CYBER CRIMES

1205   KUMARI SELJA:

Will the Minister of Electronics & Information Technology be pleased to state:-
(a)   the details of cyber crimes reported during the last two years and the present status of the said crimes;
(b)   the percentage increase in such crimes during the said period, State-wise; and
(c)   whether the Government has taken any steps to tackles cyber crime incidents with stringent cyber laws to make online transactions fool proof; and if so, the details thereof?

ANSWER

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

(a) and (b): With the proliferation of Information Technology and related services there is a rise in instances of cyber crimes in the country like elsewhere in the world. As per the data maintained by National Crime Records Bureau (NCRB), a total of 9622 and 11592 cyber crime cases were registered during the years 2014 and 2015 respectively, showing a rise of 20% during 2014 to 2015. This includes cases registered under the Information Technology (IT) Act, 2000 and related sections of Indian Penal Code and Special & Local Laws involving computer as medium/ target.   State/UT-wise data during 2014-2015 is enclosed as Annexure-I.

(c): Government has taken various steps to tackle the cyber crime incidents on the Internet. It includes:

(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), Micro ATMs, electronic Wallets, online banking, smart phones, unified payment interface, 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 (NPCI) 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, RBI has taken various action which includes:
-      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 from last year with focus on cyber security and communicates outcomes to banks for remedial action.
- 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.
- 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 Instrument (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.

****

Annexure-I

Serial Number	State/UT	2014#	2015#	% variation in 2015 over 2014
1	Andhra Pradesh	282	536	90.1
2	Arunachal Pradesh	18	6	-66.7
3	Assam	379	483	27.4
4	Bihar	114	242	112.3
5	Chhattisgarh	123	103	-16.3
6	Goa	62	17	-72.6
7	Gujarat	227	242	6.6
8	Haryana	151	224	48.3
9	Himachal Pradesh	38	50	31.6
10	Jammu & Kashmir	37	34	-8.1
11	Jharkhand	93	180	93.5
12	Karnataka	1020	1447	41.9
13	Kerala	450	290	-35.6
14	Madhya Pradesh	289	231	-20.1
15	Maharashtra	1879	2195	16.8
16	Manipur	13	6	-53.8
17	Meghalaya	60	56	-6.7
18	Mizoram	22	8	-63.6
19	Nagaland	0	0	0.0
20	Odisha	124	386	211.3
21	Punjab	226	149	-34.1
22	Rajasthan	697	949	36.2
23	Sikkim	4	1	-75.0
24	Tamil Nadu	172	142	-17.4
25	Telangana	703	687	-2.3
26	Tripura	5	13	160.0
27	Uttar Pradesh	1737	2208	27.1
28	Uttarakhand	42	48	14.3
29	West Bengal	355	398	12.1
	TOTAL STATE(S)	**9322**	**11331**	21.6

30	A & N Islands	13	6	-53.8
31	Chandigarh	55	77	40.0
32	D&N Haveli	3	0	-100.0
33	Daman & Diu	1	1	0.0
34	Delhi UT	226	177	-21.7
35	Lakshadweep	1	0	-100.0
36	Puducherry	1	0	-100.0
	TOTAL UT(S)	**300**	**261**	-13.0
	TOTAL (ALL INDIA)	**9622**	**11592**	20.5
	Source: Crime in India			