

**GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA**

STARRED QUESTION NO:568
ANSWERED ON:06.05.2015
FRAUDS BY E MAIL AND SMS
Thomas Prof. Kuruppassery Varkey

Will the Minister of COMMUNICATIONS AND INFORMATION TECHNOLOGY be pleased to state:

- (a) whether the Government is aware of frauds being committed via e-mail and SMS;
- (b) if so, the details thereof including the number of such frauds reported and the losses incurred during the last three years ; and
- (c) the steps taken/proposed to be taken by the Government to prevent such fraudulent activities?

Answer

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

(a)to (c): A statement is laid on the Table of the House.

STATEMENT REFERRED TO IN REPLY TO LOK SABHA STARRED QUESTION NO. 568 FOR 06.05.2015 FRAUDS BY E-MAIL AND SMS

(a)and (b): Several cyber attack techniques are used in combination while committing cyber frauds. The fraudulent activities comprising of phishing, lottery scams, ATM/ Credit Card frauds, internet banking frauds, and other banking frauds involve usage of e-mail and SMS to trick the users to steal their identity credentials and commit fraud. Losses are normally computed as a whole with respect to each category of cyber crimes reported in the area of operation such as ATM/Debit cards, credit cards, Internet Banking etc.

As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In) a total number of 887, 955, 1122 and 84 security incidents pertaining to phishing were handled during the year 2012, 2013, 2014 and 2015 (upto March) respectively.

According to the data maintained by Reserve Bank of India (RBI) a total number of 10048, 8765, 9500, 9362 cases of Credit Cards, ATM/Debit Cards and Internet Banking frauds resulting in losses of Rs. 38, 68, 78 and 60 crores were reported during the year 2011-2012, 2012-13, 2013-14 and April – December 2014 respectively.

As per Central Bureau of Investigation (CBI), a total no. of 8 cases have been registered relating to frauds committed by e-mail & SMS during the year 2012, 2013, 2014 and 2015 (upto 31.03.2015). The losses incurred in these cases were to the tune of Rs. 3.25 lakhs and USD 3,37,962.

(c): Government has taken following steps to prevent fraudulent activities and cyber crimes in the country:

i) CERT-In is working in coordination with Reserve Bank of India (RBI) and banks to track and disable phishing websites.

ii) Banks have implemented Two-factor authentication to mitigate risks due to theft of online credentials. Besides, SMS alerts are sent to users intimating details of transactions involving amounts above specified threshold.

iii) To create awareness about possible frauds by using email and SMS, advisories are being issued by Banks, Telecom Service Providers and Police Authorities from time to time to the users.

iv) Banks are creating user awareness for general public against phishing, lottery scams, internet banking, Credit/Debit cards and other frauds.

v) Steps have been taken to monitor and prevent financial frauds through phishing attacks, Credit / Debit card frauds, money laundering schemes etc.

vi) Indian Computer Emergency Response Team (CERT-In) has published whitepapaer on countering phishing attacks and regularly conducts training programme for system administrators and general users in the Government, public and private sector on countering cyber frauds and phishing attacks.

vii) The Information Technology Act, 2000, provides legal framework to address various types of prevalent cyber crimes and security

breaches of information technology infrastructure.

viii) Government has set up cyber forensic training and investigation labs in the States of Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur and Jammu & Kashmir for training of Law Enforcement and Judiciary in these States.

ix) Cyber Crime Cells have been set up in all States and Union Territories for reporting and investigation of Cyber Crime cases.

x) Academia like National Law School, Bangalore and NALSAR University of Law, Hyderabad are also engaged in conducting several awareness and training programmes on Cyber Laws and Cyber crimes for judicial officers.

xi) Number of Cyber forensics tools for collection, analysis, presentation of the digital evidence have been developed and are being used by Law Enforcement Agencies.

xii) Indian Computer Emergency Response Team (CERT-In) and Centre for Development of Advanced Computing (CDAC) are involved in providing basic and advanced training to Law Enforcement Agencies, Forensic labs and judiciary on the procedures and methodology of collecting, analysing and presenting digital evidence.

xiii) Government has formulated a set of investigation manuals with procedures for Search, Seizure Analysis and Presentation of digital evidence in courts. The manuals have been circulated to Law Enforcement Agencies in all States.

xiv) Department of Electronics & Information Technology (DEITY) is conducting programs to generate information security awareness. Specific book, videos and online materials are developed for children, parents and general users about information security which are disseminated through Portals like "secureyourpc.in" and "www.secureyourelectronics.in".