GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 2807
TO BE ANSWERED ON: 24.03.2023

SAFETY OF DIGITAL DATA IN THE COUNTRY

2807. SHRI PARIMAL NATHWANI

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

(a) whether it is a fact that the digital data in the country is fully safe;
(b) the details of the defence mechanism to safeguard the digital data from the danger of being hacked, attacked and hijacked;
(c) whether Government or any institution, private or public, was ever made to pay huge sum in ransom to the hacker/attacker/hijacker of digital data in the last five years; and
(d) the extent the Aadhar data in the country is vulnerable and the special defence mechanism to protect that data.

ANSWER

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

(a) and (b): Government is committed to ensure that Internet in India is Open, Safe and Trusted and Accountable for its users. With emergence of new technology and rise in the usage of Internet, the growing risk to digital data in the cyberspace is a global phenomenon, and Government is fully cognizant of the same.

The following measures have been taken to strengthen the defence mechanism for safety of digital data:

(i) The Indian Computer Emergency Response Team (CERT-In) coordinates incident response measures with affected organisations, service providers, respective sector regulators and law enforcement agencies, and notifies the affected organisations regarding cyber incidents, along with remedial actions to be taken.

(ii) CERT-In issues alerts and advisories on an ongoing basis regarding the latest cyber-threats/vulnerabilities and countermeasures to protect computers and networks.

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

(iv) 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.

(v) CERT-In regularly conducts training programmes for network and system administrators and 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 were conducted, covering 11,486 participants, during the years 2021 and 2022.

(vi) Government websites and applications are audited with respect to cybersecurity and compliance with the Government of India Guidelines for Websites, prior to hosting.

(vii) CERT-In has empanelled 150 security auditing organisations to support and audit implementation of Information Security Best Practices.

(viii) 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 cybersecurity tips and best practices for citizens and organisations.

(ix) Cybersecurity mock drills are being conducted to enable assessment of 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 various States and sectors participated.

(x) Security tips are published for users to secure desktops and mobile phones and to prevent phishing attacks.

(xi) CERT-In regularly disseminates information and shares security tips on cybersafety and cybersecurity through social media handles and websites. It organised various events and activities for citizens during the Safe Internet Day on 8.2.2022 and the 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 the Centre of 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 MyGov platform.

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

(xiii) 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 about information security, which are disseminated through portals such as www.infosecawareness.in and www.csk.gov.in.

(c): CERT-In has apprised that it is not in receipt of any report regarding any such payment.

(d): The Unique Identification Authority of India (UIDAI) has deployed extensive security defense mechanisms and safeguards to protects its digital data, as under:

(i) Amulti-layered security infrastructure is in place to protect the Central Identities Data Repository (CIDR) database of the Authority. It is protected through strong data encryption, sharding to prevent data leak, IP address obfuscation, web application firewalls, database activity monitoring tools, sophisticated security management devices, encrypted connectivity with agencies in the Aadhaar ecosystem, a demilitarised zone for external access to applications.

(ii) A security operation centre continuously assesses and monitors CIDR for security risks, threats and cyber-attack indicators.

(iii) The CIDR is notified as a “protected system” and complies with the security requirements and advisories issued by the National Critical Information Infrastructure Protection Centre. Its infrastructure is certified by STQC as compliant with the security requirements and controls prescribed by the ISO/IEC 27001 international standard.

(iv) An independent auditing agency performs periodic cyber security audits and risk assessments, besides external information security audits undertaken previously by various other agencies concerned with cybersecurity matters.

******