

An unanticipated problem was encountered, check back soon and try again

Error Code: MEDIA_ERR_UNKNOWN

Session ID: 2023-09-27:47137469b7657ca78bcc96d Player Element ID: vjs_video_3



OK

Once a financial securities analyst in China, Lu Xiangri never imagined he might be a victim of trafficking and enslavement by Chinese cyber-scam operations in Cambodia.

Arriving in the Southeast Asian country in September 2020, the 32-year-old dreamed of starting his own business. To learn the ropes, he offered to help manage a friend's restaurant in the capital, Phnom Penh. His friend was from the same village in China. Lu had watched him become wealthy, buying a big house and living well. He wanted the same for himself and his family - his parents, wife and two-year-old son.

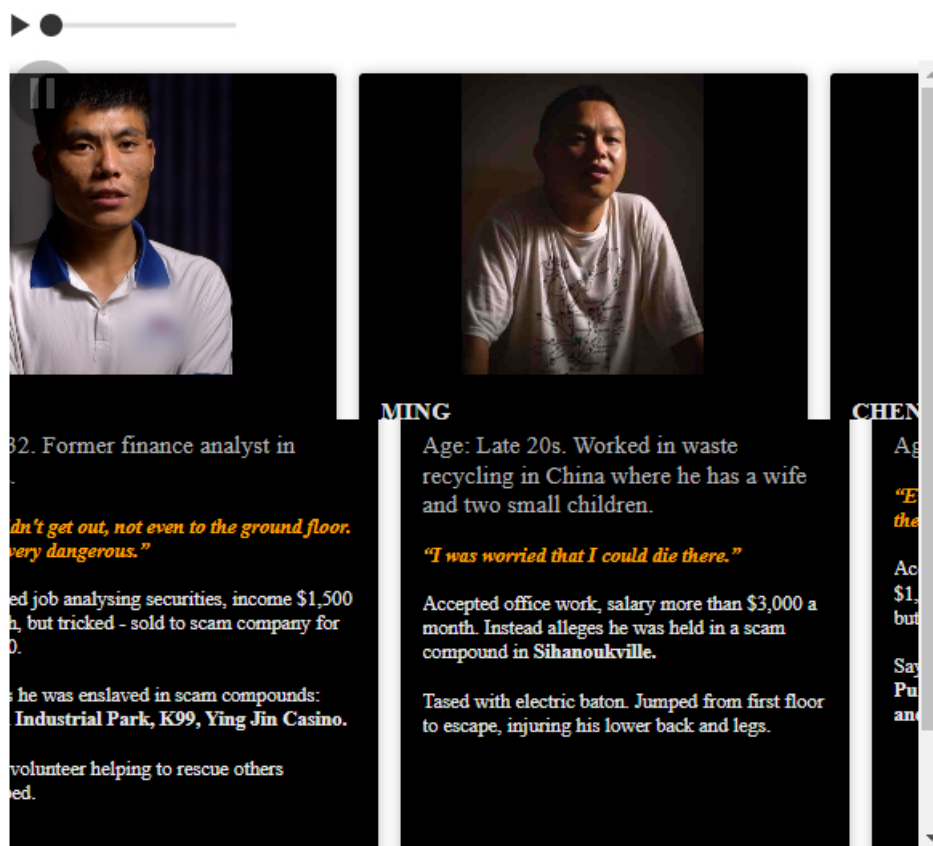
But in 2021 COVID-19 hit hard, and the restaurant closed. Lu was stranded in Cambodia without a job, unable to afford the escalating airfares and quarantine expenses to get him home.

That is when a regular diner offered him a job he would quickly re-

gret accepting.

“He said I just needed to analyse the securities market for clients and that the salary would be more than \$1,500 a month. I thought I just needed to work for two months to go back to China,” Lu tells Al Jazeera with a somewhat bemused smile.

When he arrived for his first day of work, Lu discovered it was a scam operation and, worse still, when he tried to leave, he was told he could not. The reason? He’d been sold to the company for \$12,000 and was now theirs until he paid the money back in full.



Note: Names of all the victims (except Lu) have been changed to protect their identities.

Jake Sims, Cambodia director of the human rights NGO International Justice Mission (IJM), says cases of trafficking and enslavement are not uncommon. “There are thousands of people in Cambodia being forced to work in scamming compounds,” he says.

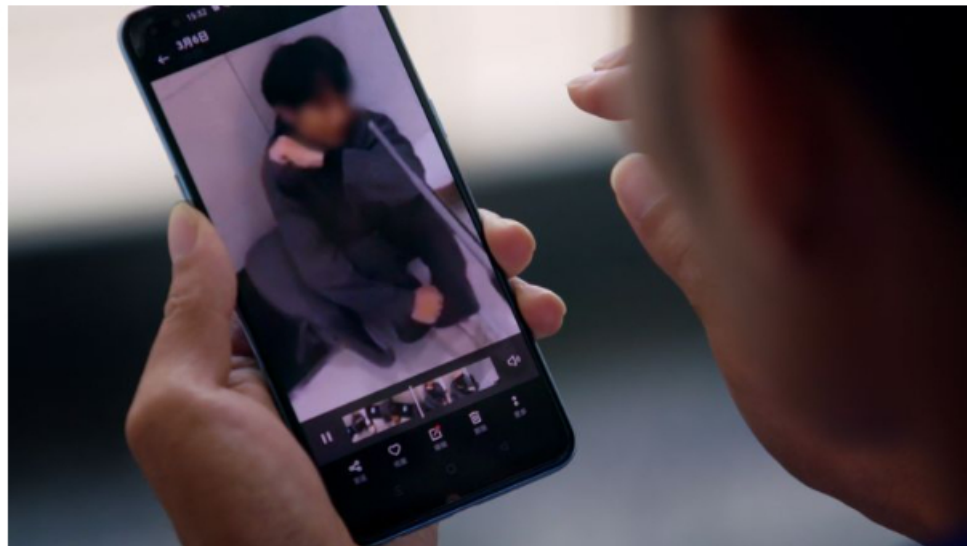
Spread throughout the country, scamming compounds are found in casinos, hotels, resorts, residential developments and office complexes. Their distinguishing features are bars on windows and balconies and barbed wire fortifying surrounding fences. With tight security placed at every entrance, they are impenetrable to anyone

every place at every entrance, they are impervious to anyone other than the criminal syndicates that run them.

Sims and his team have been working to assist the rescue of dozens of foreign nationals – Chinese, Thais, Vietnamese, Indonesians, Malaysians, people from Myanmar, and others from further afield - entrapped in cyber-scam operations in the country.

“They’re constantly reporting that there are armed guards preventing them from leaving the building. So, we know there’s confinement going on,” Sims explains.

“There are reports of people being beaten. They’re told if they call the police that they’re going to get beaten. They’re threatened to be sold at what appear to be marketplaces where humans are sold for thousands of dollars to conduct these scamming operations.”



A man watches a video of abuse inside Cambodian cyber-scam operations that was received by Lu Xiangri [101 East/Al Jazeera]

Horrifying videos and photographs of atrocities inside scam companies began surfacing on the internet in mid-2021. They show people being physically threatened, beaten with large sticks, struck with electric batons in front of other workers or while handcuffed to iron bed frames, their faces contorted in agony, their bodies covered in bleeding wounds.

In one video a man cowers in a corner of a room, spreading his hands across his head desperately trying to protect it from blows from a baton, his captor threatening to cut off his hands if his family does not pay the company \$3,000 within hours. Extortion appears

to be one of the methods of abuse used by the criminal syndicates against victims who refuse to become scammers.

In another online video, a young Thai woman sobs as she cries out for help: “I am scared that one day they will kill me.”

During months of investigation, Al Jazeera spoke to more than a dozen victims in Cambodia, China, Thailand and more recently Malaysia, who escaped from Cambodian cyber-scam operations and allege their captors are committing atrocities. We have given them pseudonyms to protect their identities.



“They’d beat you, tase you with an electric baton if you didn’t complete your task,” Ming tells Al Jazeera, still clearly shaken by the experience eight months after badly injuring his back jumping from the first floor of a scam compound to escape.

In his late 20s, with a wife, toddler and newborn baby, in March 2021, Ming answered an advertisement on the Chinese social media app WeChat for office work in Cambodia offering a salary 10 times

higher than his job in waste recycling in China.

But like many others from all over Asia who answered job ads on apps such as WeChat, QQ, WhatsApp or Telegram, Ming was tricked and then trafficked into Cambodia's cyber-scam industry.

He describes the terror he felt as armed traffickers drove him and others in his group on motorbikes across the Vietnamese border. "I could only hope that their guns wouldn't be used on us."

"I never expected to be smuggled to Cambodia without a passport. I also didn't expect the job to be in online scams," he says, his voice heavy with regret.

Ming recounts being held in a multi-storey compound housing a couple of hundred people and numerous scam companies perpetrating various types of online shopping scams roping in people in China, Europe, the United States, Japan, Vietnam and Thailand.



People from across Asia have been trafficked into Cambodia by fraud syndicates [Al Jazeera]

Sixteen-year-old Lin was working in a hotpot restaurant in her local town in China when a man she knew offered her a much better-paid typing job in Guangxi province on the border with Vietnam, but instead she and her friend were abducted and driven out of China to scam operations in Cambodia.

She tells how at one stage they were forced to walk across a mountain range. "He got his gun out and told us to stop talking because if he was caught he'd kill us. We were very scared," she says quietly.

he was caught, he'd kill us. We were very scared," she says quietly, tightly twisting the edge of a sheet between her fingers as she sits on a bed in a safe house.

Lin explains how she was forced to do sex scams. The company, she says, created an online club for men wanting to meet women. These women's profiles were stolen from all over the internet. "We'd tell the men that they had to pay for the membership before we sent the girls to meet them. But it was all fake."

The teenager says the company supervisors constantly abused them if they did not perform.

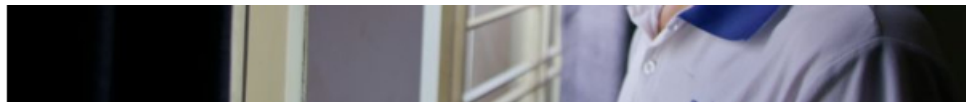
"They wouldn't hide the violence, they'd beat people in front of everyone. The supervisor knew that I couldn't bring in money. He would hit me with an electric baton as he walked past. It was really scary when he hit me."

And then at night, she says one of the supervisors would prey on them in the dormitory. Tears slip down her cheeks as she reluctantly recalls how he would touch them and they would force him away and hide in other dormitories.

To block out the horror of it all, she says she started taking sleeping tablets. After three months, unable to leave the upper floors of the scam building and knowing she was a long way from home and unable to afford to get there even if she could, she was overwhelmed with depression and desperation.

"I thought I might as well just die. I found the pills when I got back to the dorm and I took them," she murmurs, her head tilting to her chest.





Lu Xiangri was sold to scam companies in Sihanoukville. He now volunteers to help other victims of cyber-fraud syndicates [101 East/Al Jazeera]

Lin woke up in hospital where she was rescued by a team of volunteers, among them Lu Xiangri.

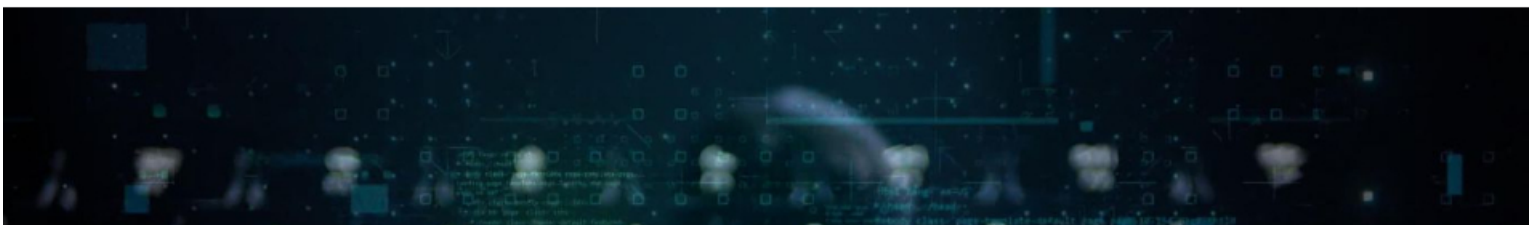
Lu had been freed a few months earlier after being held in three different scam compounds over 11 days. He says he was sold between them, his price rising each time from the initial \$12,000 the first company paid for him to \$16,700 for the second to \$18,000 paid for by the third company.

Within hours of him being sold again, he was rescued by police. Lu had made contact with them after seeking help from the Chinese Embassy and the provincial governor.

Twenty-three-year-old Chinese national Chen was also sold between three different compounds. The former chef accepted what he thought was a job promoting online games in Cambodia and even had his airfares and hotel quarantine paid for only to discover he had been sold to a scam syndicate.

He says the scam companies he was sold to did everything from online gambling scams to cryptocurrency romance scams, which he describes as “disgusting”, his repulsion palpable even with the lower half of his face hidden by a mask.

Watching footage of one of the compounds where he was confined inside a building, the young man expels his breath and shakes his head. “It was like being in prison. Even in prison, there are human rights, but in there, they don’t care,” he says, staring fixedly at the crisscrossed bars on every window.





BILLIONS IN PROFITS

Chinese cyber-scam operations are big business, stealing tens of billions of dollars a year. The scammers target not just their own countrymen but foreigners from Europe to the US to Australasia.

Twenty-four-year-old Hong tells Al Jazeera he was forced to work in a lottery scam aimed at uneducated Chinese farmers.

The aspiring golf coach was duped when he accepted what he thought was a job as a quality controller in a food factory earning up to \$3,000 a month with his airfares from China and hotel quarantine in Cambodia paid for. He says he was made to contact scam victims on the Chinese social media app, QQ, build a relationship, then entice them to invest in a lottery by downloading two apps, a legitimate lottery draw programme and the scam company's fake one.

"I'll tell them that our tag-on programme hacks into the lottery system. If you log into both applications, we can make sure you win by controlling the draws from behind the scene," he recounts matter-of-factly describing what they were instructed to do. But he says they were not allowed to tell victims that they would never be able to collect their winnings or ever get back the money invested. "When he didn't want to invest more, we had to block his account so that he couldn't cash out," he says.

According to Hong there were about 200 people working for the company and the success rate was high - thousands of victims investing between \$15,000 and \$30,000 over a couple of months.

“Ten to 20 people could make more than \$900,000 profit,” he says, his voice dropping, seemingly ashamed of having been caught up in an industry that rips off people and, more so, his fellow countrymen.



Twenty-three-year-old 'Chen' was sold to cyber-scam compounds and forced to work on cryptocurrency romance scams [101 East/Al Jazeera]

Others like Chen tell of large profits made from cryptocurrency romance scams that went after wealthy Chinese women living abroad.

The first thing he says the scam company made them do was create a fake persona using videos and photos from the internet.

“We needed to be someone handsome, positive who has a good steady job. Not like a rich kid. Just needed a proper job. I was a widower. I was told the sadder my story was, the better,” he says rolling his eyes, appalled by the deception.

“Everyone had to write a script of their life story because when you’re talking to more and more people, it’s difficult to keep track.”

The company’s success rate was seemingly high. Chen recalls a team of six people from Chengdu in Sichuan scamming more than \$3m and a woman in Canada being tricked out of \$1.5m.

According to Chen, this was just the tip of the iceberg. With access to sophisticated technology the companies made them set a goal of getting 500 people a day.

“We had this programme that you just needed to insert the country code, city code, [and] it could list all the phone numbers for the city. Then we could send greeting messages to people directly.”

He says the company also had software that enabled them to log into 20 to 30 WhatsApp accounts simultaneously and instantaneously translate messages from Chinese into any language of those being singled out.



Hieu Minh Ngo tracks Cambodian cyber-scam websites for Vietnam's National Cyber Security Centre [101 East/Al Jazeera]

The sophistication stuns Hieu Minh Ngo, who penetrates the cyber-scam websites for Vietnam's National Cyber Security Centre.

“They work very professionally, not really like a normal scam operation,” he says.

But the reformed cyber-criminal, who was convicted in the US of enormous online fraud, is even more astounded by the scale of scamming he's observed in Cambodia.

“Here's another one, another scam, 'Easy Lottery'... in Chinese completely, the same server and so many, it's uncountable!” he gasps as he sits in front of his computer, flicking from one scam website to another, to prove his point that cyber-fraud in Cambodia is on a scale like nothing he's ever seen.

“So much money. Imagine only one scam company can make up to a million dollars a day ... and there are so many, it's uncountable!”

WHY CAMBODIA?

Cambodia is the third-most corrupt country in Asia, trailing only North Korea and Afghanistan on Transparency International's Corruption Perception Index.

Prime Minister Hun Sen and his Cambodian People's Party have ruled the country for almost 40 years. International rights groups have accused him and his associates of corruption, brutality and [repression](#). They have shut down independent media, persecuted critics and banned the main opposition party; many say they treat the country like their own business empire.

The country's growing ties with China have emboldened them even more with close military cooperation and a tidal wave of Chinese investors.

Three of the most prominent investors - Dong Lecheng, Xu Aimin and She Zhijiang - have been convicted in China of financial crimes totalling tens of millions of dollars.

They all have links to cyber-slave compounds in Cambodia, espe-

cially in the southern coastal city of Sihanoukville.



1 of 3



Chinese investment has turned the once-tranquil beachside town of Sihanoukville into a casino metropolis where organised crime and corruption are rife.

In the past few years, it has become ground zero for human trafficking and slavery as Chinese cyber-scam operations stream into compounds in the city.

One enormous compound housing scam operations is adjacent to the city's main beach in a precinct known as "Chinatown".

Another is located beside the national highway leading into the city from Phnom Penh.

And another, the White Sand Palace Hotel, is directly opposite the prime minister's summer residence.

China security expert from the United States Institute of Peace, Jason Tower, investigates the web of criminal complicity behind the

cyber-slave compounds.

“If you start to look at who are the names on the titles of some of the buildings in which these activities take place, you’ll find there are people who are closely connected to the highest level of leadership in Cambodia,” he says.



Senator Kok An's Crown Industrial Park, home to cyber-scam companies, sits directly on the highway from Phnom Penh to Sihanoukville [101 East/Al Jazeera]

Most of the chief tycoons behind the scam compounds share one thing in common - close relationships with Prime Minister Hun Sen. They include a nephew, an adviser, a former adviser and a generous supporter who flew the prime minister to the UN in New York on a luxury private jet and one of his longest-serving political allies.

While Sihanoukville is the epicentre, cyber-slave compounds exist throughout the country.

Just 50km (31 miles) across the bay, victims have begun emerging from another scam compound - Long Bay.

Marketed as a luxury resort, Long Bay lies within the country's biggest real estate development, owned by a Chinese conglomerate, Union Development Group (UDG). In 2020, the US declared UDG a state-owned enterprise and sanctioned it for mass forced evictions.

The Chinese fugitive She Zhijian is a key investor in Long Bay. According to police sources, at least 50 people have been rescued from the scam compound.



Luxury resort or scam compound? Long Bay is one of the establishments in the country's biggest real estate development, owned by a Chinese conglomerate [101 East/Al Jazeera]

About 150km (93 miles) north in a remote mountain range lies another compound - this one linked to Prime Minister Hun Sen's nephew, Hun To, who has reportedly been investigated by Australian police for drug trafficking.

He is a director of multiple Heng He companies - the Chinese conglomerate behind the compound. Once again, it sits within the protective umbrella of a large concession - a Special Economic Zone owned by a former adviser to Hun Sen, Try Pheap, who has also been sanctioned by the US for environmental destruction and human rights abuses.

China security expert Jason Tower says protective zones are notorious for housing cyber-scam operations and other illicit activity, not only in Cambodia, but across the region, particularly in Myanmar.

"You might even call it a 'special criminal zone' in that they're providing a place beyond the rule of law," he says.

"They're providing a place where people who want to be involved in all sorts of fraud or other illicit activities can safely base themselves."

DENIALS

None of the individuals named by Al Jazeera responded to allegations of their involvement in cyber-scam operations, except for the prime minister's nephew, Hun To.

Declining to be interviewed, he says he is “not a competent authority to deal with the issues and not aware of any cyber-scam operations”.

In interviews with Al Jazeera, Sihanoukville's Deputy Governor, Long Dimanche and the head of Cambodia's National Committee for Counter Trafficking, Chou Bun Eng, claim almost all the complaints of trafficking, confinement and enforced labour by cyber-scam operations are fake.

“They want to change working places because they think they will be paid more and have better working conditions. And when they are not allowed to leave, they announce that they are confined,” says Dimanche.

For 27-year-old Chong, the confinement is still vividly real.

Lying in a bed, unable to walk after breaking his back and foot while desperately trying to escape from the third floor of a scam compound, the former graphic designer from China tells Al Jazeera of

his grave mistake accepting what he thought was a well-paid customer service job.

Entrapped in a company located in the northern Thai border city of Poipet, he was put to work on a type of online shopping scam targeting Russians. Having surrendered his passport, he was told he would have to pay \$20,000 to leave. Unable to afford it, he began to plot his escape.

“I thought I could tie up some clothes and pants and climb down from the third floor in the middle of the night,” he says.

But the belt he attached to the railing broke. He plummeted to the ground.

Lu Xiangri visits 27-year-old Chong who fell from the third floor of a scam compound while trying to escape [101 East/Al Jazeera]

Security guards then dragged him back to the compound and extorted \$30,000 from his family before taking him to hospital.

“They locked me up in the little dark room. I couldn't move at all. I stayed in that room for two days, and then my family paid the money.”

Now, like so many other victims of cyber-scam syndicates, he is waiting until he can return home to China.

But in the meantime he has become yet another victim on Lu Xiangri's ever-growing list of people needing help.

The former financial securities analyst has decided to stay in Cambodia to help others break free from enslavement and assist