GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION. NO. 4576
TO BE ANSWERED ON: 30.03.2022

CYBER COMPLAINTS

4576. SHRI KALYAN BANERJEE:

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

(a) whether the Government is aware of the complaints related to the use of the internet cyber mechanism for software attacks, theft of intellectual property, identity theft, theft of software equipment or information, sabotage, operational implementation and information extortion which has surged to very alarming situation;

(b) if so, the details thereof; year-wise since 2017 including the main five cyber complaints registered in India; and

(c) the details of the action taken to prevent all such electronic frauds and data breaches including the banking system with effective address of the cyber threats and securing electronic devices from malicious attacks thereof?

ANSWER

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

(a):Government is fully cognizant and aware of increasing number of various cyber security threats. With the borderless cyberspace coupled with the anonymity, along with rapid growth of Internet, rise in cyber security incidents is a global phenomenon.

(b): Indian Computer Emergency Response Team (CERT-In) is mandated to track and monitor cyber security incidents in India. As per CERT-In, a total number of 552, 454, 472, 280 and 523 phishing incidents were observed during the year 2017, 2018, 2019, 2020 and 2021 respectively. Further, a total number of 56, 30, 43, 54 and 132 ransomware incidents were observed during the year 2017, 2018, 2019, 2020 and 2021 respectively.

As per the data maintained by National Crime Records Bureau (NCRB), Ministry of Home Affairs, a total of 21796, 27248, 44735, 50035 cybercrime cases were registered during the years 2017, 2018, 2019 and 2020 respectively. Cyber Crime head wise data for year 2017 to 2020, as provided by NCRB is at annexure I

(c): “Police” and “Public Order” are State subjects as per the Constitution of India. The Law Enforcement Agencies (LEAs) take legal action as per provisions of law against the cyber-crime offenders.

Government of India has taken a number of legal, technical and administrative measures to effectively address the cyber threats which, inter alia, include:

(i) Enactment of the Information Technology Act, 2000 which has provisions to deal with prevalent cybercrimes.
(ii) The 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 68 advisories for organisations and users for data security and mitigating fraudulent activities.

(iii) CERT-In notifies the affected organizations along with remedial actions to be taken on observing the data breach/leakage and ransomware incidents.

(iv) Government has issued guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing 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 96 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. 64 such drills have so far been conducted by CERT-In where 820 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. 15 and 19 training programs were conducted covering 708 and 5169 participants during the year 2020 and 2021 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.

(xi) CERT-In provides the requisite leadership for the Computer Security Incident Response Team-Finance Sector (CSIRT-Fin) operations under its umbrella for responding to, containment and mitigation of cyber security incidents reported from the financial sector.

(xii) 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.

(xiii) 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”.

(xiv) National Cyber Crime Reporting Portal, www.cybercrime.gov.in launched by Ministry of Home Affairs (MHA) enables citizens to online report complaints pertaining to all types of cybercrimes with special focus on cyber crimes against women and children. Complaints reported on this portal are attended by the respective Law Enforcement Authorities of States.

(xv) To spread awareness on cybercrime, MHA has taken several steps that include dissemination of messages on cybercrime through Twitter handle @cyberDost, radio campaign, Handbook for Adolescents / Students, Information Security Best practices for the benefit of Govt. Officials/ Officers, cyber Safety and Security Awareness weeks, in association with police department in different States/UTs etc., alerts/advisories on cyber-crimes, capacity building/training of law enforcement personnel/ prosecutors/ judicial officers, improving cyber forensics facilities etc.

(xvi) Reserve Bank of India (RBI) has issued various instructions in respect of security and risk mitigation measures related to electronic/digital transactions which includes Securing Card Transactions, Securing Payments through Internet Banking / Electronic Payments, ATM Transactions, Prepaid Payment Instruments (PPIs), Limiting Customer Liability on Unauthorized Electronic Banking Transactions, Limiting Customer Liability in Unauthorized Electronic Banking Transactions in PPIs issued by Authorised Non-banks, Enhancing Security of Card Transactions etc.

Annexure I

Crime Head-wise Cases Registered under Cyber Crimes during 2017-2020

SL	Crime Head	2017	2018	2019	2020
1	Tampering computer source documents	233	257	173	338
2	Computer Related Offences	10108	14141	23734	21926
3	Cyber Terrorism	13	21	12	26
4	Publication/transmission of obscene / sexually explicit act in electronic form	1768	3076	4203	6308
5	Interception or Monitoring or decryption of Information	4	6	9	7
6	Un-authorized access/attempt to access to protected computer system	2	0	2	2
7	Abetment to Commit Offences	0	1	0	1
8	Attempt to Commit Offences	4	13	14	18
9	Other Sections of IT Act	1503	980	2699	1017
A	**Total Offences under I.T. Act**	**13635**	**18495**	**30846**	**29643**
10	Abetment of Suicide (Online)	0	7	7	10
11	Cyber Stalking/Bullying of Women/Children	542	739	771	872
12	Data theft	307	106	282	98
13	Fraud	3466	3353	6229	10395
14	Cheating	1896	2051	3367	4480
15	Forgery	99	260	511	582
16	Defamation/Morphing	12	18	19	51
17	Fake Profile	86	78	85	149
18	Counterfeiting	1	2	5	9
19	Cyber Blackmailing/Threatening	311	223	362	303
20	Fake News on Social Media	170	97	188	578
21	Other Offences	1086	1713	1974	2674
B	**Total Offences under IPC**	**7976**	**8647**	**13800**	**20201**
22	Gambling Act (Online Gambling)	45	20	22	63
23	Lotteries Act (Online Lotteries)	11	2	9	26
24	Copy Right Act	89	62	34	49
25	Trade Marks Act	11	0	1	5
26	Other SLL Crimes	29	22	23	48
C	**Total Offences under SLL**	**185**	**106**	**89**	**191**
	Total Cyber Crimes (A+B+C)	**21796**	**27248**	**44735**	**50035**