Inside Southeast Asia’s Scam Compounds: How Cybercrime Hubs Trap Victims

November 2, 2025 • vajiramandravi.com

Scam Compounds Latest News

- Around 500 Indian citizens who recently escaped the KK Park cybercrime hub in Myawaddy, Myanmar, near the Thailand border, are being repatriated by the Indian government.
- The episode underscores the rapidly growing crisis of transnational scam centres in Southeast Asia, where thousands are trafficked or coerced into running online fraud operations across the region.

KK Park: Myanmar’s Infamous Scam Hub on the Thai Border

- KK Park is one of the most notorious scam centres located in **Myawaddy township, Karen State, on the Myanmar–Thailand border**.
- It is controlled by the Border Guard Force (BGF) led by warlord Saw Chit Thu, who is closely linked to Myanmar’s junta chief, Min Aung Hlaing.

- Recently, after reports of illegal Starlink internet use at these scam centres, the Myanmar junta carried out a so-called “raid” at KK Park.
- While the **raid was mostly symbolic**, it caused panic among thousands of low-level workers, many of whom escaped the compound and queued at the border hoping to cross into Thailand.
- Locals said the BGF coordinated the operation with the junta, highlighting the **deep collusion between military authorities and criminal networks**.

Inside the Scam Centre Business Model

- According to the Global Initiative Against Transnational Organized Crime (GI-TOC), scam centres are large, jail-like compounds where thousands of people are trafficked and forced to commit cybercrimes.
- These facilities operate like factories — highly organised, guarded, and profit-driven.

How Victims Are Trapped

- Scammers post fake job ads online for high-paying IT or marketing roles.
- Victims — mostly from India, China, Vietnam, the Philippines, Africa, and Latin America — are flown to major hubs like Bangkok and then smuggled across borders into Myanmar or Cambodia.
- Once inside, their passports are seized, and they are told they’ve been “sold” and must work to repay a fake debt.
- Under constant watch, they face 12-hour workdays and threats of torture — including beatings, electric shocks, starvation, and solitary confinement — if they resist.

Common Types of Scams

- The most notorious scheme is “**pig butchering**”— a mix of romance and investment scams.
    - Scammers build emotional trust with targets online, pretend to offer profitable crypto investments, and show fake early profits to gain confidence.
    - Once the victim invests larger sums, the scammers vanish with all the money.
- Other common frauds include impersonation scams (posing as police or bank officers) and sextortion or blackmail scams.

Myanmar’s Central Role in Southeast Asia’s Scam Network

- According to the UN Office on Drugs and Crime (UNODC), large-scale online scam centres thrive in **lawless border regions and militia-controlled zones** across Southeast Asia.
- Myanmar has become a key example, where weak governance and armed groups have created “failed state” conditions that allow such operations to flourish.

The Border Guard Force (BGF) System

- In the mid-2000s, Myanmar’s military created the Border Guard Force (BGF) scheme.
- It allowed ethnic militias in areas like Kokang (Chinese border) and Karen State (Thai border) to keep their weapons and local control in return for loyalty to the junta.

- Min Aung Hlaing, the current junta chief who led the 2021 coup, strengthened this arrangement.
- He was even photographed conferring ranks on BGF leaders such as Saw Chit Thu, many of whom are deeply involved in scam operations.

The Coup Expanded Criminal Empires

- After the 2021 coup, the junta's partners — including the BGF — were given free rein to expand illicit businesses, such as scam compounds and human trafficking networks.
- The junta "taxed" these illegal profits to fund its war effort, further embedding corruption and crime in the system.

China's Reaction and Operation 1027

- Until **2024**, most scam victims were **Chinese citizens**, making it a **domestic issue for Beijing**.
- Frustrated with the junta's inaction, **China quietly supported Operation 1027** in **late 2023**, where the **Three Brotherhood Alliance** (ethnic armed groups) launched a **major offensive** to shut down BGF-run scam centres in **northern Shan State**.
- The junta lost significant territory, and **over 41,000 suspects were handed over to China**.

The Shift Southward

- Despite this crackdown, the scam industry did not end — it moved.
- Operations shifted south toward the Thai border, including Myawaddy, Mandalay, and Yangon, and began targeting new victims outside China, including India and other countries.

Indians Trapped and Targeted in Southeast Asia's Scam Crisis

- India has been hit both as a victim and a target of the growing scam hub network in Southeast Asia.
- Hundreds of Indians have been trafficked through fake overseas job offers and forced into cybercrime operations.
- In March 2025, the Indian Air Force rescued 283 citizens from Thailand, while over 1,600 Indians have been repatriated from Myanmar's scam compounds since July 2022.
- The 500 who recently escaped KK Park are part of this continuing trend.
- According to External Affairs Minister S. Jaishankar, India is deeply concerned about these cyber scam centres that have entrapped Indian nationals.
- At the same time, Indians have also become major targets of "pig butchering" and impersonation scams, turning the issue into both a consular emergency and a domestic cyber security challenge.

Source: TH | UNODC
