GOVERNMENT OF INDIA
MINISTRY OF FINANCE
DEPARTMENT OF FINANCIAL SERVICES

RAJYA SABHA
UNSTARRED QUESTION NO 404

ANSWERED ON TUESDAY, 3 FEBRUARY, 2026/ 14 MAGHA, 1947 (SAKA)

CYBER SECURITY IN DIGITAL PAYMENT SYSTEMS

404 SHRI SANJAY SETH:

Will the Minister of Finance be pleased to state:

(a) the manner in which robust collaboration with private stakeholders is ensured to enhance cybersecurity measures in digital payment systems;
(b) the specific frameworks being developed to address cyber threats targeting rural digital financial infrastructure;
(c) why Government has prioritized certain payment platforms for cybersecurity audits over others;
(d) the measures in place to educate users about safe digital payment practices and build public trust in fintech systems; and
(e) the manner in which the Ministry is planning to strengthen the capacity of financial institutions to detect and respond to emerging digital payment frauds?

ANSWER

THE MINISTER OF STATE IN THE MINISTRY OF FINANCE

(SHRI PANKAJ CHAUDHARY)

(a): The Government has been proactively engaging with different stakeholders to review the changing threat landscape, mitigation measures, and creating awareness among the common citizens. The engagement inter alia, include holding periodic review meetings, organising workshops, conducting awareness camps and undertaking various awareness activities through print and social media.

(b): Reserve Bank of India(RBI) has issued Master Directions on Digital Payment Security Controls in February, 2021 to combat web and mobile app threats. These guidelines mandate the banks to implement a common minimum standards of security controls for various payment channels like internet, mobile banking, card payment etc. RBI has also launched an Artificial Intelligence (AI) based tool ‘MuleHunter’ for identification of money mule and advised the banks and financial institutions for its uses. Further, in order to prevent frauds related to UPI transaction, the National Payments Corporation of India(NPCI) has provided an AI / Machine Learning (ML) based fraud monitoring solution to all the banks to generate alerts and decline suspicious transactions.

(c) In order to ensure the best security practices, all the supervised entities including the banks, payment system operators, and pre-paid payment instruments have been advised to conduct special audit through Indian Computer Emergency Response Team (CERT-In) empanelled auditors and to take necessary steps to comply with the findings of such audit reports.

(d) & (e) : RBI and Banks have been taking up awareness campaigns through short SMS, radio campaign, publicity on prevention of ‘cyber-crime’. Further, RBI has been conducting electronic-banking awareness and training (e-BAAT) programmes which focuses on awareness about frauds and risk mitigation.

CERT-In is regularly sharing safety and security tips, awareness posters, info-graphics, booklets and videos through its official websites and social media handles for sensitizing internet users on cyber security threats and prevention measures.

CERT-In conducts Cyber security mock drills regularly to enable assessment of cyber security posture and preparedness of organisations in the critical sectors including banking sector. Further, it also conducts joint cyber security training programs in collaboration with industry partners to upskill the cyber security workforce in Government, public and private organizations.

******