GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 182
TO BE ANSWERED ON: 7.12.2022

CYBER FRAUDS

182. DR. MANOJ RAJORIA: SHRIMATI RANJEETA KOLI:
SHRI BALAK NATH: SHRI SUMEDHANAND SARASWATI:

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

(a) whether the Government has received a number of complaints related to cyber frauds during the last two years and if so, the details thereof;
(b) whether the Government is aware that these cyber criminals are far from being caught due to lack of technocrats at present and if so, the details thereof alongwith the number of such criminals punished so far;
(c) the efforts being made by the Government to effectively check the increasing cases of cyber fraud including the punishment for such criminals; and
(d) whether the Government is also initiating any awareness campaign to prevent cyber frauds, if so, the details thereof and if not, the reasons therefor?

ANSWER

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

(a) and (b):The policies of the Government are aimed at ensuring an Open, Safe and Trusted and Accountable Internet for its users. With the expansion of the Internet and more and more Indians coming online, the number of Indians exposed to cyber frauds has also grown. The many challenges in securing cyberspace against cyber frauds also flow from its vastness and borderless nature. As per data reported by the National Crime Records Bureau, the number of complaints reported under the online financial fraud category of the National Cyber Crime Reporting Portal over the period from 1.1.2021 to 30.11.2022 is 8,84,863. Further, the Bureau has informed that as per data reported to it by States and Union territories, a total of 10,395 and 14,007 cases were registered under the category "Frauds for cybercrimes" during the years 2020 and 2021 respectively and, further, 2,332 and 3,503 persons respectively were arrested in relation to the said category in the said years.

The Information Technology Act, 2000 ("IT Act") penalises various offences relating to the cyberspace, including tampering with computer source documents (section 65), dishonestly or fraudulently accessing a computer resource without the permission of its owneror person in charge (section 66), identity theft (section 66C), cheating by impersonation (section 66D), etc. These offences are in addition to the penal provisions under the Indian Penal Code for various offences relating to fraud. Such offences are cognizable offences. As per the provisions of the Code of Criminal Procedure, 1973, prevention and investigation of cognizable offences is to be done by the police, and as per the Seventh Schedule to the Constitution, 'Police' is a State subject. As such, States are primarily responsible for the prevention, investigation etc. of such offences through the State police departments, which take preventive and penal action as per law.

Public has been enabled to report financial cyber fraud incidents through the National Cyber Crime Reporting Portal (cybercrime.gov.in), which is connected to police stations and helps them in investigating effectively and improving coordination across States, districts and police stations.

(c) and (d): Government has taken a number of measures to check cyber frauds and to create awareness to prevent the same. These include the following:
(i) The Indian Cyber Crime Coordination Centre (I4C) under the Ministry of Home Affairs has been designated as the nodal point in the fight against cybercrime. A toll-free number 1930 has been made operational for citizens to get assistance in lodging online complaints in their own language. To spread

awareness on cybercrime, the Ministry of Home Affairs has taken several steps that include dissemination of messages on cybercrime through the Twitter handle @cyberDost and radio campaigns.

(ii) The Indian Computer Emergency Response Team (CERT-In) has formulated a Cyber Crisis Management Plan for countering cyber-attacks and cyber terrorism for implementation by all Ministries and Departments of the Central Government, State Governments and their organisations and critical sectors.

(iii) CERT-In conducts regular training programmes for network and system administrators and the Chief Information Security Officers of Government and critical sector organisations regarding securing the information technology infrastructure and mitigating cyber-attacks. A total of 41 training programmes were conducted, covering 11,377 participants, during the years 2021 and 2022 (upto November).

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

(v) CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on an ongoing basis.

(i) Security tips have been published for users to secure their desktops and mobile phones and to prevent phishing attacks.

(ii) 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.

(iii) All authorised entities and banks issuing pre-paid payment instruments (wallets) in the country have been advised by CERT-In through the Reserve Bank of India to carry out special audit by empanelled auditors of CERT-In on priority basis and to take immediate steps to comply with the findings of the audit report and ensure implementation of security best practices.

(iv) Cyber security mock drills are being conducted to enable assessment of cyber security posture and preparedness of organisations in the Government and critical sectors. 74 such drills have so far been conducted by CERT-In, in which 990 organisations from different States and sectors participated.

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

(vi) 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.

(vii) CERT-In provides leadership for the Computer Security Incident Response Team-Finance Sector (CSIRT-Fin) operations under its umbrella for responding toand containing and mitigating cyber security incidents reported from the financial sector.

(viii) CERT-In, National Institute of Securities Markets and the Centre for Development of Advanced Computing (C-DAC) conducts a self-paced 60-hour certification Cyber Security Foundation Course for professionals in the financial sector.

(ix) CERT-In regularly disseminates information and shares 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 Safe Internet Day on 8.2.2022 and Cyber Security Awareness Month in October 2022 by posting security tips using posters and videos on social media platforms and websites. CERT-In, in association with C-DAC, conducted an 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.

(x) CERT-In and the Reserve Bank of India jointly carry out a cyber security awareness campaign on ‘beware and be aware of financial frauds’ through the Digital India Platform.

(xi) The Ministry of Electronics and Information Technology conducts programmes 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 such as www.infosecawareness.in and www.csk.gov.in.

****