GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 4408
TO BE ANSWERED ON: 29.03.2017

SECURITY OF TRANSACTIONS

4408 SHRI NANA PATOLE:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:
(a) whether using of mobile wallet and mobile banking applications is not safe as the features of the hardware installed in mobile is not of requisite quality;
(b) if so, the details and the reasons therefor;
(c) whether online transaction is not so safe on account of the reason cited above; and
(d) if so, the steps taken or being taken by the Government to make online transaction more secured?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI P. P. CHAUDHARY)

(a), (b) and (c): Mobile wallet, mobile banking and online transactions are as safe as any other financial transaction.

(d): Government has taken several steps to ensure the safety and security of mobile wallet, mobile banking, online and other digital transactions. Some major steps being taken by the Government are given below:

(i) Indian Computer Emergency Response Team (CERT-In) conducts regular training programmes to make the network and system administrators aware about securing the IT infrastructure and mitigating cyber attacks. 18 such training programs were conducted covering 580 participants during the year 2016.

(ii) Reserve Bank of India (RBI) has mandated Non-Bank Entities operating Payment Systems in India to undertake System Audit on an annual basis by CISA/DISA certified auditor, vide their circular dated December 7, 2009 and amended on April 15, 2011. The scope of the annual audits includes evaluation of the hardware infrastructure, operating systems and critical applications, security and controls in place, including access controls on key applications, disaster recovery plans, training of personnel managing systems and applications, documentation, etc.

(iii) RBI has issued circular dated December 9, 2016 instructing all authorized entities / banks issuing PPIs in the country to:

- Carry out a special audit by the empanelled auditors of Indian Computer Emergency Response Team (CERT-In) on a priority basis and take immediate steps thereafter to comply with the findings of the audit report. The audit should cover compliance as per security best practices, specifically the application security lifecycle and patch/vulnerability and change management aspects for

the system authorized and adherence to the process flow approved by the Reserve Bank.

- Take appropriate measures on mitigating phishing attacks considering that the new customers are likely to be first time users of the digital channels. Safety and security best practices may be disseminated to the customers periodically.

- Implement additional measures dynamically depending upon the risk perception or threats as they emerge.

(iv) Department of Payment and Settlement Systems (DPSS), RBI has issued a Master Circular on Mobile Banking Transactions in India – Operative Guidelines for Banks on July 01, 2016 asking them to ensure that the technology used for mobile banking must be secure and should ensure confidentiality, integrity, authenticity and non-repudiability.

(v) RBI has given approval to NPCI to go-live for UPI on August 24, 2016. This process of approval involved, among others, scrutiny of the relevant system audit report submitted by NPCI.

(vi) DPSS, RBI has also issued circulars dated February 28, 2013 for securing electronic (online and e-banking) transactions advising banks to introduce inter-alia, additional security measures, as under:

- 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.
- Limit on the number of beneficiaries that may be added in a day per account could be considered.
- A system of alert may be introduced when a beneficiary is added.
- 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.
- Introduction of additional factor of authentication (preferably dynamic in nature) for such payment transactions should be considered.

(vii) All UPI based apps are using mobile device identifier and app binding feature to provide security control. For card authentication, Hardware Security Module (HSM) is used by all banks using RuPay cards. NPCI and Banks have launched BHIM & other UPI based Mobile Applications with regulatory guidelines.

(viii) In addition, all organizations providing digital payment services have been mandated to report cyber security incidents to CERT-In expeditiously.

(ix) Apart from audits and incident reporting, Government has taken various steps to enhance user awareness to ensure security of digital payments. These include:

- Alerts and advisories are issued by CERT-In regarding latest cyber threats and countermeasures on regular basis. 21 Advisories have been issued by CERT-In regarding safeguards for users and institutions to secure digital payments.
- Cyber security awareness sessions have been conducted under the Digishala Awareness Campaign.

- Workshops have been held for banks and PPIs regarding security of digital payments systems.
- 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.
- 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.
- Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. Till date, 11 such drills have been conducted by the Indian Computer Emergency Response Team (CERT-In) involving 110 organizations from different sectors including Finance sector.

****