GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 4521
TO BE ANSWERED ON: 29.03.2017

FINANCIAL CYBER CRIME

4521. SHRI DUSHYANT SINGH:
SHRI MANOJ TIWARI:

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

(a) whether there has been an exponential increase in number of financial cyber crime cases in the country in the last three years;
(b) if so, the details regarding the kind of financial crimes that have increased with digitalization;
(c) the steps that have been taken to counter financial cyber crimes;
(d) whether the Government has any mechanism to help State Governments to ensure security of important Government Data and if so, the details thereof;
(e) whether the Government has any update about the fraud web companies which duped thousands of innocent people and if so, the details thereof, State-wise; and
(f) the steps taken by the Government in this regard?

ANSWER

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

(a) and (b): National Crime Record Bureau (NCRB) collects and maintains statistical data of police recorded cognizable crimes from 35 States /Union Territories. As per the data maintained by NCRB, following data pertains to financial cyber crime cases in the country:

Type of case	**2013**	**2014**	**2015**	**% Increase / Decrease in 2014 since 2013**	**% Increase / Decrease in 2015 since 2014**
Cheating using computer as a medium or target.	-	1115	2255	-	102.2
Forgery using computer as a medium or target	747	63	45	-91.5	-28.6
Criminal breach of trust/fraud using computer as a medium or target	518	54	42	-89.6	-22.2
Counterfeiting using computer as a medium or target	59	10	12	-83.0	20.0

Further, as per the data made available by Reserve Bank of India (RBI), 9500, 13083 and 16468 cases related to Cyber Frauds (ATM/ Debit Card, Credit Card & Net Banking frauds) were reported by the banks during 2013-14,2014-15 and 2015-16 respectively.

(c): Strengthening of cyber security is a continuing process. It is the primary responsibility of agencies providing digital payment options / systems to maintain adequate cyber security of their payment systems to avoid any mishap. Besides, Govt. has taken several steps towards enabling a secure online payment systems. These, inter alia, include:

(i) RBI has issued a comprehensive circular on "Cyber Security Framework in Banks" on June 2, 2016 covering best practices pertaining to various aspects of cyber security.

(ii) RBI has issued circular on 09th December 2016 on Security and Risk mitigation measure for all authorised entities / banks issuing Prepaid Payment Instrument (PPI) in the country.

(i) (CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities alongwith countermeasures to create awareness among stakeholders to take appropriate measures to ensure safe usage of digital technologies. 21 advisories have been issued for users and institutions pertaining to digital payments.

(ii) In addition, all authorised entities/banks issuing Prepaid Payment Instruments (PPIs) in the country have been advised by Indian Computer Emergency Response Team (CERT-In) to carry out audit by the empanelled auditors of CERT-In on a priority basis and take immediate steps thereafter to comply with the findings of the audit report and ensure implementation of security best practices.

(iii) All organizations providing digital payment services have been mandated to report cyber security incidents to CERT-In expeditiously.

(iv) Reserve Bank of India (RBI) carries out IT Examination of banks separately from the regular financial examination of banks from last year. This examination report has a special focus on cyber security. The reports have been issued to the banks for remedial action.

(v) RBI has also set up Cyber Crisis Management Group to address any major incidents reported including suggesting ways to respond and recover to/ from the incidents.

(vi) RBI also conducts cyber security preparedness testing among banks on the basis of hypothetical scenarios with the help of CERT-In.

(vii) RBI has also set up an IT subsidiary, which would focus, inter-alia on cyber security within RBI as well as in regulated entities.

(viii) In addition, RBI issues Circulars/advisories to all Commercial Banks on phishing attacks and preventive / detective measures to tackle phishing attacks.

(ix) RBI has set up a Cyber Security and IT Examination (CSITE) cell within its Department of Banking Supervision in 2015.

(x) Ministry of Electronics & Information Technology (MeitY) has formulated draft rules on Security of Prepaid Payment Instruments under Information Technology Act, 2000. The objective of the proposed rules is to ensure adequate integrity, security and confidentiality of electronic payments effected through electronic prepaid payment instruments. The draft rules have been published on MeitY website inviting comments from public at large and all stakeholders.

(d): Government by virtue of Information Technology (IT) Act, 2000 and organisations like Indian Computer Emergency Response Team (ICERT) and National Critical Information Infrastructure Protection Centre. (NCIIPC) created under the provisions of this Act provides security mechanisms for any orgnaisation the country. Further, State IT infrastructure including state data centers and state wide area network are required to follow security best practices as defined in national and international standards.

(e): Government has not carried out any study in this regard.
(f): Does not arise.

****