Transnational Scams: How to Protect Yourself and Your Family

Lisa Feldman
Assistant United States Attorney
Cyber & Intellectual Property Crimes Section
U.S. Attorney's Office, Los Angeles

Assemblymember Jacqui Irwin
"Scam Alert" Town Hall
May 1, 2024

DISCLAIMER:

The views and opinions expressed in this presentation are those of the presenter. They do not necessarily reflect the views or positions of the Department of Justice.

Why Scams are Harder to Detect Now

- **Transnational Organizations**
  - ➢ Highly organized overseas groups
  - ➢ <u>Extremely</u> sophisticated
  - ➢ Groups share scripts and scam training materials
- **Manipulative and Realistic Looking**
  - ➢ No typos or bad grammar
  - ➢ Social Engineering: “Spoofing,” “Catfishing”
  - ➢ Phishing Kits: official looking business websites
  - ➢ Hacking and Artificial Intelligence (AI)

MOST COMMON TRANSNATIONAL SCAMS

- **Grandparent Scam**
- **Tech Support Scam**
- **Romance Scam**
- **Business Email Compromise**
- **Escrow Fraud**
- **“Pig Butchering” Scam**
- **(Sextortion – teenage boys)**

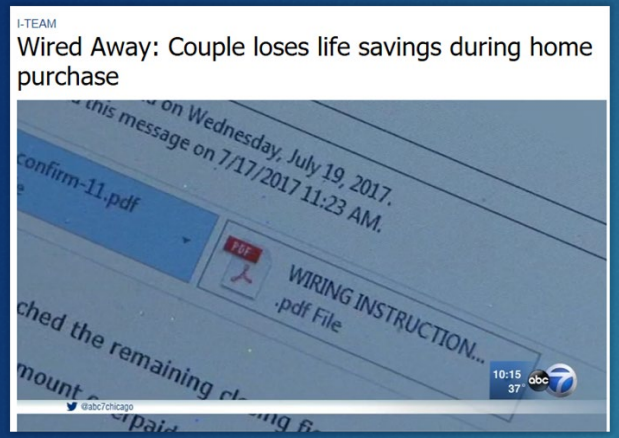
How to Recognize RED FLAGS

- **“Act Now” Scams: Urgency or Fear**
  - Frontal lobe won’t process well; “fight or flight,” not logic
  - Purpose: So you “can’t think straight”
- **“Grooming” Scams: Slowly Gain Your Trust Over Time**
  - Befriend you over dating sites, social media, wrong # texts
  - You become invested in relationship and overlook red flags
- **Payment Methods:** Gift Cards, Wire, Cash, Cryptocurrency
- **Secrecy –** “Don’t Tell Anyone”
- **Online or Phone** (Not in Person)
- **Too Good to be True**

Grandparent Scam

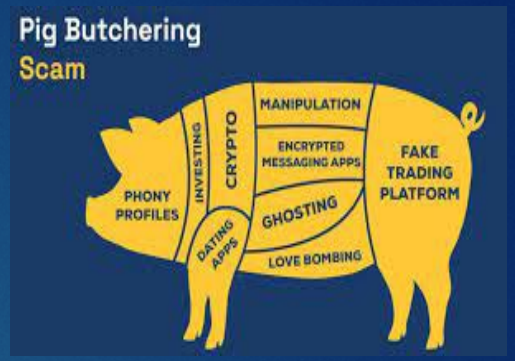
- EXAMPLES:
  - "Arrested, in jail in Mexico, need bail money."
  - "Car accident, need money for hospital."
  - "I've been kidnapped, pay ransom."
  - "Don't tell Mom and Dad!"
  - AI software can copy child's voice *EXACTLY*.
- TIPS: If you get such a call – Don't panic:
  - Create a family code – ask caller for code
  - Hang up - Call grandchild / parent to verify OK
  - Don't pay over phone

Escrow Fraud



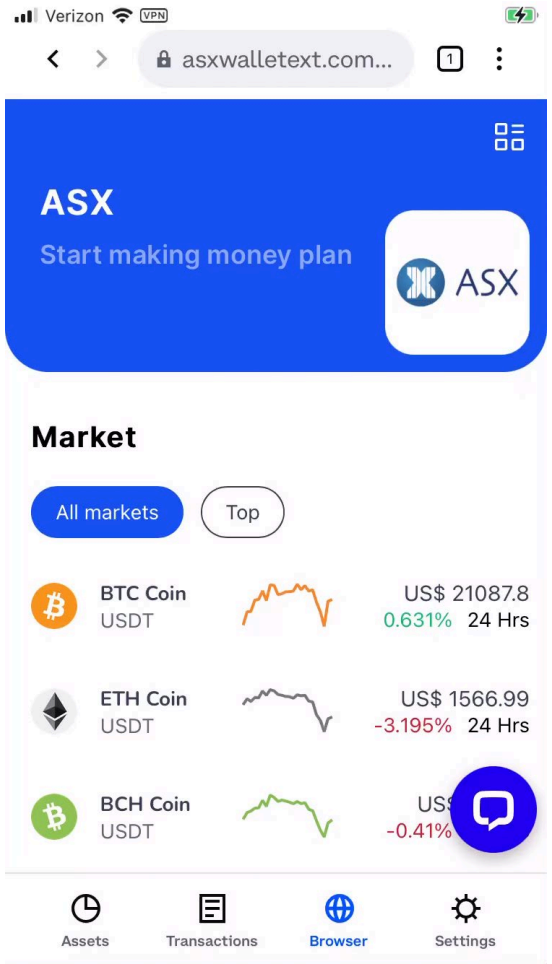
- Scammer accesses escrow officer email account and sends fraudulent email to home buyer with FAKE wiring instructions
- Buyer wires money, unaware account is FAKE, discovering scam too late to get money back
- TIP: Before wiring money, ALWAYS go directly to the source: Call Escrow Officer at number you know and verify correct wire instructions! (Don't call number in email.)

“Pig Butchering” Scam



- Why called “Pig Butchering”?
- Initial Contact and Grooming – Build Trust
- Referral to crypto “investment” app/website; let guard down
- Victim “account balance” rises – so induced to “invest” more. When ready to withdraw funds, must pay “fees,” “taxes,” “fines.” When victim realizes duped, scammer gone – with all money.
- Why? App/Website is FAKE! Funds were NEVER INVESTED and were sent DIRECTLY TO SCAMMER from beginning Watch John Oliver “Last Week Tonight” episode on Pig Butchering (Youtube).

Extremely Realistic (but FAKE) “Investment” App



Currency: BTC/USDT
Purchase: Buy or fall
Time: 180 seconds
Amount: It is recommended to trade with 10% of the account funds

- **File a complaint: www. IC3.gov**

- **If wired money, contact BANK: Financial Fraud "Kill Chain"**