GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 5512
TO BE ANSWERED ON: 05.04.2023

DATA PHISHING ACTIVITIES

5512. SHRI RAJU BISTA:

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

(a) whether the Government is aware of the hundreds of thousands of personal data mining and phishing activities being undertaken by the anti-social elements and if so, the details thereof;
(b) whether any action has been taken to tackle this problem;
(c) if so, the details thereof and if not, the reasons therefor;
(d) whether there is recourse for victims of phishing activities especially those who are less technically sound like elderly citizens and if so, the details thereof; and
(e) the list of resources that the citizens can use to prevent such phishing activities, Ministry-wise?

ANSWER

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

(a) to (e): The policies of the Government are aimed at ensuring an Open, Safe and Trusted and Accountable Internet for its users. Government is cognizant of growing threats to data security on account of activities such as unauthorised data-mining and phishing, and has taken a number of measures to safeguards against such threats, including the following:

(i) The Ministry of Home Affairs has set up the Indian Cyber Crime Coordination Centre (I4C) to deal with all types of cybercrime, including cybercrime against children, in a coordinated and comprehensive manner. A toll-free number 1930 has been made operational for citizens to get assistance in lodging online complaints in their own language. The Ministry of Home Affairs has also taken several steps to spread awareness on cybercrime, including through dissemination of messages on cybercrime through the Twitter handle @CyberDost and radio campaigns.
(ii) The Indian Computer Emergency Response Team (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.
(iii) CERT-In issues alerts and advisories on an ongoing basis regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks. It also publishes security tips for users to secure their desktops, mobile phones and prevent phishing attacks.
(iv) 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, including elderly citizens, about information security, which are disseminated through portals such as www.infosecawareness.in and www.csk.gov.in.
(v) CERT-In coordinates incident response measures with affected organisations, service providers, sector regulators concern and law enforcement agencies. It also notifies affected organisations of cyber incidents, along with remedial actions to be taken by them.

(vi) CERT-In operates an automated cyber-threat exchange platform for proactively collecting, analysing and sharing tailored alerts with organisations for proactive threat mitigation actions by them.

(vii) 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 organisations.

(viii) CERT-In has empanelled 150 security auditing organisations to support and audit implementation of information security best practices.

(ix) A Cyber Crisis Management Plan has been formulated by CERT-In for implementation by all Ministries and Departments of the Central Government and State Governments and their organisations and critical sectors, to help counter cyber-attacks and cyber-terrorism.

(x) CERT-In conducts regular training programmes for network and system administrators and Chief Information Security Officers of government organisations regarding securing information technology infrastructure and mitigating cyber-attacks. 42 training programmes, covering 11,486 participants, have been conducted during the years 2021 and 2022.

(xi) Government websites and applications are audited with respect to cybersecurity and compliance with the Guidelines for Indian Government Websites prior to their hosting. Such auditing is done after hosting as well.

(xii) Cybersecurity mock drills are conducted to enable assessment of cybersecurity posture and preparedness of organisations in the government and critical sectors. 74 such drills have been conducted by CERT-In, covering 990 organisations from different States and sectors.

(xiii) 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.

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

****