GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 2298
TO BE ANSWERED ON: 19.12.2025

CYBERSECURITY IN BANKING SECTOR

2298. SHRI MASTHAN RAO YADAV BEEDHA:

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

(a) whether cyberattacks are increasingly targeting the banking sector in India;
(b) if so, the details of such cyberattacks reported so far; and
(c) the measures taken or proposed by Government to strengthen cybersecurity in the banking sector?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI JITIN PRASADA)

(a) to (c): The policies of the Government of India aim to ensure a safe, trusted, & accountable cyberspace. It remains vigilant & fully conscious of the cyber threat to India's digital infrastructure. Banking sector forms an integral part of the government's strategy.

The Indian Computer Emergency Response Team (CERT-In) is designated as the national agency for responding to cyber security incidents under the provisions of section 70B of the Information Technology Act, 2000.

Banking and financial services also form part of the Critical Information Infrastructure (CII) National Critical Information Infrastructure Protection Centre (NCIIPC), designated under Section 70A of the Information Technology Act, 2000, plays a key role in protecting such critical systems.

NCIIPC works closely with CERT-In, RBI, CERT-Fin and banking institutions to protect systems critical to the banking sector. It regularly conducts the risk assessment, issuance of sector-specific advisories and implementation of protective measures.

Computer Security Incident Response Team - Finance (CSIRT-Fin) regularly responds to the cyber security incidents reported from the financial sector under the umbrella and guidance of CERT-In.

Reserve Bank of India (RBI) has issued a comprehensive circular on the Cyber Security Framework for banks, which sets standards and guidelines for implementing robust cyber security controls.

Several other initiatives to strengthen cyber security in the country, including the banking sector as follows:

1. National Cyber Coordination Centre (NCCC), implemented by CERT-In, examines the cyberspace to detect cyber security threats. It shares the information with concerned organizations, state governments and stakeholder agencies for taking action.

2. Cyber Swachhta Kendra (CSK)
   - A citizen-centric service provided by CERT-In, which extends the vision of Swachh Bharat to the Cyber Space.
   - It is the Botnet Cleaning and Malware Analysis Centre and helps to detect malicious programs and provides free tools to remove the same.
   - It also provides cyber security tips and best practices for citizens and organisations.
3. CERT-In has empanelled 231 security auditing organisations to support and audit implementation of Information Security Best Practices.
4. Cyber Crisis Management Plan formulated by CERT-In for countering cyber-attacks and cyber terrorism for implementation by all Ministries/Departments.
5. Cyber security mock drills by CERT-In for assessment of cyber security posture and preparedness of organisations in Government and critical sectors including banking sector.
6. Advisory by CERT-In to all authorised entities/banks issuing Prepaid Payment Instruments (PPI) in the country to carry out special audit by empanelled auditors of CERT-In on a priority basis.
   a. Immediate steps are taken to ensure compliance with the findings and ensure implementation of security best practices.
7. RBI's Public awareness campaign called 'RBI Kehta Hai' informs people about digital payment options and how to use them safely, securely, and conveniently.

*****