GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 1638
TO BE ANSWERED ON: 27.07.2022

PREVENTION OF CYBER CRIMES

1638. SHRI RAJESH VERMA:
SHRI SANJAY SETH:

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

(a) whether the Government is aware of the large scale incidents of withdrawal of money through message and other means by cyber criminals in Jharkhand;

(b) if so, the details thereof including the action taken to check the above incidents;

(c) the State-wise details of the victims of cyber crimes during the last two years;

(d) whether the Government has formulated any plan to prevent/check cyber crime/attack and if so, the details thereof along with its outcome; and

(e) the details of increase in cyber crimes in Uttar Pradesh during the last two years?

ANSWER

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

(a) and (b): Yes sir. With the growth of the internet and proliferation of applications, products & services on it, citizens are being empowered and their lives transformed. However, with the growth of the internet, cyber crimes are also on the increase. The Government is aware of cyber crimes incidents including phishing originating in some parts of India including Jharkhand.

'Police' and 'Public Order' are State subjects as per the Seventh Schedule of the Constitution of India. States/UTs are primarily responsible for the prevention, detection, investigation and prosecution of crimes including cyber crime through their Law Enforcement Agencies (LEAs). The LEAs take legal action as per provisions of law against the offenders. The Central Government supplements the initiatives of the State Governments through advisories and financial assistance under various schemes for their capacity building.

As per Ministry of Home Affairs (MHA), to strengthen the mechanism to deal with cyber crimes in a comprehensive and coordinated manner, the Ministry of Home Affairs has provided financial assistance to all the States & UTs under Cyber Crime Prevention against Women & Children (CCPWC) scheme to support their efforts for setting up of cyber forensic-cum-training laboratories, training, and hiring of junior cyber consultants. Cyber forensic-cum-training laboratories have been commissioned in 28 States. The Central Government has taken steps for spreading awareness about cyber crimes, issuance of alerts/ advisories, capacity

building/ training of law enforcement personnel/ prosecutors/ judicial officers, improving cyber forensic facilities etc.

The Government has established Indian Cyber Crime Coordination Centre (I4C) to provide a framework and eco-system for LEAs to deal with the cyber crimes in a comprehensive and coordinated manner. 'Joint Cyber Coordination Teams' have been constituted for seven regions at Mewat, Jamtara, Ahmedabad, Hyderabad, Chandigarh, Vishakhapatnam and Guwahati under the I4C to address the issue of jurisdictional complexity, based upon cyber crime hotspots/ areas, by on-boarding all the States/UTs to provide a robust coordination framework to the LEAs.

The Government has launched the National Cyber Crime Reporting Portal (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. A toll-free number 1930 has been operationalized to get assistance in lodging online cyber complaints. The Citizen Financial Cyber Fraud Reporting and Management System module has also been launched for immediate reporting of financial frauds and to stop siphoning off fund by the fraudsters.

(c): State-wise details of the victims of cyber crimes during 2019-20 as provided by National Crime Record Bureau (NCRB) is enclosed as Annexure -I.

(d): Government is fully cognizant and aware of various cyber security threats; and has taken following measures to enhance the cyber security posture and prevent cyber-attacks:

(i) Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on regular basis. CERT-In has issued 70 advisories for organisations and users to create awareness on safe usage of digital technologies.

(ii) CERT-In operates an automated cyber threat exchange platform to proactively collect, analyse and share tailored alerts with organisations across sectors for proactive threat mitigation actions by them.

(iii) Security tips have been published for users to secure their Desktops, mobile/smart phones and prevent phishing attacks.

(iv) Government has issued guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities to secure applications / infrastructure and compliance.

(v) All the government websites and applications are audited with respect to cyber security prior to their hosting. The auditing of the websites and applications is conducted on a regular basis after hosting also.

(vi) CERT-In has empanelled 97 security auditing organisations to support and audit implementation of Information Security Best Practices.

(vii) CERT-In has formulated a Cyber Crisis Management Plan for countering cyber attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.

(viii) Cyber security mock drills are conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 67 such drills have so far been conducted by CERT-In where 886 organizations from different States and sectors participated.

(ix) CERT-In conducts regular training programmes for network / system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organisations regarding securing the IT infrastructure and mitigating cyber attacks. 19 and 5 training programs were conducted covering 5169 and 449 participants during the year 2021 and 2022 (upto June) respectively.

(x) CERT-In operates the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre provides detection of malicious programs and free tools to remove the same alongwith cyber security tips and best practices for citizens and organisations.

(xi) CERT-In 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.

(xii) CERT-In also co-operates, works and coordinates incident response measures with international CERTs, overseas organisations and service providers as well as Law Enforcement Agencies.

(xiii) CERT-In provides the requisite leadership for the Computer Security Incident Response Team-Finance Sector (CSIRT-Fin) operations under its umbrella to respond to, contain and mitigate cyber security incidents reported from the financial sector.

(xiv) Computer Security incident Response Team-Finance (CSIRT-Fin), CERT-In, National Institute of Securities Markets (NISM) and Centre for Development of Advanced Computing (CDAC) are conducting a self-paced 60 hour certification program on "Cyber Security Foundation Course" for professionals in financial sector.

(xv) CERT-In regularly disseminates information and share security tips on cyber safety and security through its official social media handles and websites. CERT-In organised various events and activities for citizens during Cyber Security Awareness Month in October 2021 and Safe Internet day on 8 February 2022 by posting security tips using posters and videos on social media platforms and websites. CERT-In in association with CDAC conducted online awareness campaign for citizens covering topics such as general online safety, social media risks and safety, mobile related frauds and safety, secure digital payment practices etc. through videos and quizzes on MyGov platform.

(xvi) CERT-In, Reserve Bank of India (RBI) and Digital India jointly carry out a cyber security awareness campaign on 'beware and be aware of financial frauds' through Digital India Platform.

(xvii) Ministry of Electronics & Information Technology (MeitY) conducts 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.csk.gov.in".

(e): As per the data provided by National Crime Record Bureau (NCRB), total number of cases registered under cyber crime in Uttar Pradesh were 11,416 and 11,097 in year 2019 and 2020 respectively.

****

Annexure-I

State/UT-wise Cases Registered(CR), Cases Charge sheeted(CCS), Cases Convicted(CON), Number of Victims (VIC), Persons Arrested(PAR), Persons Charge sheeted(PCS) and Persons Convicted(PCV) under Total Cyber Crimes during 2019-2020

SL	State/UT	2019							2020						
		CR	CCS	CON	TVIC	PAR	PCS	PCV	CR	CCS	CON	TVIC	PAR	PCS	PCV
1	Andhra Pradesh	1886	235	3	1909	452	344	5	1899	314	6	1917	475	446	9
2	Arunachal Pradesh	8	0	0	8	1	0	0	30	1	0	30	12	1	0
3	Assam	2231	349	13	2249	1636	733	13	3530	385	0	3556	1717	395	0
4	Bihar	1050	288	4	1050	1014	519	17	1512	651	0	1537	751	727	0
5	Chhattisgarh	175	94	13	178	139	136	19	297	152	3	299	209	188	3
6	Goa	15	20	0	15	3	25	0	40	6	0	41	15	15	0
7	Gujarat	784	447	0	784	1083	1064	0	1283	475	0	1292	942	906	0
8	Haryana	564	188	6	564	314	288	10	656	221	0	671	347	323	0
9	Himachal Pradesh	76	20	2	76	44	24	2	98	31	0	99	46	39	0
10	Jharkhand	1095	344	19	1095	402	568	19	1204	462	125	1219	820	791	131
11	Karnataka	12020	111	9	12159	446	183	10	10741	2842	2	10882	489	2916	2
12	Kerala	307	176	2	313	220	214	2	426	161	0	447	299	179	0
13	Madhya Pradesh	602	405	18	610	659	531	24	699	445	14	714	692	598	15
14	Maharashtra	4967	980	7	5029	1739	1470	9	5496	902	3	5757	1735	1238	3
15	Manipur	4	0	0	4	8	0	0	79	0	0	82	17	0	0
16	Meghalaya	89	2	0	89	3	3	0	142	1	0	132	9	7	0
17	Mizoram	8	4	0	8	5	5	0	13	8	2	13	4	8	2
18	Nagaland	2	0	0	2	0	0	0	8	0	0	8	0	0	0
19	Odisha	1485	220	0	1486	316	351	0	1931	282	0	1934	369	396	0
20	Punjab	243	90	5	245	259	118	9	378	106	1	390	298	162	1
21	Rajasthan	1762	312	35	1770	571	556	41	1354	340	24	1388	541	520	32
22	Sikkim	2	1	0	2	3	2	0	0	0	0	0	0	0	0
23	Tamil Nadu	385	113	8	388	400	161	10	782	135	7	807	516	237	9
24	Telangana	2691	847	10	2700	748	1564	11	5024	939	280	5133	1169	1158	282
25	Tripura	20	4	0	20	1	5	0	34	5	0	34	6	5	0
26	Uttar Pradesh	11416	3705	201	11510	4324	5258	272	11097	4987	642	11360	6491	6427	878
27	Uttarakhand	100	40	1	103	71	72	1	243	58	0	266	93	80	0
28	West Bengal	524	104	4	526	215	124	4	712	178	0	721	203	313	0
	TOTAL STATE(S)	**44511**	**9099**	**360**	**44892**	**15076**	**14318**	**478**	**49708**	**14087**	**1109**	**50729**	**18265**	**18075**	**1367**
29	A&N Islands	2	0	0	2	0	0	0	5	5	0	5	3	5	0
30	Chandigarh	23	9	5	23	14	14	6	17	3	1	17	4	3	2
31	D&N Haveli and Daman & Diu+	3	0	0	3	1	0	0	3	1	0	3	1	1	0
32	Delhi	115	58	2	116	147	80	2	168	61	0	168	107	77	0
33	Jammu & Kashmir*	73	18	0	78	22	22	0	120	14	0	122	33	23	0
34	Ladakh	-	-	-	-	-	-	-	1	0	0	1	0	0	0
35	Lakshadweep	4	0	0	4	0	0	0	3	0	0	3	2	0	0
36	Puducherry	4	3	0	4	8	8	0	10	5	0	10	5	5	0
	TOTAL UT(S)	**224**	**88**	**7**	**230**	**192**	**124**	**8**	**327**	**89**	**1**	**329**	**155**	**114**	**2**
	TOTAL (ALL INDIA)	**44735**	**9187**	**367**	**45122**	**15268**	**14442**	**486**	**50035**	**14176**	**1110**	**51058**	**18420**	**18189**	**1369**

Source: Crime in India

Note : '+' Combined data of erstwhile D&N Haveli UT and Daman & Diu UT during 2019

*' Data of erstwhile Jammu & Kashmir State including Ladakh during 2019