GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 391
TO BE ANSWERED ON: 22.07.2021

INCREASE IN SOCIAL ENGINEERING FRAUDS AND ATTACKS

391   SHRI P. WILSON:

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

(a) whether Government has taken steps to tackle the menace of various organised online social engineering frauds and attacks, if so, the details thereof including the number of such cases reported during each of the last three years, State/UT-wise including Tamil Nadu;

(b) whether Government has developed and encouraged the expertise in this field which could detect these type of online frauds by providing necessary support to these type of investigations and if so, the details thereof; and

(c) details of the action taken by Government in this regard and the measures being taken by Government to strengthen cyber security frauds?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAJEEV CHANDRASEKHAR)

(a) As per National Crime Records Bureau (NCRB), the State/UT wise cases registered under fraud for cyber-crimes involving communication devices as medium/target during 2017-2019 are given at Annexure – I.

As per information reported to and tracked by the Indian Computer Emergency Response Team (CERT-In), activities of fraudulent emails, SMS messages and phishing websites pretending to be from legitimate services, are reported luring users to divulge credentials to conduct frauds. A total number of 454, 472, 280 and 138 phishing incidents were observed by CERT-Induring the year 2018, 2019, 2020 and 2021 (upto June) respectively.

(b) Government has taken the following measures for reporting and investigation of online frauds:

i) Government has launched National Cyber Crime reporting portal namely www.cybercrime.gov.in to enable public to report incidents pertaining to all types of cyber crimes with a special focus on cyber crimes against women and children.
ii) CERT-In works in coordination with service providers, regulators and Law Enforcement Agencies (LEAs) to track and disable phishing websites and facilitate investigation of fraudulent activities.

(c) Government has taken following measures to enhance the cyber security posture in the country:

i. CERT-In issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis to ensure safe usage of digital technologies. CERT-In has issued 60 advisories for data security and mitigating fraudulent activities.

ii. Security tips have been published for users to secure their Desktops, mobile/smart phones and preventing phishing attacks.

iii. Government has empanelled security auditing organisations to support and audit implementation of Information Security Best Practices.

iv. Cyber security mock drills are conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 53 such drills have so far been conducted by CERT-In where 479 organisations from different States and sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS, etc participated.

v. Government has set up the National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats. Phase-I of NCCC is operational.

vi. Government is operating 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 citizens and organisations.

vii. Ministry of Electronics & Information Technology (MEITY) is conducting programs to generate information security awareness. Specific books, videos and online materials are developed for children, parents and general users about information security which are disseminated through portals like "www.infosecawareness.in" and "www.cyberswachhtakendra.gov.in".

****

As per National Crime Records Bureau (NCRB), the State/UT wise cases registered for fraud (section 420 read with section 465, 468-471 IPC read with Information Technology Act) under cybercrimes during 2017-2019 are given below:

SL	State/UT	2017	2018	2019
1	Andhra Pradesh	166	195	703
2	Arunachal Pradesh	0	0	0
3	Assam	5	6	83
4	Bihar	427	357	1008
5	Chhattisgarh	33	18	35
6	Goa	0	0	0
7	Gujarat	123	139	107
8	Haryana	53	0	107
9	Himachal Pradesh	0	0	0
10	Jammu & Kashmir	3	3	6
11	Jharkhand	72	175	18
12	Karnataka	11	49	7
13	Kerala	20	14	14
14	Madhya Pradesh	66	43	25
15	Maharashtra	1426	1036	1681
16	Manipur	5	0	0
17	Meghalaya	3	0	0
18	Mizoram	0	0	0
19	Nagaland	0	0	0
20	Odisha	333	392	956
21	Punjab	5	7	35
22	Rajasthan	92	72	324
23	Sikkim	0	0	0
24	Tamil Nadu	21	5	11
25	Telangana	277	347	282
26	Tripura	3	0	0
27	Uttar Pradesh	270	454	813
28	Uttarakhand	1	28	3
29	West Bengal	22	4	4
	TOTAL STATE(S)	**3437**	**3344**	**6222**
30	A&N Islands	0	2	0
31	Chandigarh	6	2	0
32	D&N Haveli	0	0	0
33	Daman & Diu	0	0	0
34	Delhi	23	3	11
35	Lakshadweep	0	2	0
36	Puducherry	0	0	0
	TOTAL UT(S)	**29**	**9**	**11**
	TOTAL (ALL INDIA)	**3466**	**3353**	**6233**

******

******