



# Survivor perspectives on combating exploitation in scamming centers and disrupting their operations

Report from a focus group discussion with survivors repatriated from Cambodia

**Date of Focus Group Discussion:** May 27, 2025  
**Interviews conducted by:** Winrock International



## PARTICIPANTS AND BACKGROUND

Three survivors participated in the discussion. All are Bangladeshi survivors of human trafficking and had been recently repatriated from Cambodia. Participants included: Md. Asjib (21 years old); Arsel (21); and Md. Al Main Khan (31). *(Please note: pseudonyms are used for interview participants to protect their confidentiality.)*

The three FGD participants have diverse educational backgrounds, ranging from university students to madrasa (religious school) graduates, and each participant is from different regions of Bangladesh, such as Kushtia and Kishoreganj.

All three survivors had been promised legitimate employment in Cambodia but ended up trapped in scam operations under exploitative and severely abusive conditions.

## INTRODUCTION

This discussion organized by Winrock aimed to understand the lived experiences of the survivors in detail – from the recruitment process to the trafficking journey, and finally, through their repatriation and recovery. The session also explored tactics used by trafficking networks, the structure of scamming centers in Cambodia, and how policy and community-level interventions can help to prevent such incidents in the future.

# QUESTIONS AND SURVIVOR RESPONSES

## **1. Who took you abroad? What promises were made regarding the work? How did you end up in a scamming center?**

All three participants said they were taken abroad by people they personally knew – either by relatives or neighbors. They made promises of high-paying, legitimate jobs, mostly in computer-related fields such as data entry, digital marketing, accounting jobs or administrative roles. The idea presented to each of the survivors was appealing: No need for large formalities, minimal costs and jobs with good facilities including food, accommodation and healthcare. Salaries promised by the traffickers ranged from \$1,000- \$1,200 per month.

None of the participants knew they would be working in scam centers. Upon arrival in Cambodia, they said they were taken directly to what they thought were office spaces but later realized were scamming centers. These centers are operated by foreign-led criminal syndicates, with most of the scam centers owned by Chinese nationals. In these scam centers, new arrivals were either coerced or sold from source countries including Bangladesh, Pakistan, Nepal, Sri Lanka, India and Myanmar. Once inside, participants said they were trained and forced to carry out scam operations targeting people in foreign countries including in the U.S., the United Kingdom, Australia and some Asian countries.

## **2. What was your relationship with the person who took you abroad? How were you convinced to go?**

Each participant shared that they had strong social ties with the person who facilitated their journey. Md. Al Main was convinced by a paternal cousin, while Asjib and Arsel said they were convinced by Facebook posts from their neighbors and friends. These traffickers used emotional trust and familial loyalty to build trustworthiness. The offers were tempting, promising a better future, higher earnings and even a refund if the work did not suit them.

The survivors say they now recognize that these were strategic tactics designed to manipulate their aspirations and vulnerabilities. Traffickers used persuasive language and provided partial truths, citing examples of others who had gone abroad and sharing pictures of what they described as “successful” migrants.

## **3. Who selects the targets for scamming? Are there particular methods or categories of people targeted?**

According to the survivors, the scamming centers operate through a well-structured system. Specific departments are assigned to target individuals based on geographic location and vulnerability. For example, one team might target people from the U.S., another from Bangladesh, and others from various parts of Asia or Europe.

The selection of scam targets is based on psychological profiling and country-specific trends. Victims are often approached under the pretense of offering loan services, online investments, romantic relationships or by using official-sounding threats (e.g., by someone posing as a police officer). Scam recruiters are given long lists of phone numbers, and their initial role – often called “number collect” (or “hooking”) – is to send out thousands of messages. Once someone responds, the call or chat is transferred to more senior scammers who impersonate professionals like bank managers or law enforcement officials, or who pretend to be good looking and seeking a friend or girlfriend. The participants said that these initial phone numbers are collected through an app called “Index.”

#### 4. Are there specific methods used to build trust with scam victims? Is AI used in the process?

The participants noted that building trust is central to scam success. Actual people (not AI bots) are used to establish relationships and communicate with the targets. However, AI could be used in the initial stages to organize, filter or categorize large datasets such as phone numbers, email addresses or chat logs.

The trust-building process includes creating a false sense of intimacy or urgency. For instance, scammers might pretend to be government officials, romantic partners, or financial service providers. Communication platforms such as WhatsApp, Telegram, Imo, TikTok, Telegram, and even Facebook are widely used, participants said. In some cases, AI-generated messages (templated or scripted) are sent out, but real-time conversations are managed by trained scam workers.

#### 5. What are some potential ways to intercept and prevent these scamming tactics?

**a. Social media:** The survivors strongly recommended conducting awareness campaigns through platforms like Facebook, YouTube, WhatsApp, TikTok and TV talk shows. They emphasized the importance of digital literacy and teaching people to identify scam indicators and avoid engaging with unknown profiles or people.

**b. Financial monitoring:** The use of suspicious bank accounts and digital wallets (like bKash) for scam payments should be monitored by financial institutions. Survivors suggested setting up red-flag systems for identifying unusual transactions, especially large cross-border transfers. They specifically highlighted that governments need to step up to monitor all formal transactions deposited for going abroad. However, because most such transactions occur via informal channels, they often go unnoticed.

**c. Technological monitoring:** Internet surveillance systems could be used to detect scam traffic patterns. Additionally, collaboration with tech firms can help trace IP addresses or deactivate numbers involved in scamming operations. The survivors also mentioned that the Cyber Security Unit of the Crime Investigation Department of Bangladesh Police can take a lead role to prevent scamming by using their technology.

**d. Public Knowledge Sharing:** Participants shared that widely disseminating real-life stories could also be an effective way to raise awareness among aspiring migrants about the potential risks of trafficking. While countries like Cambodia officially deny the existence of such scam centers, survivor testimonies serve as crucial evidence. Education campaigns, community meetings and survivor-led activities, including focus group sessions, can be powerful tools to deter others.

#### WHAT ARE RED FLAGS IN ONLINE COMMUNICATION?

The survivors identified several warning signs:

- Unsolicited offers of money, jobs or romantic interest.
- Requests for personal or financial information.
- Overly persistent or emotionally manipulative messages.
- Claims that the caller is a representative of police, banks, or from an official agency asking for private information.

#### WHAT CAN BE DONE SPECIFICALLY FOR YOUTH AND THE ELDERLY WHO ARE TARGETED?

Young people are often attracted by the lure of fast money and careers abroad, while older people are more susceptible to scams due to lower technological literacy. Programs should be tailored to these groups, such as job training, digital safety courses, and pre-migration orientations. Families should also be involved in creating a support system that encourages safe decision-making.



## 6. How are money transactions carried out?

Survivors said payments were made either in cash or deposited into bank accounts not directly registered under the traffickers' names. These transactions often involved witnesses, creating a sense of legitimacy.

In the scam operations, money from global targets was collected through digital wallets, using links and banking apps. Scam workers – often forced laborers themselves – only handled the initial communication. Actual money transfers were managed by more advanced scammers within the center. Participants said they lacked insight into the final steps of the financial process, because they were removed from it.

## 7. What other ideas do you have for protective and preventive measures?

Participants emphasized several key strategies:

**Regulating labor migration:** Government authorities should tighten the screening of tourist visa travelers and investigate potential links between immigration officers and traffickers. All three survivors said they passed through immigration with the unethical support from immigration police.

**Awareness programs:** Nongovernmental organizations like Winrock International can organize community-level programs showcasing survivor stories.

**Cross-border cooperation:** More collaboration between governments and international organizations is needed to dismantle scamming centers and repatriate victims.

**Safe migration training:** Promoting platforms like the [Bureau of Manpower, Employment and Training \(BMET\)](#), District Employment and Manpower Offices (DEMO), and technical training centers (TTC) can inform youth about secure, legal pathways to overseas employment.

## 8. How can we identify and protect individuals who are forced to commit scams?

All participants acknowledged that many scam workers are themselves victims of trafficking. These individuals are often locked up, tortured and denied basic rights. To protect them, authorities must recognize them not as criminals but as victims of modern slavery.

The government, NGOs and media can play a vital role by collecting data on those who traveled to high-risk countries with tourist visas. Digital trials, testimonies from returnees, and intelligence sharing can help identify ongoing cases. Victims who have been repatriated should also be given opportunities to share their stories and help build safer migration networks.

# CONCLUSION

This Focus Group Discussion provided valuable insight into the complex, multilayered nature of modern human trafficking. The survivors' stories highlight how trusted relationships, misinformation, and systemic loopholes contribute to exploitation. By documenting and sharing their experiences, we not only amplify their voices but help build better informed, protective systems that help prevent trafficking and interrupt scams.