GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS

LOK SABHA
UNSTARRED QUESTION NO. 3376

TO BE ANSWERED ON THE 21ST MARCH, 2023/ PHALGUNA 30, 1944 (SAKA)

CYBER FINANCIAL CRIMES

3376. SHRI M.K. RAGHAVAN:

Will the Minister of HOME AFFAIRS be pleased to state:

(a) whether the Government has observed that there is a huge rise in cyber financial crimes ever since adoption of digital payment systems in the country and if so, the details regarding the number of cyber financial crimes reported since 2019;

(b) the steps and measures taken to prevent cyber financial crimes in the country;

(c) whether there is rise in cyber digital crimes in the country by way of hacking computer servers and if so, the details regarding the same;

(d) the steps taken by the Government to ensure that our critical infrastructure is protected against cyber crimes; and

(e) whether the Government has any data regarding the number of district-wise cyber crimes reported for the State of Kerala and if so, the details regarding the same including the category of the crimes?

ANSWER

MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS
(SHRI AJAY KUMAR MISHRA)

(a) to (d) : With enhanced use of cyber space, number of cyber crimes is also increasing. The National Crime Records Bureau (NCRB) compiles and publishes the statistical data on crimes in its publication "Crime in India". The latest published report is for the year 2021. As per the data published by the NCRB, Crime Head-wise details of cases registered under cyber crimes (involving communication devices as medium/target) during the period from 2019 to 2021 is at the Annexure-I.

'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 financial crimes. The Central Government supplements the initiatives of the State Governments through advisories and schemes for the capacity building of their Law Enforcement Agencies (LEAs). To strengthen the mechanism to deal with cyber crimes including cyber crime against critical infrastructure in a comprehensive and coordinated manner, the Central Government has taken steps which, inter-alia, include the following:

i.   The Ministry of Home Affairs has set up the 'Indian Cyber Crime Coordination Centre (I4C)' to deal with all types of cyber crime in the country, in a coordinated and comprehensive manner.

ii. The state of the art National Cyber Forensic Laboratory has been established, as a part of the I4C, at New Delhi to provide early stage cyber forensic assistance to Investigating Officers (IOs) of State/UT Police.

iii. The Massive Open Online Courses (MOOC) platform, namely 'CyTrain' portal has been developed under the Indian Cyber Crime Coordination Centre (I4C), for capacity building of police officers/judicial officers through online course on critical aspects of cyber crime investigation, forensics, prosecution etc. along with certification. More than 31,000 Police Officers from States/UTs are registered and more than 8,300 Certificates issued through the portal.

iv. The National Cyber Crime Reporting Portal (www.cybercrime.gov.in) has been launched, as a part of the I4C, to enable public to report incidents pertaining to all types of cyber crimes, with special focus on cyber crimes against women and children. Cyber crime incidents reported on this portal, their conversion into FIRs and subsequent action thereon are handled by the State/UT Law Enforcement Agencies (LEAs) concerned as per the provisions of the law.

v. The Citizen Financial Cyber Fraud Reporting and Management System, under I4C, has been launched for immediate reporting of financial frauds and to stop siphoning off funds by the fraudsters. So far, financial fraud transactions amounting to more than Rs. 265 Crore have been saved. A toll-free Helpline number '1930' has been operationalized to get assistance in lodging online cyber complaints.

vi. Seven Joint Cyber Coordination Teams have been constituted under I4C covering the whole country based upon cyber crime hotspots/ areas having multi jurisdictional issues by on boarding States/UTs to enhance the coordination framework among the LEAs of the States/UTs.

vii. To spread awareness on cyber crime, the Central Government has taken steps which, inter-alia, include; dissemination of messages through SMS, I4C social media account i.e. Twitter handle (@Cyberdost), Facebook(CyberDostI4C), Instagram(cyberdosti4c), Telegram(cyberdosti4c), Radio campaign, engaged MyGov for publicity in multiple mediums, organizing Cyber Safety and Security Awareness

weeks in association with States/UTs, publishing of Handbook for Adolescents/Students, etc. The States/UTs have also been requested to carry out publicity to create mass awareness.

viii. National Critical Information Infrastructure Protection Centre (NCIIPC) has been notified as the national nodal agency in respect of Critical Information Infrastructure Protection vide Gazette notification no. G.S.R. 18(E) dated 16 Jan 2014. NCIIPC provides threat intelligence, situational awareness, alerts & advisories and information on vulnerabilities to organizations having Critical Information Infrastructures (CIIs)/ Protected Systems (PSs) for taking preventive measures from cyber-attacks and cyber terrorism. Further, it follows up with concerned organizations for compliance of the IT (Information Security Practices & Procedures for Protected Systems) Rules, 2018 notified by Ministry of Electronics & Information Technology vide Gazette notification no. S.O. 2235(E) dated 22nd May 2018 to improve their cyber security posture. It also organises training/awareness sessions for employees of entities having CIIs/PSs.

ix. The Indian Computer Emergency Response Team (CERT-In) is designated as the national agency for responding to cyber security incidents. CERT-In operates an automated cyber threat exchange platform for proactively collecting, analysing and sharing tailored alerts with organisations across sectors for proactive threat mitigation actions by them.

x.   CERT-In has set up the National Cyber Coordination Centre to generate situational awareness regarding existing and potential cyber security threats.

xi.   CERT-In has empanelled 150 security auditing organisations to support and audit implementation of Information Security Best Practices.

xii.   A Cyber Crisis Management Plan formulated by CERT-In for implementation by all Ministries and Departments of the Central / State Governments and their organisations and critical sectors help to counter cyber-attacks and cyber-terrorism.

xiii.   Government websites and applications are audited with respect to cyber security and compliance with the Government of India Guidelines for Websites prior to their hosting. The auditing of the websites and applications is conducted on a regular basis after hosting also.

xiv.   CERT-In operates the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) to detect malicious programs and provides free tools to remove the same, and also provides cyber security tips and best practices for citizens and organisations.

(e):   As per the data published by the NCRB, crime head-wise details of cases registered in districts of Kerala state under cyber crimes (involving communication devices as medium/target) for year 2021 is at the Annexure-II.

*****

Crime Heads-wise Cases Registered (CR), Cases Chargesheeted (CCS), Cases Convicted (CON), Persons Arrested (PAR), Persons Chargesheeted (PCS) and Persons Convicted (PCV) under Cyber Crimes during 2019-2021

SL	Crime Heads	2019						2020						2021					
		CR	CCS	CON	PAR	PCS	PCV	CR	CCS	CON	PAR	PCS	PCV	CR	CCS	CON	PAR	PCS	PCV
1	Tampering computer source documents	173	42	2	60	62	8	338	76	20	153	134	23	55	51	0	106	72	0
2	Computer Related Offences	23734	3691	161	5174	5586	188	21926	6435	508	6499	7726	568	19915	10256	211	9577	12852	295
3	Cyber Terrorism	12	3	0	17	11	0	26	4	0	20	6	0	15	6	0	8	10	0
4	Publication/transmission of obscene / sexually explicit act in electronic form	4203	1567	86	2531	2111	106	6308	2343	66	3858	3170	82	6598	2811	123	4819	3547	139
5	Interception or Monitoring or decryption of Information	9	8	0	8	8	0	7	3	0	3	3	0	2	1	0	0	2	0
6	Un-authorized access/attempt to access to protected computer system	2	2	0	2	2	0	2	0	0	0	0	0	3	0	0	0	0	0
7	Abetment to Commit Offences	0	0	0	0	0	0	1	1	0	1	1	0	7	4	0	5	5	0
8	Attempt to Commit Offences	14	10	0	16	14	0	18	12	0	16	14	0	5	3	0	3	3	0
9	Other Sections of IT Act	2699	451	50	727	690	78	1017	320	37	509	431	48	827	386	19	671	536	35
A	Total Offences under I.T. Act	30846	5774	299	8535	8484	380	29643	9194	631	11059	11485	721	27427	13518	353	15189	17027	469
10	Abetment of Suicide (Online)	7	6	0	12	12	0	10	6	0	12	7	0	10	10	0	13	12	0
11	Cyber Stalking/Bullying of Women/Children	771	463	12	673	581	15	872	438	8	619	525	10	1176	702	15	870	830	16
12	Data theft	282	28	1	59	42	1	98	137	75	205	195	75	170	33	3	156	42	4
13	Fraud	6229	1119	18	2539	1980	40	10395	1688	221	2332	2268	246	14007	1815	30	3503	2988	73
14	Cheating	3367	535	10	1249	1292	14	4480	771	60	1277	1163	85	6343	842	27	3977	1707	30
15	Forgery	511	127	0	167	463	0	582	419	77	479	454	189	198	102	16	541	271	21
16	Defamation/Morphing	19	4	0	5	4	0	51	4	0	15	6	0	31	11	0	13	12	0
17	Fake Profile	85	35	0	45	43	0	149	43	2	65	65	2	123	39	1	47	43	1
18	Counterfeiting	5	5	0	8	8	0	9	2	0	10	4	0	2	1	0	1	1	0
19	Cyber Blackmailing/Threatening	362	109	2	296	145	2	303	121	6	203	153	6	689	238	2	1020	553	3
20	Fake News on Social Media	188	60	1	171	94	1	578	145	1	213	207	1	179	148	0	145	185	0
21	Other Offences	1974	883	23	1404	1204	31	2674	1123	9	1716	1501	14	2456	1198	36	1673	1624	39
B	Total Offences under IPC	13800	3374	67	6628	5868	104	20201	4897	459	7146	6548	628	25384	5139	130	11959	8268	187
22	Gambling Act (Online Gambling)	22	16	0	58	54	0	63	31	7	116	85	7	27	26	3	125	107	15
23	Lotteries Act (Online Lotteries)	9	1	0	11	1	0	26	12	11	14	12	11	4	5	0	0	15	0
24	Copy Right Act	34	10	0	8	11	0	49	24	0	44	36	0	32	28	0	40	38	0
25	Trade Marks Act	1	3	0	2	3	0	5	2	0	3	2	0	1	0	0	0	0	0
26	Other SLL Crimes	23	9	1	26	21	2	48	16	2	38	21	2	99	28	5	61	57	65
C	Total Offences under SLL	89	39	1	105	90	2	191	85	20	215	156	20	163	87	8	226	217	80
	Total Cyber Crimes	**44735**	**9187**	**367**	**15268**	**14442**	**486**	**50035**	**14176**	**1110**	**18420**	**18189**	**1369**	**52974**	**18744**	**491**	**27374**	**25512**	**736**

Source: Crime in India

Crime Heads-wise Cases Registered under Cyber Crimes in the Districts of Kerala during 2021

SL	Districts	Tampering computer source documents	Computer Related Offences Total	Cyber Terrorism	Publication/ transmision of obscene or sexually explicit act in electronic form	Interception or Monitoring or decryption of Information	Un-authorized access/ attempt to access protected system	Abetment to Commit Offences	Attempt to Commit Offences	Other Sections of IT Act	Total Offences under IT Act (A)	Abetment of Suicide (Online)	Cyber Stalking or Bullying of Women or Children	Data theft	Fraud
1	Alapuzha	0	3	0	8	0	0	0	0	0	11	0	0	0	0
2	Ernakulam Commr.	0	6	1	4	0	0	0	0	0	11	0	8	0	1
3	Ernakulam Rural	3	5	0	8	0	0	0	0	2	18	0	0	0	0
4	Idukki	0	5	0	6	0	0	0	0	1	12	0	0	0	0
5	Kannur City	0	13	0	10	0	0	0	0	2	25	0	0	0	0
6	Kasargod	0	0	0	0	0	0	0	0	5	5	1	1	0	2
7	Kollam Commr.	0	20	0	9	0	0	0	0	0	29	0	0	0	0
8	Kollam Rural	0	5	0	5	0	0	0	0	0	10	0	1	0	10
9	Kottayam	0	1	0	6	0	0	0	0	0	7	0	0	0	0
10	Kozhikode Commr.	0	5	0	3	0	0	0	0	0	8	0	6	0	2
11	Kozhikode Rural	0	3	0	10	0	0	0	0	0	13	0	0	0	0
12	Malappuram	1	2	0	50	0	0	0	0	6	59	0	3	0	0
13	Palakkad	0	1	0	29	0	0	0	0	0	30	0	0	0	0
14	Pathanamthitta	0	1	0	4	0	1	0	0	0	6	0	0	0	0
15	Railways	0	0	0	0	0	0	0	0	0	0	0	0	1	0
16	Thrissur Commr.	0	22	0	12	0	0	0	0	0	34	0	0	0	0
17	Thrissur Rural	0	2	0	15	0	0	0	0	0	17	0	0	0	0
18	Trivandrum Commr.	1	50	0	37	0	0	0	0	2	90	0	0	0	0
19	Trivandrum Rural	0	33	0	30	0	0	0	0	0	63	0	0	0	1
20	Wayanadu	1	0	0	4	0	0	0	0	1	6	0	0	0	0
21	Crime Branch	1	1	0	1	0	0	0	0	0	3	0	0	0	0
22	Kannur Rural	0	1	0	2	0	0	0	0	0	3	0	0	0	0
	Districts Total	**7**	**179**	**1**	**253**	**0**	**1**	**0**	**0**	**19**	**460**	**1**	**19**	**1**	**16**

Source: Crime in India

SL	Districts	Cheating	Forgery	Defamation/Morphing	Fake Profile	Counterfeiting	Cyber Blackmailing or Threatening	Fake News on Social Media	Other Offences	Total Offences under IPC (B)	Gambling Act (Online Gambling)	Lotteries Act (Online Lotteries)	Copy Right Act	Trade Marks Act	Other SLL Crimes	Total Offences under SLL (C)	Total Cyber Crimes (A+B+C)
1	Alapuzha	2	0	0	0	0	0	0	0	2	0	0	0	0	0	0	13
2	Ernakulam Commr.	12	1	0	0	0	2	0	26	50	0	0	1	0	0	1	62
3	Ernakulam Rural	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	18
4	Idukki	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	12
5	Kannur City	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	25
6	Kasargod	22	0	0	0	0	0	0	0	26	0	0	0	0	0	0	31
7	Kollam Commr.	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	29
8	Kollam Rural	0	0	0	0	0	0	0	7	18	0	0	0	0	1	1	29
9	Kottayam	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	7
10	Kozhikode Commr.	8	2	0	0	0	1	0	8	27	0	0	0	0	2	2	37
11	Kozhikode Rural	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	13
12	Malappuram	1	0	0	0	0	0	0	5	9	0	0	0	0	0	0	68
13	Palakkad	6	0	0	0	0	0	0	0	6	0	0	0	0	0	0	36
14	Pathanamthitta	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6
15	Railways	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1
16	Thrissur Commr.	10	0	0	0	0	7	0	0	17	0	0	0	0	0	0	51
17	Thrissur Rural	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	18
18	Trivandrum Commr.	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	91
19	Trivandrum Rural	0	0	0	0	0	0	0	3	4	0	0	0	0	0	0	67
20	Wayanadu	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6
21	Crime Branch	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3
22	Kannur Rural	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3
	Districts Total	**61**	**3**	**0**	**0**	**0**	**10**	**0**	**50**	**161**	**0**	**0**	**2**	**0**	**3**	**5**	**626**

Source: Crime in India