Cybercrime Threats: Panel Identifies Vulnerabilities Targeting Indian Jobseekers

July 28, 2024 • vajiramandravi.com

What's in today's article?

- Why in News?
- Cybercrimes Originating from these Southeast Asian Countries
- Types of Cybercrimes Originating from these Southeast Asian Countries
- Panel Report
- Proposed steps to address this issue

Why in News?

- The Centre's high-level interministerial panel has identified loopholes in banking, immigration and telecom sectors that enable cyber scams originating from Southeast Asian countries.

Cybercrimes Originating from these Southeast Asian Countries

- As per various reports, over 5,000 Indians are suspected of being stuck in Cambodia and forced to carry out cyber fraud.
- According to government estimates, Indians have been duped of at least Rs 500 crore in the past six months.
- Analysis of data by the Indian Cyber Crime Coordination Centre (I4C) has observed an increase in the number of cybercrime incidents targeting India.
    - About 45% of them originate from the Southeast Asia region, mainly Cambodia, Myanmar and Laos PDR.
- Around 1 lakh cyber complaints have been registered with the National Cybercrime Reporting Portal (NCRP) since January 2023, and 800 complaints from January to June 1 this year.

Types of Cybercrimes Originating from these Southeast Asian Countries

- **Trading scams:**
    - The alleged fraudsters issued ads on social media offering free trading tips, often using pictures of well-known stock market experts and fake news articles.
    - The victims would be asked to install some specific trading applications and start investing on the apps.
    - The victims deposited money in particular bank accounts to buy shares, and were shown some fake profits in their digital wallets. But when they tried to withdraw this money, they were unable to do so.
    - **Between January and April this year, Indians lost Rs 222 crore to 20,043 trading scams.**
- **Digital arrest:**
    - A caller would inform potential victims that they had either sent or were the intended recipients of a package containing contraband, illegal products, drugs, forged passports, etc.
    - Once they had the target, the criminals would contact them over **Skype or another video calling platform.**
    - **They would pose as law enforcement officials** and demand money for a compromise and closure of the case.
    - **The victims were digitally arrested**, which meant they were forced to stay visible to the criminals until their demands had been met.
    - **Between January and April this year, Indians lost Rs 120 crore to 4,600 digital arrest scams.**
- **Investment/ task-based scams:**
    - Scammers target victims through WhatsApp, promising money for boosting social media ratings of some entities.
    - They are then asked for bank details, receive a small sum, and are lured into larger investments with promised returns.
    - Profits never materialise, leaving victims trapped in a fraudulent scheme, highlighting the exploitation of trust for financial gain.
    - **Between January and April this year, Indians lost Rs 1,420 crore to 62,587 investment scams.**
- **Dating scams:**
    - The male victims were seduced by individuals they mistook for foreign women.

    - These “women” would make preparations to meet in person after making marriage or relationship proposals.
    - The victim would receive a call from the “woman” explaining that she had been held at the airport and needed money to be released.
- **Between January and April this year, Indians lost Rs 13 crore to 1,725 romance/dating scams.**

Panel Report

- The high-level interministerial panel has identified three shortcomings in the system:
    - Involvement of the senior bank managers of two nationalised banks to open mule accounts;
        - It was found that maximum accounts were allegedly opened with the connivance of senior bank managers/ staffers in several branches of State Bank of India and Punjab National Bank.
    - around 30,000 unreturned passengers travelling on visitor visa to Cambodia, Thailand, Myanmar and Vietnam from January 2022-May 2024; and
    - misuse of bulk SIM cards.

Proposed steps to address this issue

- In the first six months, around 4 lakh mule accounts (bank accounts used for laundering cybercrime funds by using KYC documents of others) have been frozen.
- Between January 2022 and May 2024, around 73,000 Indians traveled on visitor visas to Thailand, Myanmar, Malaysia, Vietnam, and Cambodia. However, about 30,000 of them did not return.
- The immigration bureau plans to share the details of these individuals with the relevant states—Kerala, Tamil Nadu, Punjab, Andhra Pradesh, Delhi, Odisha, Madhya Pradesh, Mumbai, Telangana, and Uttar Pradesh.
- These states are tasked with tracing the families of the missing individuals to gather more information about their whereabouts.

Q.1. What are mule accounts?

Mule accounts are bank accounts used by criminals to launder money obtained from illegal activities. These accounts are often opened with stolen or fake identities, allowing funds to be transferred and withdrawn without detection. Account holders, or “mules,” may be complicit or unwitting participants in these schemes, facilitating cybercrime operations.

Q.2. What is digital arrest?

A digital arrest is a type of cyber scam where criminals deceive victims into believing they are involved in illegal activities, often through fake law enforcement communications. Victims are pressured to make payments to avoid arrest or legal consequences. This scam can involve threats, impersonation of officials, and demands for money, leaving victims fearful and financially exploited.

Source: Panel finds cracks that help hackers target jobseekers

Times of India

Indian Express
