GOVERNMENT OF INDIA
MINISTRY OF FINANCE
DEPARTMENT OF FINANCIAL SERVICES

LOK SABHA
UNSTARRED QUESTION No. 1812
TO BE ANSWERED ON THE 10th MARCH, 2017, PHALGUNA 19, 1938(SAKA)

CYBER SECURITY INCIDENTS

1812. SHRI KAMAL NATH, SHRIMATI SANTOSH AHLAWAT,
SHRI JYOTIRADITYA M. SCINDIA

Will the MINISTER of FINANCE be pleased to state:

(a) whether the Reserve Bank of India has issued instructions to banks to report any cyber security incident within maximum six hours;

(b) if so, the details of cyber incidents came to the notice of the various banks in the past six months ad reported to RBI;

(c) whether there is sharp increase in cyber incidents in banks in the past few months ; and

(d) if so, the details thereof and the reasons therefor and the steps taken by the RBI/other banks to provide fool proof security to bank account holders?

ANSWER
(MINISTER OF STATE IN THE MINISTRY OF FINANCE)
(SHRI SANTOSH KUMAR GANGWAR)

(a): Banks have been advised to report all unusual cyber security incidents to Reserve Bank of India (RBI) within 2 - 6 hours of detection as per Circular no. DBS.CO/CSITE/BC.11/33.01.001/2015-16 dated June 2, 2016 on Cyber Security Framework.

(b): As of February 28, 2017 the details of the incidents reported by bank are as under:

Sl No	Type of Incidents	Total no of incidents reported
1	Ransomware	7
2	Distributed Denial of Service (DDos)	2
3	Phishing Attacks	6
4	Rogue Mobile Application	6
5	Card Skimming	3
6	Virus/Malware	13

(c) & (d): There is some increase in number of cyber incidents in banks. The data on frauds related to ATM / Credit / Debit cards & Net banking related frauds reported by the banks during last three years and current year is given in **Annexure I.** The measures taken to address the problem are mentioned in **Annexure II.**

Annexure I

Details of frauds reported in Credit Cards/ ATM/Debit Cards and Internet Banking Categories (Amount in Lakh)

Financial Year	**Credit Cards**		**ATM/ Debit Cards**		**Internet Banking**		**Total (All three categories)**	
	No. of Frauds	**Amount**	**No. of Frauds**	**Amount**	**No. of Frauds**	**Amount**	**No. of Frauds**	**Amount**
2013-14	7890	5481.59	1307	823.17	303	1495.83	9500	7800.59
2014-15	10382	4231.97	2498	1385.98	203	2445.8	13083	8063.75
2015-16	9849	4597.79	6585	3126.85	34	175.31	16468	7899.95
June, September, December Quarter 2016	4557	2156.78	4064	1900.8	68	158.18	8689	4215.76

Source: RBI

Annexure II

Measures taken to provide fool proof security to bank account holders

1. Banks were advised to take various preventive measures to combat frauds relating to skimming or duplicating of credit/debit cards and net banking related frauds. The banks, inter alia, were also advised to inform to customers not to reveal PIN in response to requests received through e-mail, to periodically verify the transaction history to ensure its correctness and if any unauthorized transaction observed it should be immediately reported to the bank and inform the bank if the card is lost or stolen.

2. In January 2016, Central Fraud Registry (CFR) has been operationised as searchable online central data base for use by the banks for frauds above Rs. 1 lakh. This data base is helpful to the banks not only during credit decisions but also to know about fraud in other areas of the banking including cyber frauds, ATM/debit/ credit card and internet banking.

3. Caution advices are also issued as and when necessary for preventing and controlling the frauds. Two caution advices (copies enclosed) have been issued recently in connection with (i) Fraud in Mobile Application (CA No. 4097) and (ii) ATMs-Large value cash shortages-Malware attacks (CA No. 4087).

4. On September 28, 2016,RBI have reiterated instruction vide circular DBS.CO.CFMC.BC.No.6/23.04.001/2016-17 dated September 28, 2016 on funds transfer requirement received through email/fax messages. Banks were advised to strengthen the mechanism put in place by them in this regards and also to adhere to it strictly, including contacting the customer over phone at his registered phone number to ensure genuineness of request of the customer. RBI have also advised banks that the issue encompasses both cyber security and customer liability, and, therefore banks should sensitize their staff suitably to be vigilant.

5. In order to focus more attention on IT related matters, Reserve Bank has set up a Cyber Security and IT Examination (CSITE) Cell within its Department of Banking Supervision in 2015. The comprehensive circular on Cyber Security Framework in Banks issued on June 2, 2016 covers best practices pertaining to various aspects of cyber security. The circular requires banks to have among other things, a cyber-security policy, cyber crisis management plan, a gap assessment vis-a-vis the baseline requirements indicated in the circular, monitoring certain risk indicators in this area, report unusual cyber security incidents within 2 to 6 hours, ensure board involvement in the matter and robust vendor risk management. The progress of banks in scaling up their cyber security preparedness is monitored.

6. RBI has also set up a Cyber Crisis Management Group to address any major incidents reported including suggesting ways to respond. Further, Department of Banking Supervision conducts cyber security preparedness testing among banks on the basis of hypothetical scenarios with the help of CERT-In. RBI carries out IT Examination of banks separately from the regular financial examination of the banks from last year. This report has a special focus on cyber security. The reports have been issued to the banks for remedial action.

7. An inter-disciplinary Standing Committee on Cyber Security as indicated in the Statement on Developmental and Regulatory Policies issued along with the Sixth Bi-monthly Monetary Policy Statement, 2016-17 announced on February 8, 2017 has been constituted. The Committee, inter alia, reviews the threats inherent in the existing/emerging technology and suggest appropriate policy interventions to strengthen cyber security and resilience.

8. RBI has also set up an IT Subsidiary, which would focus, among other things, on cyber security within RBI as well as in regulated entities. The subsidiary is in the process of recruiting the experts.