GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
STARRED QUESTION NO. *112
TO BE ANSWERED ON: 16.12.2022

PREVENTION OF CYBER ATTACKS

***112. SHRI B. PARTHASARADHI REDDY**

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 of measures taken by Government to prevent such cyber attacks to ensure data safety of the citizens;

(c) whether Government is working in collaboration with other countries and with international experts to strengthen the digital security of the country; and

(d) if so, the details thereof?

ANSWER

MINISTER OF ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI ASHWINI VAISHNAW)

(a) to (d): A statement is laid on the Table of the House.

STATEMENT REFERRED TO IN THE REPLY TO RAJYA SABHA STARRED QUESTION NO. *112 FOR 16.12.2022
REGARDING PREVENTION OF CYBER ATTACKS
…..

(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 innovation of technology and rise in usage of cyber space and digital infrastructure for businesses and services, rise in cyber-attacks and cyber security incidents is a global phenomenon. Government is fully cognizant and aware of various cyber security threats, and has taken the following measures to prevent cyber-attacks to ensure data safety of the citizens:

(i) The Indian Computer Emergency Response Team (CERT-In) has been issuing alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on an ongoing basis.

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

(iii) 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.

(iv) 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.

(v) Cyber security mock drills are conducted to enable assessment of the 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.

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

(vii) 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.

(viii) 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.

(ix) 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.

(x) 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 have been conducted, covering 11,377 participants, during the years 2021 and 2022 (up to November).

(xi) The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, made by the Central Government in exercise of its powers under the Information Technology Act, 2000,

provide the security practices and procedures that a body corporate or any person collecting, receiving, possessing, storing, dealing or handling information on behalf of such body corporate is required to observe for protecting personal data of users.

(xii) To protect sensitive information, theNational Informatics Centre (NIC) adopts a layered security approach, in the form of practices, procedures and technologies put in place on the network and application levels. This is strengthened through periodic compliance, audit and vulnerability assessment.

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

(xiv) 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.

(xv) The Ministry of Electronics and Information Technology 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.

(xvi) 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 has taken several steps, which include dissemination of messages on cybercrime through the Twitter handle @cyberDost and radio campaigns.

(xvii) RBI organises Financial Literacy Week activities annually to propagate financial education messages among the public. The theme for the current year'sweek (February 2022) was "go digital, go secure", with a focus on creating awareness about convenience of digital transactions, security of digital transactions and protection of customers. Banks were advised to disseminate information and create awareness among their customers and the general public. Further, RBI ran a mass media campaign during February 2022 to disseminate essential financial awareness messages.

(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 cyber security posture and to ensure protection of all digital nagriks. The following actions have been taken to strengthen cooperation with stakeholders for dealing effectively with cyber security issues:

(i) CERT-In has entered into cooperation arrangements, in the form of Memorandum of Understanding, with overseas counterpart agencies for collaborating in the area of cyber security. At present, such Memoranda have been signed with Bangladesh, Brazil, France, Israel, Japan, Maldives, Nigeria, 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.

****