imagine IT

THE STATE OF CYBERSECURITY | Q4 2025

Scam-Center Slavery

WRITTEN BY

Peter Durand

IMAGINE IT FOUNDER | CISO

imit.com

INTRODUCTION TO SCAM-CENTER SLAVERY

The Big Picture

THE HARD TRUTH

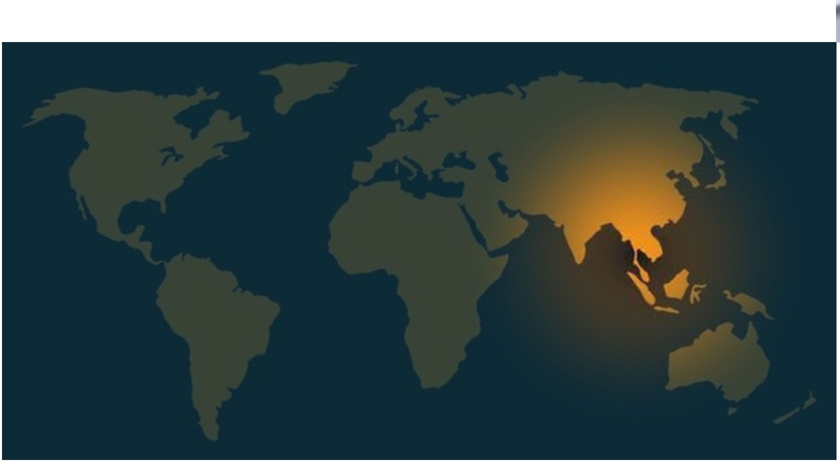
If you lose $ to cyber crime, you could be harming scam-center slavery victims.

Losing money to a cyber-criminal can be a devastating experience. Beyond the immediate financial loss, you could be exposed to identity theft, your credit rating could be harmed, and those in your business and personal circles can become targets.

What could be worse than that?

How about that you may have just facilitated kidnapping and forced labor of trafficked humans.

That's right. You are partially to blame.



There are estimated to be **over 200,000** trafficked humans held captive forced to work in scam centers.

- Most are in Southeast Asia, and there are other centers around the world.

Why This Matters

These victims are not criminals.

They are enslaved workers forced into fraud. The scam industry exploits two sets of victims: those coerced into committing crimes and those defrauded online.

Scam Centers Explained

How does it work?

A scam center is an operation run by criminal groups that use deceptive tactics to defraud individuals or businesses. These centers can be physical offices or virtual setups and are usually structured like call centers or tech support hubs.

Here's what they generally involve:

Purpose

Their main goal is to trick victims into giving away money, personal information, or access to accounts.

Methods Used

- Phone scams: Pretending to be tech support, government agencies, or banks.
- Online scams: Fake websites, phishing emails, or social media impersonation.
- Investment fraud: Promising high returns on fake schemes.

Structure

They often have scripts, training, and quotas – similar to legitimate businesses, but for illegal purposes.

Common Examples

- Tech support scams claiming your computer is infected.
- Lottery or prize scams asking for "processing fees."
- Romance scams run from call centers targeting vulnerable individuals.

Who Works in a Scam Center?

Scam centers are part of a growing human trafficking crisis tied to organized cybercrime. These operations, often called fraud factories, lure people with fake job offers and then trap them in prisonlike compounds where they are forced to run online scams under threat of violence.

Scam Centers Explained

How Victims Are Trapped

Recruitment

Victims respond to ads promising high-paying jobs in tech, customer service, or marketing. Interviews and contracts make the offers look legitimate.

Travel & Seizure

Once they arrive, traffickers confiscate passports, phones, and IDs, cutting off escape routes.

Detention

Victims are locked in guarded compounds surrounded by fences and barbed wire. Leaving is impossible without risking severe punishment.

Conditions Inside Scam Centers

Forced Labor

Victims work up to 18–20 hours a day running romance scams, crypto fraud, and phishing schemes.

Violence & Torture

Non-compliance leads to beatings, electric shocks, starvation, or even resale to other scam gangs. Some survivors report tasering and forced physical punishment.

Debt Bondage

Victims are told they owe money for travel or housing, creating a cycle of coercion.

Psychological Abuse

Threats against families and constant surveillance keep victims compliant.

Scale Of The Problem

100,000
Slaves in Cambodia

120,000
Slaves in Myanmar

60+ Countries
with trafficked victims

Spreading Globally

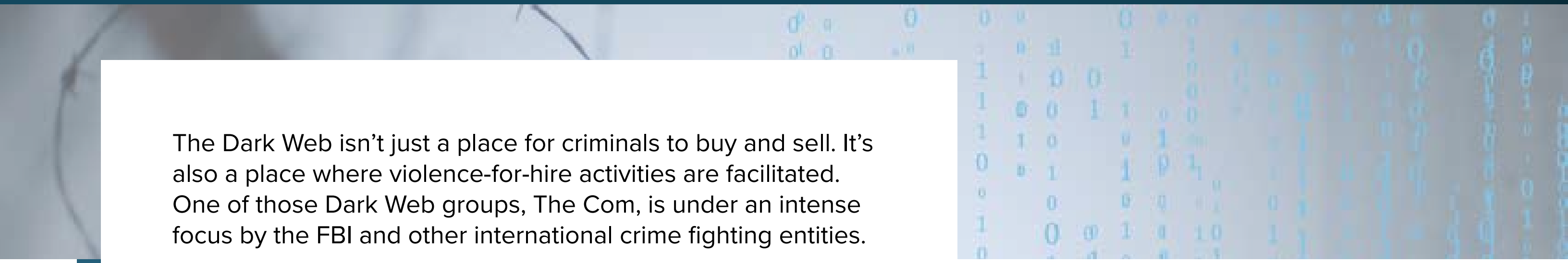
Originally concentrated in Southeast Asia, these operations now appear in West Africa, the Middle East, and Latin America.

Powerful Criminal Networks

Many centers are linked to Chinese organized crime and transnational syndicates, generating billions annually.

INTRODUCTION TO “**THE COM**”

A New Dark Web Terror Group



The Dark Web isn’t just a place for criminals to buy and sell. It’s also a place where violence-for-hire activities are facilitated. One of those Dark Web groups, The Com, is under an intense focus by the FBI and other international crime fighting entities.

Here’s a detailed overview of The Com hacking group:

The FBI classifies The Com as one of the most urgent online threats to young people.

Name and Origin

“The Com” (short for The Community) is a decentralized cybercriminal ecosystem that primarily operates in English-speaking regions.

Membership

Thousands of members, mostly aged 11–25, making it one of the most youth-driven cybercrime networks.

Structure

It’s not a single gang but a loose federation of subgroups with overlapping memberships.

Core Subgroups

- **Hacker Com:** Focused on technical cybercrime (ransomware, SIM swapping, phishing, IP theft, malware development).
- **IRL Com (In Real Life):** Focused on Real-world violence-for-hire, kidnappings, and extortion. Often coordinates with Hacker Com for intimidation.
- **Extortion Com:** Sextortion and exploitation of minors, often luring teens into providing embarrassing photos or videos. They use threats of doxing, swatting, and violence to coerce victims into compliance.

Recruitment

Targets minors via gaming platforms and social media, exploiting their belief that juveniles can’t be prosecuted.

Motivations

Financial Gain **Retaliation** **Notoriety** *Status within the group*

Why It’s Dangerous

- Combines digital crime with real-world violence.
- Decentralized and fluid structure makes law enforcement tracking difficult.
- Heavy involvement of minors increases long-term risk and complicates prosecution.

Stay Protected

How to Avoid Scam Center Fraud

Avoiding scams requires a mix of awareness, verification, and security practices.

Here's a practical guide:

Recognize Common Red Flags

- Unsolicited Contact: Calls, emails, or messages claiming urgent action (e.g., "Your account will be suspended").
- Pressure Tactics: Threats, time-limited offers, or emotional manipulation.
- Requests for Sensitive Data: Asking for passwords, MFA codes, or payment details.
- Unusual Payment Methods: Gift cards, crypto, wire transfers.

Verify Before You Act

- Check Official Sources: Contact the company or agency directly using official numbers – not those provided in the message.
- Look for Domain Authenticity: Scam centers often use misspelled or lookalike URLs.
- Search Reviews & Warnings: Use scam-reporting sites or government advisories.

Stay Alert for Job Scams

- Too-Good-To-Be-True Offers: High pay for minimal work, especially overseas.
- Upfront Fees: Legitimate employers never ask for money for training or visas.
- Verify Company Legitimacy: Check registration, LinkedIn presence, and reviews.

Strengthen Your Digital Security

- Multi-Factor Authentication (MFA): Adds a layer of protection even if credentials are stolen.
- Use a Password Manager: Avoid reusing passwords across accounts.
- Keep Software Updated: Reduces vulnerability to malware scams.

Report and Block

- Report suspicious activity to the FTC, local cybercrime units, or anti-fraud hotlines.
- Prevent interaction with call-blocking apps and email spam filters.

Becoming a victim of a cyber-crime affects more than just you. Please do not facilitate kidnapping and physical violence against others.

If you would like more information about the current threat landscape, or would just like general cybersecurity guidance, please engage for a ***free 1-hr Business Cyber-Risk Consultation*** *with our Founder, CISO, and cybersecurity thought leader, Peter Durand.*

STABLE SAFE POWERFUL

REACH OUT

Peter Durand

IMAGINE IT FOUNDER | CISO

PDURAND@IMIT.COM