Understanding Scams:
Lifecycle, Tactics, and Countermeasures

Ts. Dr. Mohamad Nizam Kassim
Bahagian Penyelidikan Strategik
National Anti-Financial Crime Center

Sharing Agenda

Our Journey

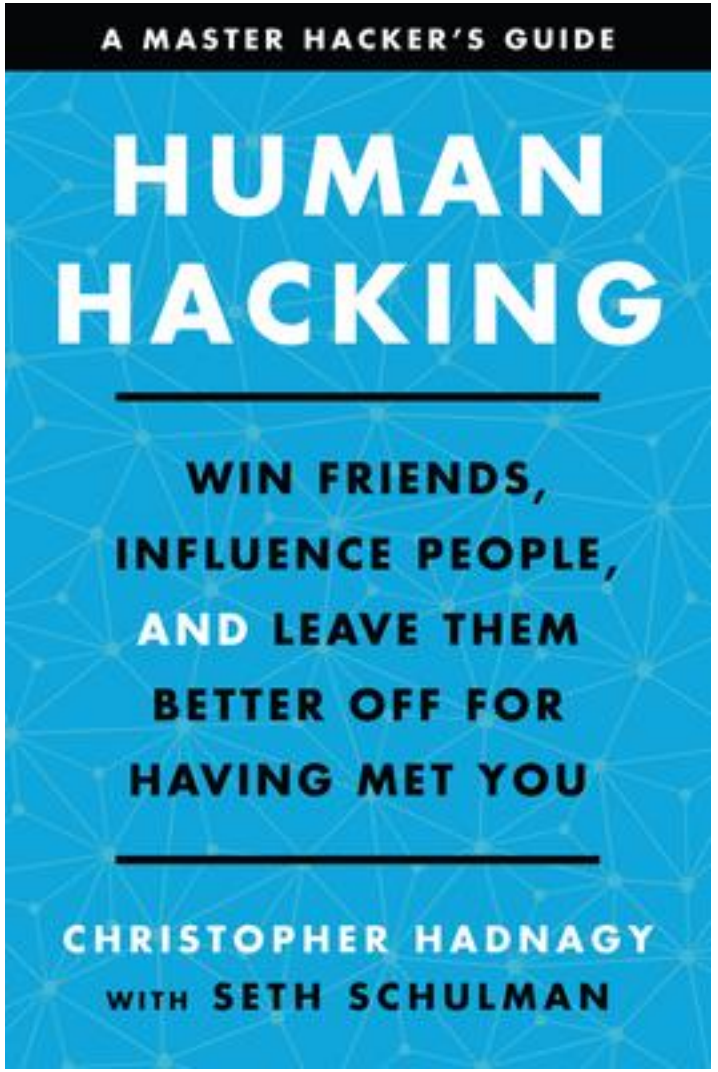
Lesson 1. What is a Scam?
Lesson 2. The Scam Lifecycle: From Setup to Exit
Lesson 3. Profile of Scammers: Behaviors and Operations
Lesson 4. Scammer Personas and Tactics
Lesson 5. Scammer Tactics Matrix
Lesson 6. Scam Disruption Framework: Intervening Across the Lifecycle
Lesson 7. The Role of AI in Scams and Scam Busting

Lesson 1. What is a Scam?

Recognizing and Defining Fraudulent Schemes

A scam is a dishonest invitation, request, notification or offer, designed to obtain personal information or a financial benefit by deceptive means.

- **Key Mechanism:** Uses deceit or false pretenses to make victims voluntarily give money, property, or sensitive data
- **Distinct from Theft/Hacking:** Victims authorize the transaction or share information under deception
- **Common Examples:**
  - Fake investment opportunities
  - Romance scams
  - Impersonation of officials
  - Phishing or fake notifications



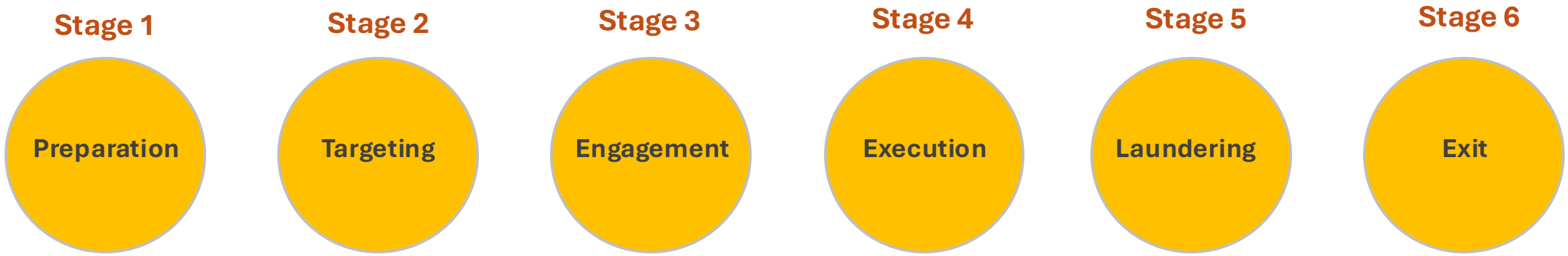
SOCIAL ENGINEER FRAMEWORK

Source: https://www.social-engineer.org/framework/general-discussion/

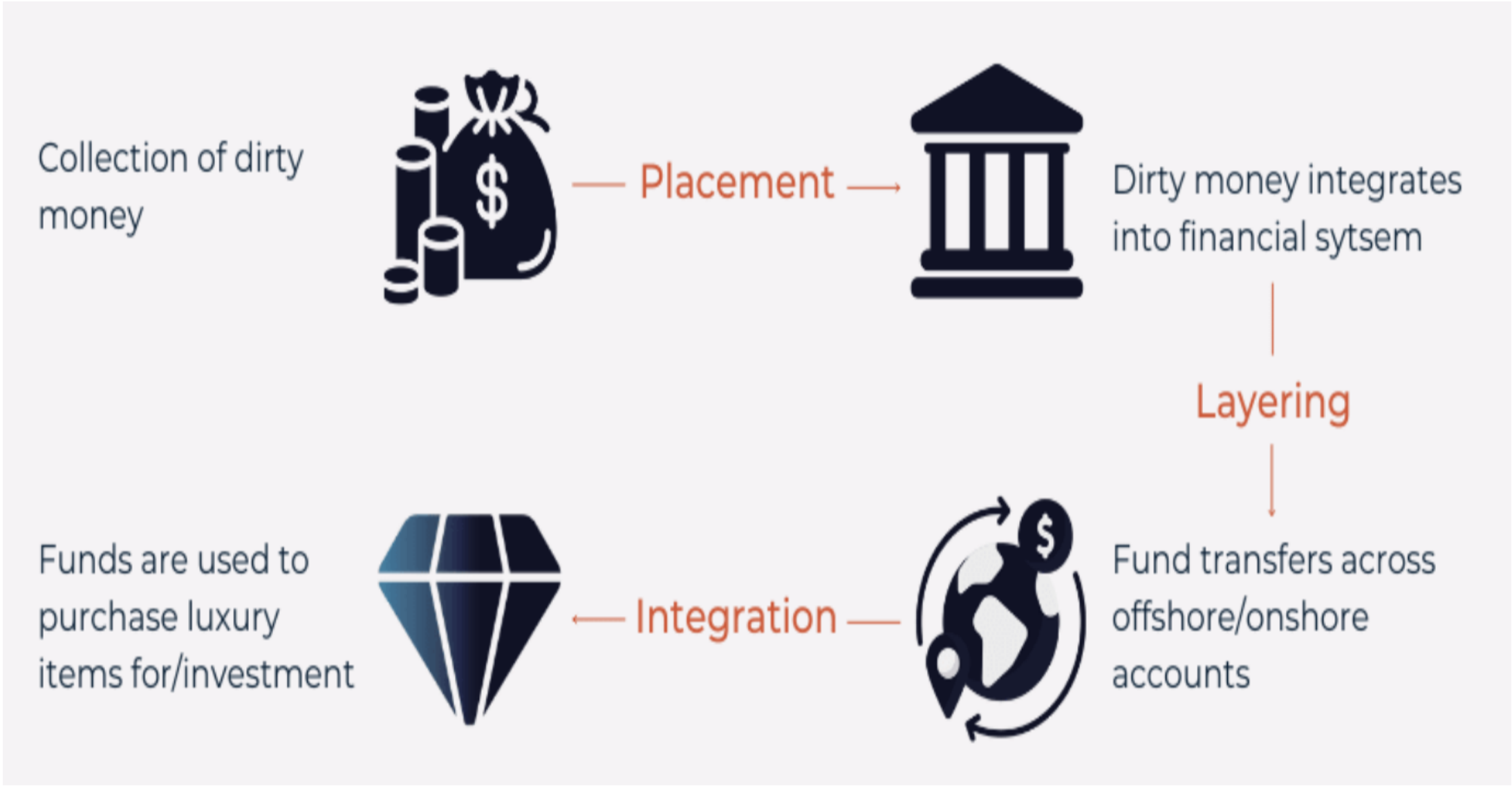
Lesson 2. The Scam Lifecycle: From Setup to Exit

6 Key Stages to Run A Scam Scheme

Scams do not happen in a single moment; they unfold through a series of stages. Understanding this scam lifecycle – from the scammer's initial preparations to the final act of disappearing with illicit gains – is key to formulating countermeasures.



Stages of Money Laundering



Lesson 3. Profile of Scammers: Behaviors and Operations

How Today's Scammers Operate, Adapt, and Deceive

Today's scammers are often professionalized criminals, whether operating in large syndicates or smaller crews. They use a blend of social cunning and tech savvy to ensnare victims, constantly refining their methods.

Not Just Lone Operators

- Many part of large, organized criminal networks with defined roles and resources
- Syndicates run call centers/boiler rooms with hundreds of staff
- Often cross-border operations (origin, target, and fund routes in different countries)

Organizational Structure

- Hierarchy: masterminds, financiers, tech specialists, victim-facing agents, money mules
- Formal training, scripts, SOPs, performance targets
- Some low-level actors coerced via human trafficking

Risk Appetite & Adaptability

- Rapid response to new security measures and regulatory changes
- Shift channels (SMS → WhatsApp/Telegram) to evade blocks
- Share scripts/tactics globally – quick adoption of new scam types

Use of Technology

- VoIP spoofing, phishing kits, automation tools, social media bots
- Encryption, VPNs, disposable accounts to evade detection
- AI tools for voice cloning, chatbots, and realistic impersonation

Lesson 4. Scammer Personas and Tactics

Psychological Manipulation

The Impersonator Official

Poses as police, bank, or gov't officials; uses fear & authority to demand payments.

The Tech Support Scammer

Pretends to be IT support; exploits fear/confusion to gain device access or fees.

The Romance Scammer

Builds fake relationships; exploits love & trust for long-term financial gain.

The Investment 'Guru'

Promises high returns; manipulates greed via fake investments & social proof.

The Job/Loan Scammer

Offers fake jobs or loans; demands upfront fees from desperate victims.

The Mule Recruiter

Recruits people to launder money; exploits greed or ignorance.

Lesson 5. Scammer Tactics Matrix

Scammer Playbook

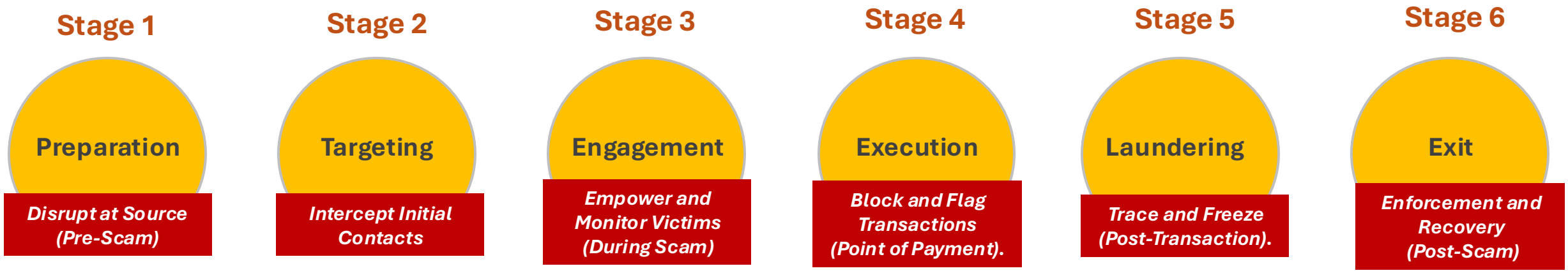
Scammers skillfully **manipulate emotions** from fear to greed and **use technology** (spoofing, fake websites, AI voices) to bolster their deceit.

Scam Tactic	Psychological Lever	Tech Tools Used	Detection Signals (Red Flags)
Phishing Email – Fake emails posing as trusted entities asking for logins or payments	Urgency ("verify now"), fear of loss, curiosity (prizes)	Mass email tools, spoofed senders, phishing kits	Generic greeting, poor grammar, suspicious sender domain, misspelled links, requests for sensitive info
SMiShing (SMS Phishing) – Scam texts with malicious links	Urgency, fear (account issues), enticement (prizes)	Bulk SMS via SIM farms, URL shorteners, spoofed sender IDs	Unsolicited SMS urging quick action, random or short sender numbers, mixed-language text, odd phrasing
Voice Impersonation Call – Pretends to be authority or familiar person (AI voice cloning)	Fear (threats), trust/affection (family)	VoIP with spoofed caller ID, AI voice cloning, robocalls	Pressure for secrecy and urgency, requests for personal data or transfers, unnatural cadence/noise in cloned voices
Social Media Scam Posts/Ads – Fake giveaways, investments, sales	Greed (freebies, high returns), excitement, trust (celebrity images)	Fake pages, stolen images/endorsements, bot sharing, links to phishing or WhatsApp	Too-good-to-be-true offers, new page, mismatched URL, "guaranteed profit" claims

Lesson 6. Scam Disruption Framework: Intervening Across the Lifecycle

Breaking the Scam Chain

Fighting scams effectively requires a coordinated Scam Disruption Framework – a blueprint that maps each stage of the scam lifecycle to specific intervention points, responsible parties, and the urgency of response needed.



Deterrence and infrastructure takedown. *Even before scammers reach victims, authorities can target their preparations.*

Filtering and early warning. *When scammers attempt to contact victims (via calls, SMS, emails, social media), various stakeholders can intercept or warn.*

Education, behavioral detection, and victim outreach. *Once a victim is in conversation with a scammer, traditional policing can't directly intervene (they often don't know it's happening).*

Payment intervention and authentication*. This is the "last clear chance" to stop the scam before money leaves the victim's control.*

Rapid response to trace funds and shut down mule accounts. *When a scam succeeds and money is sent, the focus shifts to containment.*

Investigation, prosecution, and victim support. *In the aftermath, disrupting the scam means ensuring the perpetrators are identified and brought to justice.*

Lesson 7. The Role of AI in Scams and Scam Busting

AI in Executing Scams - The New Arsenal for Fraudsters

Deepfake Voice and Video Impersonation:
Perhaps the most alarming trend is the use of AI to clone voices and even create video illusions of real people. With just a few seconds of audio of a person, AI voice synthesis can produce speech that mimics that person near-perfectly.

Conversational Chatbots and AI Personas:
Scammers also use AI-driven chatbots to conduct conversations with potential victims, especially in the early stages of scams. Advances in natural language processing allow bots to mimic human-like chatting.

Image Generation and Document Forgery:
AI image generators can create profile pictures that look photorealistic but are of non-existent people – scammers use these for fake social media or LinkedIn profiles that aren't reverse-searchable.

Scaling and Targeting via AI:
AI can sift through big data (like leaked databases or social media info) to identify prime targets. For example, an AI model could analyze profiles to find people recently widowed (for romance scam targeting) or small business owners (for BEC or loan scams).

Lesson 7. The Role of AI in Scams and Scam Busting

AI in Scam Detection and Disruption

Anomaly Detection In Transactions:
Financial institutions deploy machine learning models to monitor transactions in real-time and flag those that deviate from a customer's usual behavior or known legitimate patterns

AI-based Voice And Behavior Biometrics:
To counter AI voice scams, some institutions use voice biometrics for identity verification – essentially using AI to recognize if the speaker's voice matches the legitimate person or if it's synthesized.

Natural Language Processing (NLP) For Scam Content:
AI is used to scan and filter communications for scam signs. Email providers use NLP classifiers to identify phishing emails (look at language about passwords, urgency phrases etc.)

Image/Video Analysis For Deepfakes:
On the defender side, research is intense on deepfake detection. AI models can sometimes tell a deepfake video by subtle artifacts (like inconsistent lighting in eyes, or unnatural facial muscle movements).

Community Reporting Platforms Enhanced By AI:
Another aspect is aggregating scam reports through AI. AI helps by clustering reports that are likely about the same scammer or group, even if victims describe it differently.

AI In Law Enforcement Analysis:
Law enforcement is starting to use AI to analyze big data for investigations. For scams, that might mean using link analysis (graph AI algorithms) to find connections between suspects, phone numbers, bank accounts, and online aliases.

Scams cross borders and platforms
- so must our defenses.

Thank You.