GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS

LOK SABHA
UNSTARRED QUESTION NO. 5124

TO BE ANSWERED ON THE 24TH MARCH, 2026/ CHAITRA 3, 1948 (SAKA)

CYBER SECURE BHARAT

5124. SHRI NAVEEN JINDAL:

Will the Minister of HOME AFFAIRS be pleased to state:

(a) whether the Government has formulated any framework against illegal payment gateways created using mule bank accounts by Transnational Organized Cyber criminals, facilitating money laundering as a service, if so, the details thereof; and

(b) the preventive steps taken being taken by the Government to create a 'Cyber Secure Bharat'?

ANSWER

MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS
(SHRI BANDI SANJAY KUMAR)

(a) & (b): Reserve Bank of India (RBI) reviews the cyber security developments and threats on an ongoing basis in order to strengthen security of digital transactions and necessary measures are taken to strengthen the cyber resilience of banks.

RBI has advised the banks to establish robust procedures and processes to imbibe "security by design" principle in development of mobile banking applications including UPI applications, with appropriate testing mechanism through confidential circulars/advisories/alerts/caution advice.

RBI has taken various measures to address the issue of cyber-enabled frauds and suspected mule accounts which, inter-alia, includes close monitoring of any misuse of the banking channels for proliferation of the cyber-enabled frauds; issuance of various Confidential Advisories delineating specific actions to be taken by the banks in mitigating the misuse of banking channel through robust systems; focused thematic assessments in major banks with high-number of money mule accounts; regular outreach programmes through seminars / workshops conducted, etc. Further, the banks have been advised to ensure deployment and adoption of robust software for real-time transaction monitoring and use of Artificial Intelligence/Machine Learning tools in detecting suspicious and fraudulent transaction patterns as well as use of network analytics in identifying mule networks.

The Ministry of Home Affairs has set up the 'Indian Cyber Crime Coordination Centre' (I4C) as an attached office to deal with all types of cyber crimes in the country, in a coordinated and comprehensive manner. The 'National Cyber Crime Reporting Portal' (NCRP) (https://cybercrime.gov.in) has been launched. A toll-free Helpline number '1930' has been operationalized to get assistance in lodging online cyber complaints.

The 'Citizen Financial Cyber Fraud Reporting and Management System' (CFCFRMS), under I4C, has been launched in year 2021 for immediate reporting of financial frauds and to stop siphoning off funds by the fraudsters. Till 31.01.2026, financial amount of more than Rs. 8,690 Crore has been saved in more than 24.65 lakh complaints.

A State of the Art, Cyber Fraud Mitigation Centre (CFMC) has been established at I4C where representatives of major banks, Financial Intermediaries, Payment Aggregators, Telecom Service Providers, IT Intermediaries and representatives of States/UTs Law Enforcement Agency are working together for immediate action and seamless cooperation to tackle cybercrime.

A Suspect Registry of identifiers of cyber criminals has been launched by I4C on 10.09.2024 in collaboration with Banks/Financial Institutions. Till 31.01.2026, more than 23.05 lakh suspect identifier data received from Banks and 27.37 lakh Layer 1 mule accounts have been shared with the participating entities of Suspect Registry and declined transactions worth Rs. 9518.91 crores.

The Ministry of Home Affairs has formed CyMAC (Cyber Multi Agency Centre) under the MAC (Multi Agency Centre) platform on 22.01.2025 with

the objective to effectively address cybersecurity threats, cyber espionage, misuse of emerging technologies and similar concerns against national security.

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. CERT-In has taken following measures to provide assistance to all States and UTs for enhancing cyber security and prevent cyber attacks:

i. **CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers, networks and data on an ongoing basis.**
ii. **National Cyber Coordination Centre (NCCC) implemented by CERT-In, examines the cyberspace to detect cyber security threats. It shares the information with concerned State Governments, organisations across sectors, and stakeholder agencies for taking action.**
iii. **CERT-In operates an automated cyber threat exchange platform for proactively collecting, analysing and sharing tailored alerts with State Governments and organisations across sectors for proactive threat mitigation actions by them.**

iv. Cyber Swachhta Kendra (CSK) is a service provided by CERT-In, which extends the vision of Swachh Bharat to the cyber space. Cyber Swachhta Kendra helps to detect malicious programs and vulnerable services and provide remedial measures to organisations across States and sectors.

v. CERT-In has empanelled 237 security auditing organisations to support and audit implementation of Information Security Best Practices.

vi. Cyber security mock drills are conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government (Central & States) and critical sectors. Workshops along with these drills are conducted in States for facilitating coordination and information sharing in the area of cyber security.

vii. CERT-In has launched a specific cybersecurity program "Cyber Bharat Setu" which focuses on promoting cybersecurity culture in States/UTs. Madhya Pradesh, Tripura, Uttarakhand and Jammu & Kashmir Administration participated in this program in 2025.

viii. CERT-In conducts joint cyber security training programs in collaboration with Industry partners to upskill the cyber security workforce in Government (Central & States), public and private organizations across sectors.

*****