GOVERNMENT OF INDIA
MINISTRY OF EARTH SCIENCES
LOK SABHA
UNSTARRED QUESTION NO. 5174
TO BE ANSWERED ON WEDNESDAY, 2ND APRIL, 2025

CYBER FRAUD IN INCOIS

5174. SHRI SASIKANTH SENTHIL:

Will the Minister of EARTH SCIENCES be pleased to state:

(a) whether there are recent incidents of cyber fraud, particularly at the Indian National Centre for Ocean Information Services (INCOIS) and if so, the details thereof along with the financial losses incurred due to these fraudulent activities;
(b) the steps taken by the Government to strengthen the cybersecurity measures within its agencies especially at INCOIS to prevent further incidents of cyber fraud and safeguard sensitive financial data;
(c) whether the Government has conducted any internal audits or reviews to assess the vulnerabilities in the current cybersecurity infrastructure of INCOIS and other related institutions and if so, the details thereof; and
(d) the details of collaborative efforts undertaken by the Government with cybersecurity experts or agencies to enhance the security of financial transactions and protect public funds from cyber threats and the specific actions being taken to train employees on identifying and preventing such fraud?

ANSWER
THE MINISTER OF STATE (INDEPENDENT CHARGE) FOR
MINISTRY OF SCIENCES AND TECHNOLOGY
AND EARTH SCIENCES
(DR. JITENDRA SINGH)

(a) Yes Sir. There were two incidents of cyber fraud at the Indian National Centre for Ocean Information Services (INCOIS), Hyderabad. A man-in-the-middle (MITM) attack on 29th June 2024 and on 15thJuly, 2024, with the financial losses to the extent of Euro 44,946 and USD 1,98,943.65 respectively.

However, USD 1,98,943.65 was completely recovered after continuous follow-up with all the stake holders and credited back to INCOIS on 07th October 2024. With respect to the incident of Euro 44,946, efforts were initiated for recovery of the funds in co-ordination with Cyber Crime Police, Bankers at India & abroad as well as the Embassy of India at Portugal.

(b) Measures taken to strengthen the cyber security system at INCOIS are as follows:

- Securing access to INCOIS emails/ systems to authorized personnel using Virtual Private Network (VPN).
- Strengthening the email/system access by two factor authentication (2FA), complex passwords, periodic change of passwords, etc.

- Filtering of SPAM.
- Sensitizing staff on cyber security aspects for prevention of cyber frauds.
- Migrating email services to NIC.

(c) Yes sir. INCOIS conducted an internal review of the cyber security infrastructure and implemented the above-mentioned measures.

(d) In order to enhance the security of financial transactions, INCOIS has

- Established issuance of Usance Letters of Credit (ULC) for foreign orders.
- Conducting training of staff on cyber security aspects in co-ordination with Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics and Information Technology empanelled agencies.

In addition, Government has taken following measures to strengthen India's cyber security framework and prevent cyber fraud including curbing financial cyber crimes, which inter-alia, includes:

i. The MHA has established the Indian Cyber Crime Coordination Centre (I4C) as an attached office to provide a framework and eco-system for LEAs to deal with cyber crimes in a comprehensive and coordinated manner.

ii. 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 working together for immediate action and seamless cooperation to tackle cybercrime. By bringing together financial institutions, CFMC aims to detect, prevent and mitigate the cyber financial frauds by preventing the dissemination of fraudulent funds across various financial sectors.

iii. Reserve Bank of India (RBI) has issued Master Directions on Fraud Risk Management for the Regulated Entities viz. (i) Commercial Banks (including Regional Rural Banks) and All India Financial Institutions; (ii) Cooperative Banks (Urban Cooperative Banks / State Cooperative Banks / Central Cooperative Banks); and (iii) Non-Banking Finance Companies (including Housing Finance Companies) on 15.07.2024 for strengthening of framework on Early Warning Signals (EWS), inter alia, to monitor transactions / unusual activities in the non-KYC compliant and money mule accounts etc., to contain unauthorized / fraudulent transactions.

iv. RBI through "RBI Kehta Hai" has issued awareness material / useful information on aspects such as different types of frauds, modus-operandi and measures to be taken during digital payment transactions and also through advertising (through prominent personalities) for creating awareness amongst public, etc. RBI has also issued the booklet "BE (A)WARE‟ on modus operandi of financial frauds in the public domain to educate the public.

v. National Cyber Security Coordinator (NCSC) under the National Security Council Secretariat (NSCS) to ensure coordination amongst different agencies.

vi. National Cyber Coordination Centre (NCCC) implemented by the CERT-In serves as the control room to scan the cyberspace in the country and detect cyber security threats. NCCC facilitates coordination among different agencies by sharing with them the metadata from cyberspace for taking actions to mitigate cybersecurity threats.

vii. Cyber Swachhta Kendra (CSK) is a citizen-centric service provided by CERT-In, which extends the vision of Swachh Bharat to the Cyber Space. Cyber Swachhta Kendra 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.

viii. CERT-In issued Cyber Security Directions in April 2022 under sub-section (6) of section 70B of Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet.

ix. CERT-In issued guidelines on information security practices for government entities 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.

x. CERT-In has issued an advisory to various Ministries in November 2023 outlining the measures to be taken for strengthening the cybersecurity by all entities that are processing the digital personal data or information including sensitive personal data or information. CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and counter measures to protect computers, mobile phones, networks and data on an ongoing basis.

xi. NIC has deployed advanced security tools including Threat Intelligence Platform to identify the security issues associated with Government network.

*****