GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 644
TO BE ANSWERED ON: 06.12.2023

CYBER ATTACKS

644. SHRI MANOJ TIWARI:
DR. NISHIKANT DUBEY:
SHRI RAVNEET SINGH BITTU:

Will the Minister of Electronics and Information Technology be pleased to state:

(a) whether it is a fact that cyber attacks are an imminent threat to Digital Infrastructure of the country;
(b) if so, the details thereof along with the measures taken by the Government to prevent such cyber attacks to ensure data safety of the citizens;
(c) whether the Government is working in collaboration with other countries and international experts to strengthen the digital security of the country; and
(d) if so, the details thereof?

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. The Internet technology and Internet used to be seen as force for good, but in recent years, technology is also exploited for causing user harms and criminality. The number of Internet users in India are expected to increase from 88 crores today to 120 crore users by 2026.

Government is fully cognizant and aware of various cyber security threats and challenges and has taken various measures to prevent cyber-attacks to ensure data safety of the citizens.

MeitY notified Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules on 6th April 2023 after extensive consultation with stakeholders. These rules enforce greater due diligence by online gaming and social media intermediaries in respect of online games to ensure an Open, Safe & Trusted and Accountable Internet for Digital Nagriks. Apart from this, Government has taken following measures to prevent cyber-attacks:

(i) The Ministry of Electronics and Information Technology (MeitY) conducts programmes to generate information security awareness. Books, videos and online materials about information security are developed for general users, children and parents, and are disseminated through portals such as www.infosecawareness.in and www.csk.gov.in.

(ii) MeitY has issued Guidelines for Cybersecurity Audit that cover both comprehensive and limited audit on periodic basis by competent auditors with clear responsibilities for ensuring such audit regularly, inclusive of vulnerability assessment andpenetration testing.

(iii) 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.

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

(v) 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.

(vi) 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.

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

(viii) 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.

(ix) Cybersecurity mock drills are conducted to enable assessment of the cybersecurity posture and preparedness of organisations in the government and critical sectors. 86 such drills have so far been conducted by CERT-In, in which 1159 organisations from different States and sectors participated.

(x) CERT-In has empanelled 177 security auditing organisations to support and audit implementation of Information Security Best Practices.

(xi) 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 Safer Internet Day on 7.02.2023 and Cyber Security Awareness Month in October 2023, 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.

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

(xiii) 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. A total of 42 training programmes have been conducted, covering 11,486 participants, during the years 2021 and 2022. In 2023, up to October, a total of 7007 officials from Government, critical sectors, public and private sector have been trained in 21 training programs in the area of cyber security.

(xiv) National Informatics Centre (NIC) provides IT support to user ministries, departments and agencies of the Central Government, State Governments and district administrations for various e-governance solutions and, as part of this, helps maintain various government databases that contain data of citizens. NIC follows information security policies and practices in line with industry standards and practices, aimed at preventing cyber attacks and safeguarding data.

(xv) The Department of Telecommunications monitors and detects cyber-attacks and threats to Indian telecom networks, including those initiated from foreign countries, and provides timely alerts to stakeholders for necessary action.

(xvi) The National Critical Information Infrastructure Protection Centre has been setup for the protection of critical information infrastructure and responding to cyber incidents pertaining to such infrastructure. The Centre provides near-real-time threat intelligence and situational awareness, based on which regular alerts and tailored advisories are sent to the entities concerned with such infrastructure.

(xvii) The Indian Cyber Crime Coordination Centre (I4C) under the Ministry of Home Affairs is designated as the nodal point in the fight against cybercrime. A toll-free number 1930 is operational for citizens to get assistance in lodging online complaints in their own language. To spread awareness on cybercrime, the Ministry has taken several steps, which include dissemination of messages on cybercrime through the Twitter handle @cyberDost and radio campaigns.

(xviii) RBI has issued various instructions in respect of security and risk mitigation measures related to electronic/digital transactions. These cover securing of card transactions, securing payments through Internet banking / electronic payments, ATM transactions, pre-paid payment instruments (PPIs), limiting customer liability on unauthorised electronic banking transactions (including PPIs issued by authorised non-banks), safeguarding against email spoofing attacks, etc.

(c) and (d): The cyberspace is borderless and therefore collaboration and partnerships with other countries is must. The Government is committed to working with partners including Governments of other countries, private companies and start-ups to strengthen India’s cybersecurity posture and to ensure protection of all digital nagriks. The following actions have been taken to strengthen cooperation with stakeholders for dealing effectively with cybersecurity issues:

(i) CERT-In has entered into cooperation arrangements in the form of Memorandum of Understanding (MoU) with its overseas counterpart agencies for collaborating in the area of cyber security. At present such Memorandum of Understandings (MoU) have been signed with Bangladesh, Brazil, Egypt, Estonia, Japan, Maldives, Nigeria, Russian Federation, United Kingdom, Uzbekistan and Vietnam.

(ii) 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.

(iii) CERT-In is an operational member of Asia Pacific Computer Emergency Response Teams, a regional forum for Internet security in the Asia-Pacific region.

(iv) CERT-In is a member of Forum of Incident Response and Security Teams (FIRST), a global forum for cyber security teams.

(v) CERT-In is an accredited member of Task Force for Computer Security Incident Response Teams / Trusted Introducer. This signals to other parties that CERT-In has reached a certain level of maturity and functionality, which is valuable in building trust within the CERT community

****