GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO.6207
TO BE ANSWERED ON: 04.04.2018

INCREASE IN CYBER CRIME

6207. SHRI GOPAL SHETTY:

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

(a) whether the proportion of cyber crime is constantly increasing amid the rising impact of information technology in the country;

(b) whether crores of rupees are misappropriated/siphoned off every year in the country through cyber crime;

(c) if so, the details in this regard for the last three years; and

(d) the details of the steps being taken by the Government with a view to check cyber crime?

ANSWER

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

(a) to (c): As per the data maintained by National Crime Records Bureau (NCRB), Ministry of Home Affairs, a total of 9622, 11592 and 12317 cyber crime cases were registered during the years 2014, 2015 and 2016 respectively. These include cases registered under the Information Technology Act, 2000 and related sections of Indian Penal Code and Special & Local Laws involving computer as medium/target. Further, as per information provided by Reserve Bank of India (RBI) cases of frauds involving credit cards, ATM / debit cards and internet banking during the year 2014-15, 2015-16, 2016-17 and for the period April-December 2017 is as follows :

Period	**Credit Cards**		**ATM/Debit Cards**		**Internet Banking**		**Total**	
	1		**2**		**3**		**1+2+3**	
	No. of frauds	**Amount involved (in Rs. lakh)**	**No. of frauds**	**Amount involved (in Rs. lakh)**	**No. of frauds**	**Amount involved (in Rs. lakh)**	**No. of frauds**	**Amount involved (in Rs. lakh)**
2014-15	10382	4231.97	2498	1385.98	203	2445.80	**13083**	**8063.75**
2015-16	9849	4597.79	6585	3126.85	34	175.31	**16468**	**7899.95**
2016-17	6811	3202.61	6709	3866.89	133	198.43	**13653**	**7267.93**
April - Dec 2017	15952	5082.34	7804	7542.1	109	642.95	**23865**	**13267.39**

(d): Government has taken a number of legal, technical and administrative measures to prevent cyber crimes. These *inter alia*, include:

(i) Enactment of the Information Technology (IT) Act, 2000 which has adequate provisions for dealing with prevalent cyber crimes.

(ii) Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) as per the provisions of Section 70A of the IT Act, 2000 for protection of critical information infrastructure in the country.

(iii) The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis. CERT-In has published guidelines for securing IT infrastructure, which are available on its website (www.certin.org.in).

(iv) Government has set up National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities. Phase-I of NCCC has already been made operational.

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

(vi) 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 personnel and Judiciary in these States.

(vii) RBI, vide its circular on "Cyber Security Framework in Banks", has advised banks to report all unusual cyber security incidents to RBI. RBI reviews cyber security developments and threats on an ongoing basis and takes necessary measures to strengthen the cyber-resilience of banks. RBI has also advised banks to take necessary preventive and corrective measures address various types of cyber-threats. Caution advices are also issued as and when necessary for preventing and controlling frauds.

(viii) 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. Regular workshops are conducted for Ministries, Departments, States & Union Territories and critical organizations to sensitize them about the cyber security threat landscape and enabling them to prepare and implement the Cyber Crisis Management Plan.

(ix) 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.

(x) Cyber security exercises 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 wherein organisations from different sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS etc. participated.

****