GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 2287
TO BE ANSWERED ON: 15.03.2017

GLOBAL FRAUD AND RISK SURVEY

2287 SHRI S.R. VIJAYAKUMAR: SHRI T. RADHAKRISHNAN: SHRI GAJANAN KIRTIKAR: SHRI SUDHEER GUPTA: KUNWAR HARIBANSH SINGH: DR. SUNIL BALIRAM GAIKWAD: SHRI ASHOK SHANKARRAO CHAVAN:

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

(a) whether according to the 'Global Fraud and Risk Survey for 2016', one out of five top executives of global corporations have expressed their apprehensions over investing in India due to concerns over fraudulent practices and cyber security lapses and if so, the details thereof along with other issues raised in the survey;
(b) the number of cyber fraud incidents reported during each of the last three years and the current year along with the action taken/being taken by the Government in this regard, State/UT-wise;
(c) whether there are large number of fake accounts on various e-mail and social networking sites which are being used for committing cyber fraud/crime;
(d) if so, the details thereof along with the action taken/being taken by the Government in this regard; and
(e) the corrective measures taken/being taken by the Government on the findings of the Global Fraud and Risk Survey, 2016?

ANSWER

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

(a) : There have been media reports based on the 'Global Fraud and Risk Survey for 2016' indicating one out of five top executives of global corporations have expressed their apprehensions over investing in India due to concerns over fraudulent practices and cyber security lapses. However, the report has highlighted reduction in cyber fraud and cyber security incidents cases in past twelve months in India.

(b) and (e) : National Crime Records Bureau (NCRB) collects and maintains statistical data of police recorded cognizable crimes including cyber frauds and cyber crimes from 35 States /Union Territories. As per the data maintained by NCRB, a total of 1600 and 3383 cases were registered under cyber fraud using computer as medium/target during the year 2014 and 2015. Data for the year 2016 is under collection. State/UT-wise data during 2014-2015 is enclosed as Annexure-I.

Government has taken various steps in the form of legal framework, awareness, training, and implementation of best practices to address issues related to cyber crimes including risk identified in the report. These include:

(i) The IT Act, 2000 provides a comprehensive legal framework to address the issues connected with cyber crime, cyber attacks and security breaches of information technology infrastructure.

(ii) Ministry of Electronics & Information Technology (MeitY) has recently notified the scheme for evaluating any Department, body or agency of the Central Government or a State Government to notify them as Examiner of Electronic Evidence under section 79A of IT Act, 2000.

(iii) Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis. CERT-In has issued 17 advisories since Nov 27, 2016 for security safeguards covering Point of Sale (POS) machines, Micro ATMs, electronic Wallets, online banking, smart phones, Unified Payment Interface (UPI), Unstructured Supplementary Service Data (USSD), RuPay, SIM cards, wireless access points / routers, mobile banking, cloud and Aadhaar Enabled Payment System (AEPS). Advisory has also been sent by CERT-In to RBI, National Payment Corporation of India Limited (NPCIL) and Payment Card Industry Organizations covering precautions to be taken to avoid similar attacks as those that occurred recently with credit / debit cards.

(iv) CERT-In is conducting cyber security trainings for IT / cyber security professionals including Chief Information Security Officers (CISOs) of Government and critical sector organisations. 18 such training programs were conducted covering 580 participants during the year 2016. In addition 2 workshops on security of digital payments systems have been conducted for stakeholder organisations covering 110 participants.

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

(vi) With respect to the banking sector, in order to focus more attention on IT related matters, Reserve Bank of India (RBI) has taken various steps which include :

- RBI has set up a Cyber Security and IT Examination (CSITE) cell within its Department of Banking Supervision in 2015.
- The Bank 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.
- RBI carries out IT Examination of banks separately from the regular financial examination of banks since last year. The outcome reports with special focus on cyber security have been issued to the banks for remedial action.
- RBI has also set up Cyber Crisis Management Group to address any major incidents reported including suggesting ways to respond to and recover from the incidents.
- Department of Banking Supervision under RBI also conducts cyber security preparedness testing among banks on the basis of hypothetical scenarios with the help of CERT-In.
- RBI also has set up an IT subsidiary, which would focus, among other things, on cyber security within RBI as well as in regulated entities.
- RBI has issued circular on 09th December 2016 on Security and Risk mitigation measure for all authorised entities / banks issuing Prepaid Payment Instruments (PPI) in the country.
- In addition, RBI issues Circulars/advisories to all Commercial Banks on phishing attacks and preventive / detective measures to tackle phishing attacks.

(c) and (d) : The cyberspace is virtual, borderless and anonymous. Anyone can open account in any name including fake name from any part of the world. Any user with an email address is allowed to register with social networking sites with any name. No background information

check is performed by the social networking sites, which occasionally leads to creation of fake account by miscreants for committing crimes. Law enforcement agencies take necessary action to deal with cyber fraud/crime including shutting down fake accounts.

Government does not regulate content appearing on social networking sites. Information Technology (IT) Act, 2000 has provisions for removal of objectionable online content. The Information Technology (Intermediary Guidelines) Rules 2011 notified under section 79 of the IT Act require that the Intermediaries shall observe due diligence while discharging their duties and shall inform the users of computer resources not to host, display, upload, modify, publish, transmit, update or share any information that is harmful, objectionable, affects minors or is unlawful in anyway.

Further, section 69A of IT Act, 2000 provides for blocking for access of information under specific conditions related to interest of Sovereignty and Integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above.

****

Annexure-I

Cases Reported(CR), Persons Arrested(PAR), Cases Chargesheeted(CS), Persons Chargesheeted(PCS), Cases Convicted (CON) and Persons Convicted under under Various Heads Cyber Crimes During During 2014-2015

		2014						2015					
SL	STATE/UT	CR	PAR	CCS*	PCS*	CON*	PCV*	CR	PAR	CCS*	PCS*	CON*	PCV*
1	Andhra Pradesh	79	58	6	8	0	0	105	83	13	16	0	0
2	Arunachal Pradesh	4	0	0	0	0	0	0	0	0	0	0	0
3	Assam	0	0	0	0	0	0	7	3	0	0	0	0
4	Bihar	0	0	0	0	0	0	28	1317	5	13	0	0
5	Chhattisgarh	14	6	4	6	0	0	14	13	8	10	0	0
6	Goa	18	1	0	0	1	2	4	0	0	0	0	0
7	Gujarat	74	20	7	11	0	0	97	34	21	40	0	0
8	Haryana	7	7	3	7	0	0	49	25	8	20	0	0
9	Himachal Pradesh	0	0	0	0	0	0	0	0	0	0	0	0
10	Jammu & Kashmir	0	0	0	0	0	0	1	0	0	0	0	0
11	Jharkhand	0	0	0	0	0	0	4	0	0	0	0	0
12	Karnataka	52	8	3	4	0	0	429	26	10	11	0	0
13	Kerala	47	17	6	7	1	1	52	16	15	18	0	0
14	Madhya Pradesh	59	55	48	55	0	0	46	28	16	25	0	0
15	Maharashtra	738	206	105	157	1	1	1328	273	98	205	0	0
16	Manipur	3	0	0	0	0	0	2	0	0	0	0	0
17	Meghalaya	20	4	4	4	0	0	21	3	2	2	0	0
18	Mizoram	3	0	0	0	0	0	0	0	0	0	0	0
19	Nagaland	0	0	0	0	0	0	0	0	0	0	0	0
20	Odisha	28	4	4	4	0	0	233	44	20	38	0	0
21	Punjab	12	8	1	1	0	0	3	5	1	1	0	0
22	Rajasthan	121	22	13	22	0	0	218	49	30	49	0	0
23	Sikkim	0	0	0	0	0	0	0	0	0	0	0	0
24	Tamil Nadu	46	9	2	2	0	0	22	14	16	19	0	0
25	Telangana	28	10	3	3	1	1	408	265	18	22	0	0
26	Tripura	0	0	0	0	0	0	4	3	0	0	0	0
27	Uttar Pradesh	134	72	38	41	0	0	110	139	74	115	9	13
28	Uttarakhand	0	0	0	0	0	0	5	2	0	0	0	0
29	West Bengal	45	25	9	9	0	0	69	12	10	10	0	0

	TOTAL STATE(S)	**1532**	**532**	**256**	**341**	**4**	**5**	**3259**	**2354**	**365**	**614**	**9**	**13**
30	A & N Islands	9	3	2	3	0	0	1	1	2	2	0	0
31	Chandigarh	26	11	7	7	0	0	60	10	6	7	3	3
32	D&N Haveli	0	0	0	0	0	0	0	0	0	0	0	0
33	Daman & Diu	0	0	0	0	0	0	0	0	0	0	0	0
34	Delhi UT	33	9	2	2	0	0	63	11	9	10	0	0
35	Lakshadweep	0	0	0	0	0	0	0	0	0	0	0	0
36	Puducherry	0	0	0	0	0	0	0	0	0	0	0	0
	TOTAL UT(S)	**68**	**23**	**11**	**12**	**0**	**0**	**124**	**22**	**17**	**19**	**3**	**3**
	TOTAL (ALL INDIA)	**1600**	**555**	**267**	**353**	**4**	**5**	**3383**	**2376**	**382**	**633**	**12**	**16**

Source: Crime in India

'*' Data Colletion since 2014

Note: The data includes heads "Criminal Breach of Trush+Cheating+Computer Related Offences Section 66D+Create/publish/make available Electronic Signature Certificate for fraudulent/unlawful purpose (Section 74))