emerging technology and suggests appropriate policy interventions to strengthen cyber security and resilience.

7. RBI has set up an Information Technology (IT) Subsidiary, which would focus, among other things, on cyber security within RBI as well as in regulated entities.

8. Banks and Payment System Operators have been advised to enhance the security and risk mitigation measures for (a) card transactions (includes card based online transactions) and (b) electronic payment transactions (includes e-banking transactions) by taking following measures-

a) Banks have been advised to provide **online alerts** for all card transactions (card present and card not present), vide, RBI circular dated February 18, 2009 (RBI / DPSS No. 1501 / 02.14.003 / 2008-2009) and March 29, 2011 (DPSS. CO. PD 2224 /02.14.003/2010-2011).

b) Banks have been advised, vide, circular February 18, 2009 (RBI / DPSS No. 1501 / 02.14.003 / 2008-2009) and December 31, 2010 (DPSS.CO.No.1503/02.14.003/2010-2011) to put in place a system of providing **additional factor of authentication** (2FA) for all card not present transactions using the information which is not available on the card.

c) Banks have also been advised vide circulars dated February 28, 2013 (DPSS (CO) PD No.1462 / 02.14.003 / 2012-13) and June 24, 2013 (DPSS (CO) PD No.2377 / 02.14.003 / 2012-13) for securing electronic (online and e-banking) transactions, to introduce **additional security measures**.

9. For Non-Bank Entities operating Payment Systems in India, in order to ensure that the technology deployed to operate the payment system/s authorised is/are being operated in a safe, secure, sound and efficient manner, RBI has, vide circulars DPSS.AD.No.1206 / 02.27.005 / 2009-2010 dated December 7, 2009 and DPSS.1444/ 06.11.001/ 2010-2011 dated December 27, 2010, which was subsequently amended vide circular DPSS.CO.OSD.No.2374 / 06.11.001 / 2010-2011 dated April 15, 2011 (copy is available on https: // www .rbi. org. in/ scripts/ FS_Notification .aspx?Id =6344&fn=9&Mode=0), mandated System Audit to be done on an annual basis by Certified Information Systems Auditor (CISA), registered with Information Systems Audit and Control Association (ISACA) or by a holder of a Diploma in Information System Audit (DISA) qualification of the Institute of Chartered Accountants of India (ICAI).

10. With a view to address the issue of cyber resilience, RBI had, vide circular DPSS.CO.OSD.No.1485/06.08.005/2016-17 dated December 9, 2016 (copy is available on https :// www. rbi.org.in / scripts / FS_Notification.aspx ?Id =10772&fn =9&Mode=0), instructed all authorised entities/ banks issuing PPIs in the country to carry out special audit by empanelled CERT-In auditors and take appropriate measures on mitigating phishing attacks.
In addition, details of direction pertaining to security for PPI transactions, are available in section ‘Security, Fraud prevention and Risk Management Framework’ of the Master Directions for PPI issued by RBI (DPSS.CO.PD.No.1164/02.14.006/2017-18) .

11. Limited Liability of Customers: Guidelines on Limited liability of customers in Unauthorized Electronic Banking Transactions (RBI Circular Number DBR.No.Leg.BC.78/09.07.005/2017-18 dated 06.07.2016) are available at the RBI website link:
https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NOTI15D620D2C4D2CA4A33AABC928CA6204B19.PDF

12. RBI has issued various circulars wherein customer banks are advised to educate customers. These circulars are as follows:

a) Card Payments – Relaxation in requirement of Additional Factor of Authentication for small value card present transactions dated May 14, 2015 (DPSS.CO.PD.No.2163/02.14.003/2014-2015).
b) Cash Withdrawal at Point-of-Sale (POS) - Enhanced limit at Tier III to VI Centres dated August 27, 2015 (DPSS.CO.PD.No.449/02.14.003/2015-16).
c) Card Not Present transactions –Relaxation in Additional Factor of Authentication for payments upto 2000/- for card network provided authentication solutions dated December 6, 2016 (DPSS.CO.PDNo.1431/02.14.003/2016-17).
d) Master Direction on Issuance and Operation of Prepaid Payment Instruments dated October 11, 2017 (DPSS.CO.PD.No.1164/02.14.006/2017-18).
e) Banks have also been requested to educate customers about cyber security risks, as per the circular on Cyber Security Framework in Banks dated June 2, 2016 (DBS.CO/CSITE/BC.11/33.01.001/2015-16).

In addition, steps taken by Government to secure digital payment system are as under:

1. 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.
2. CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities along with countermeasures to create awareness among stakeholders to take appropriate measures to ensure safe usage of digital technologies. Regarding securing digital payments, 27 advisories have been issued for users and institutions.
3. CERT-In has empanelled 67 security auditing organizations to support and audit implementation of Information Security Best Practices.
4. All organizations providing digital payment services have been mandated to report cyber security incidents to CERT-In expeditiously.
5. Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 25 such exercises have so far been conducted by CERT-In where organisations from different States and sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS, etc. participated.
6. Cyber security awareness sessions are conducted by Ministry of Electronics and Information technology (MeitY) under the Digishala Awareness Campaign.
7. Government has established Botnet Cleaning and Malware Analysis Centre to detect and clean infected systems in the country. The project is initiated in coordination with the Internet Service Providers and Industry.
8. MeitY has organised 2 workshops for banks, Internet Service Providers (ISPs) and Prepaid Payment Instruments (PPIs) issuing entities regarding security of digital payments systems.
9. Government has issued general guidelines for Chief Information Security Officers (CISOs) for securing applications and infrastructure and their key roles and responsibilities for compliance; and is regularly conducting cyber security trainings for CISOs of Government and critical sector organisations, in addition to Information Technology (IT) / cyber security professionals, to give an exposure on current threat landscape and countermeasures.

****