Elder Abuse Schemes

- Romance Scam
- Investment Scam – "Pig Butchering"
- Overpayment Scam
- Government Imposter Scam – Smishing, Phishing, Vishing
- Tech Abuse
- Grandparent Help / Kidnapping Scam

Target Demographics

- Elderly
- People with resources
- People who are alone

Goals

- To steal money
- To steal identity
- To cause emotional pain

Investment Scam / Pig Butchering

One technique involves **assuring a victim that the scammer has made significant profits in cryptocurrency,** persuading the victim they shouldn't miss out.

Methods used in Pig Butchering:

- Contacted via social media (to build rapport)
- Discussion/Invitation to invest
- Provide evidence (screenshots) of large returns
- Express urgency of action
- Following loss of initial investment, will request larger deposit

Government Imposter Scam – Smishing, Phishing, Vishing

Criminal actors pose as IRS or Social Security Administration claiming a compromise or crime and request victim transfer funds to remedy. This scam if often originated via **Smishing** (Smishing uses text messages and apps), **Phishing** (Phishing uses emails and links), **Vishing**, (Vishing uses voice calls and voicemails).

Romance Scam

Criminal actors take advantage of people looking for romantic partners, often via dating websites, apps or social media by pretending to be prospective companions.

Methods used in Romance Scam fraud:

- Attractive online profile
- Strong emotions in short time period
- Request money for "emergencies
- Send or request to buy expensive items
- Request banking details to receive large deposits (Known as Money Muling)

Overpayment Scam

Criminal actors will claim that they falsely sent the victim an excess amount of money. The scammer will attempt to convince the victim to return the difference between the sent amount and the intended amount.

Methods used in overpayment fraud:

- Request for refunds to specific bank acct/wire transfer
- Paper check with over agreed amount
- Credit card/Pre-loaded money card for more than agreed amount
- Online purchase with over agreed amount

Tech Abuse Scams

The victim is using a computer that somehow becomes exploited. A third party now has access to this computer. Once in the system, criminal actors access victim funds and transfer the funds globally. Transfers trend to Eastern countries.

Methods used in Tech Scam fraud

- Pop-up warnings with logos from trusted companies/websites
- Online ads and listings in search results
- Phone call with trusted company name in caller ID
- Email with trusted company name in offer

Grandparent help / Kidnapping scam

Criminal actors pose as a grandson or granddaughter in a foreign country. This scam exploits trust and deceives the victim into transferring funds to a foreign country, to potentially help the grandchild.

DO's

- Sign up for two factor authentication
- Use Anti-virus
- Pay close attention to your bank and credit card statements

DON'Ts

- Convert money into giftcards for payment
- Send Cryptocurrency payments like Bitcoin, Ethereum
- Send money to someone you don't know
- Respond to phone calls, emails, or text messages that ask for personal or financial information

Contact your local office:

USSS New Orleans FO 504-841-3260;

USSS Baton Rouge RO 225-925-5436;

LACF@secretservice.gov

Please scan the QR code

and fill out the intake form.

DON'T BE A VICTIM TO CYBER CRIME

LACF@secretservice.gov

Elder Financial Abuse

U.S. Department of Homeland Security

United States Secret Service