GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 2253
TO BE ANSWERED ON: 02.08.2023

INTERNET SECURITY

2253. SHRI MANOJ KOTAK:

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

(a) whether the Government is committed to ensure that Internet in the country is open, safe and trusted and accountable for its users;
(b) if so, the details thereof along with the action taken by the Government in this regard;
(c) whether the Indian Computer Emergency Response Team (CERT-In) is mandated to track and monitor cyber security incidents in the country; and
(d) if so, the details thereof including the number of cyber attacks on Government and fintech websites during the last four years?

ANSWER

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

(a) and (b): Government of India is committed to ensure that the Indian internet is Open, Safe &Trusted, and Accountable for all its users. The government is continuously engaged in formulating policies and setting technical standards in the cyberspace to holistically ensure accessible internet and to mitigate threats & vulnerabilities in the cyberspace.

The policies of the Government are aimed at ensuring an Open, Safe & Trusted, and Accountable Internet for all digital nagriks. Safety and Trust will in turn ensure digital safety of users. The Information Technology Act, 2000 ("IT Act") and rules made thereunder contain several provisions for safeguarding Digital Nagriks.

Further, the Central Government, in exercise of powers conferred by IT Act, has notified the new Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021("IT Rules, 2021"). These new rules cast specific obligation on intermediaries vis-à-vis what kind of information is to be hosted, displayed, uploaded, published, transmitted, stored or shared. Intermediaries are also required to remove any content violative of any law for the time being in force as and when brought to their knowledge either through a court order or through a notice by appropriate government or its authorised agency. In case of failure to follow diligence as provided in the IT Rules, 2021, by intermediaries, they shall lose their exemption from liability under section 79 of the IT Act and shall be liable for consequential action as provided in such law. Further, in case an intermediary is a significant social media intermediary (an intermediary having more than 50 lakh registered users in India), to additionally observe due diligence in terms of appointing, in India, a Grievance Officer, a Chief Compliance Officer and a nodal contact person for 24x7 coordination with law enforcement agencies. As per the IT Rules, 2021, the Chief Compliance Officer is responsible for ensuring compliance with the IT Act and the rules made thereunder.

Keeping in view complaints regarding action or inaction, on the part of the social media intermediaries and other intermediaries on user grievances regarding objectionable content or suspension of their accounts, the Central Government has also established three Grievance Appellate Committees (GACs), as provided for in the said IT Rules, 2021 to enable users to appeal against the decisions taken by Grievance Officer of intermediaries on user complaints.

Government through Indian Computer Emergency Response Team (CERT-In) has taken following measures to enhance the cyber security posture and prevent cyber attacks:

i. Issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers, networks and data on an ongoing basis.

ii. Issued guidelines on information security practices for government entities for Safe & Trusted Internet in June 2023 covering domains such as data security, network security, identity and access management, application security, third-party outsourcing, hardening procedures, security monitoring, incident management and security auditing.

iii. Operating 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.

iv. Government has formulated a Cyber Crisis Management Plan for countering cyber attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.

v. Empanelled 150 security auditing organisations to support and audit implementation of Information Security Best Practices.

vi. Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 80 such drills have so far been conducted by CERT-In where 1062 organizations from different States and sectors participated.

vii. Set up the National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats.

viii. 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.

ix. Provides leadership for the Computer Security Incident Response Team-Finance Sector (CSIRT-Fin) operations under its umbrella for responding to and containing and mitigating cyber security incidents reported from the financial sector.

x. 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 June, a total of 627 officials from Government, critical sectors, public and private sector have been trained in 6 training programs in the area of cyber security.

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

xii. 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 2022, by posting security tips using posters and videos on social media platforms and websites. 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.

xiii. 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.

xiv. Co-operates, works and coordinates incident response measures with international CERTs, overseas organisations and service providers as well as Law Enforcement Agencies.

National Internet Exchange of India (NIXI), a setup by Government has extended the Internet Exchange Points (IXPs) footprint beyond the metro cities to tier 2 and tier 3 cities helping the regional Internet Service Providers (ISPs) to have the same content and quality of services as being experienced by metro based ISPs. Internet Exchanges reduces latency, improves response time and potentially reduces cost to deliver Internet services & contents.

Government has introduced know your customer eKYC/KYC for .IN domain registration that will avoid unfair, unsocial, anti-India & terrorist agencies to use .IN domain in unlawful activities. .IN is India's top-level domain on the Internet. Government is also facilitated internationalized domain names - . भारत in all official languages of the country thereby enabling access to Internet to the non-English speaking users.

(c) and (d): The Indian Computer Emergency Response Team (CERT-In) is serving as national agency for responding to cyber security incidents as per provisions of Section 70B of Information Technology Act, 2000. 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 concerned organisations and sectoral Computer Security Incident Response Teams (CSIRTs) for remedial measures. CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers, networks and data on an ongoing basis. As per the information reported to and tracked by CERT-In, details of cyber security incidents are as follows:

Year	Cyber Security Incidents pertaining to Government Organisation	Website Hacking Incidents of Central Ministries/Departments and State Government organizations	Cyber Security Incidents Pertaining to Financial Institutions
2019	85797	54	6168
2020	54314	59	700548
2021	48285	42	862073
2022	192439	50	826978
2023(upto June)	112474	36	429847

****