Indians Lose ₹1,000 Crore Monthly to Southeast Asia Cyber Frauds: Key Scam Types Explained

July 15, 2025 • vajiramandravi.com

Southeast Asia Cyber Scams India Latest News

- The Ministry of Home Affairs (MHA) estimates that over half of the ₹7,000 crore lost to cyber scams in India from January to May 2025 originated from Southeast Asia.
- Countries like Myanmar, Cambodia, Vietnam, Laos, and Thailand are key sources, with scams often operated from high-security centres controlled by Chinese networks.
- These centres reportedly use trafficked individuals, including Indians, as forced labour in running these fraud operations, according to the Indian Cyber Crime Coordination Centre (I4C).

Stock Trading and Investment Scams

- These scams promise high returns on stock market investments, cryptocurrency, or other financial products.
- Victims are contacted through social media, WhatsApp, or fake investment apps.

- Scammers pose as financial advisors or representatives from trading firms. They convince people to deposit money in fake accounts or platforms showing fake profits.
- Once a large amount is invested, the scammer disappears.

Digital Arrest Scams

- In these scams, people are tricked into believing they are under investigation by government agencies like the CBI, Income Tax Department, or Police.
- Victims receive fake calls or video calls where scammers, often wearing uniforms, say the person's identity or bank account is linked to crimes like money laundering or drugs.
- They are threatened with arrest unless they pay a fine or security deposit immediately.

Task-Based and Investment-Based Scams

- These scams involve fake job offers or freelance work, where the victim is asked to complete small tasks and gets paid at first, building trust.
- The scam starts with simple tasks like liking YouTube videos or rating apps. Victims are paid small amounts at first.
- Later, they are asked to invest money to get larger commissions. Once a big investment is made, the scammer vanishes.

Southeast Asia-Based Cyber Scams

- MHA has estimated that over half of ₹7,000 crore lost to cyber scams from January to May 2025 originated from networks based in Myanmar, Cambodia, Vietnam, Laos, and Thailand.
- India faces an average monthly loss of ₹1,000 crore due to such scams, according to the I4C.
- **Chinese-Controlled Scam Centres and Trafficked Workers**
    - The scams are reportedly operated from high-security compounds controlled by Chinese operators, where trafficked individuals, including over 5,000 Indians, are forced to work.
    - People from Africa, East and Southeast Asia, Central Asia, West Asia, Europe, and the Americas have also been identified in these centres.
- **Scam Hotspots**
    - Through intelligence inputs and survivor testimonies, the Indian government has identified at least:
        - 45 scam centres in Cambodia
        - 5 in Laos
        - 1 in Myanmar
- **Major Types of Cyber Frauds Identified**
    - Investigations revealed three primary scam categories:
        - Stock trading and investment scams
        - Digital arrest scams
        - Task-based and investment-based scams
- **Agents Recruiting Indians for Cyber Scam Work**
    - The Indian government has tracked down several agents hiring Indians for these operations.

    - These agents are from Maharashtra; Tamil Nadu; Jammu & Kashmir; Uttar Pradesh; Delhi.
- **Human Trafficking Routes Traced**
    - Rescued victims revealed various international travel routes used to traffic Indians to scam centres, including:
        - Dubai → China → Cambodia
        - Tamil Nadu → Cambodia
        - Maharashtra → Thailand → Cambodia
        - Delhi → Bangkok → Cambodia
        - Kerala → Singapore/Vietnam → Cambodia
        - Kolkata → Vietnam → Cambodia (by road)
- **Government Response**
    - The Centre formed an inter-ministerial panel, identifying loopholes in banking, immigration, and telecom systems.
    - The CBI has registered FIRs against PoS agents for issuing ghost SIM cards linked to these scams.

Source: IE
