GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 2487
TO BE ANSWERED ON: 15.03.2023

CASES OF CYBER FRAUD

2487. SHRIMATI APARAJITA SARANGI:

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

(a) the details of cyber attack cases received and the number of cases disposed of by the Government;
(b) the details of minimum and maximum days or time needed to solve such cases;
(c) whether the Government has taken any step for faster resolution and reduction in time and if so, the details thereof;
(d) the details of cases resolved which involved trans national nature of cyber attack; and
(e) whether the Government has initiated any scheme for awareness for cyber fraud and if so, the details thereof?

ANSWER

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

(a) to (c): As per the information reported to and tracked by the Indian Computer Emergency Response Team (CERT-In), a total of 14,02,809 and 13,91,457 cybersecurity incidents were reported for the years 2021 and 2022 respectively. CERT-In notifies the affected organisations along with remedial actions to be taken, and coordinates incident response measures with affected organisations, service providers, respective sector regulators and law enforcement agencies.

CERT-In has apprised that, depending upon the type and scale of cyber-attack and the assets affected, the containment of the cybersecurity incident, remedial measures and detailed analysis take one day to a few months.

CERT-In has further informed that it has taken measures to enable organisations to prevent and respond to cybersecurity incidents in a timely manner, by sending proactive threat intelligence alerts and conducting mock drills and training programmes.

(d): There have been attempts from time to time to launch cyber-attacks on Indian cyber space from systems within and outside the country. It has been observed that attackers are compromising computer systems located in different parts of the world and use masquerading techniques and hidden servers to hide the identity of actual systems from which the attacks are being launched.

CERT-In receives inputs from its situational awareness systems and threat intelligence sources about malware infections and vulnerabilities in networks of entities across sectors and issues alerts to the organisations and sectoral Computer Security Incident Response Teams (CSIRTs) concerned for remedial measures. Further, besides notifying the affected organisations along with remedial actions to be taken and coordinating incident response measures with them, the service providers, respective sector regulators and law enforcement agencies, in the case of transnational incidents, CERT-In also coordinates with international Computer Emergency Response Teams.

(e): A number of measures have been taken to raise awareness for safeguarding against incidents of cyber fraud. These include the following:

(i) The Ministry of Electronics and Information Technology is implementing the Information Security Education and Awareness (ISEA) Phase-II project to build capacities in the area of information security, train government personnel and create mass information security awareness for users. Under this, a large number of awareness workshops have been conducted across the country, school teachers trained as master trainers to reach out to crores of users in the indirect mode through Cyber Safety and Cyber Security Awareness Weeks organised in select cities in collaboration with State Cyber Cell / Police departments, mass awareness programmes broadcasted through Doordarshan / All India Radio, bimonthly newsletters published in print and digital mode, and multilingual awareness content in the form of handbooks, multimedia short videos, posters etc., which have been disseminated through print, electronic and social media and made available for download on the ISEA awareness portal (www.infosecawareness.in).

(ii) 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 Centre for Development of Advanced Computing, 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 the MyGov platform.

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

(iv) 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 an ongoing basis.

(v) CERT-In works in coordination with service providers, regulators and law enforcement agencies to track and disable phishing websites and facilitate investigation of fraudulent activities.

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

(vii) 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.

(viii) 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.

(ix) Cybersecurity mock drills are conducted to enable assessment of the cybersecurity 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.

(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 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.

(xii) 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 42 training programmes have been conducted, covering 11,486 participants, during the years 2021 and 2022.

(xiii) 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.

(xiv) CERT-In, through RBI, has advised all authorised entities and banks issuing pre-paid payment instruments (wallets) in the country to carry out special audit by CERT-In-empanelled auditors, close the non-compliances identified in the audit report and ensure implementation of security best practices.

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

****