



C A L I F O R N I A

DEPARTMENT OF JUSTICE

Online Scam Prevention

How common are online scams?



- FBI's 2024 Annual Internet Crime Report
 - \$16 billion lost to all internet crime
 - Over \$6.5 billion to investment fraud scams alone
 - Largest single category of loss

Scams and the human impact

Dennis Jones

- 82-year-old divorcee
- Facebook “friend”
 - Spent months building the relationship
- Convinced him to “invest” in cryptocurrency
- Lost everything, committed suicide



<https://www.cnn.com/2024/06/17/asia/pig-butcheringscam-southeast-asia-dst-intl-hnk/index.html>

Pig Butchering

- Organized crime operating in Southeast Asia
 - Fattening up: investing the time to maximize the taking
 - May use any of type of scam
- Incredibly sophisticated
 - Gather information about you and your finances
 - Often involve networks of fake people, websites
 - May include believable real-time video calls
 - Often collect “taxes” and “fees” when victim seeks return of money
 - Frequently launder stolen funds via crypto

Scammers are Predators that Prey on Your Emotions

- Tech Support Scams
- Romance Scams
- Investment Scams
- Work from Home Scams
- Fear-Based Scams
- Pig Butchering



Tech Support Scams

- Pop-Up or Email leads victim to Scammer
- Scammer pretends there is a computer problem
- Problem starts affecting bank accounts, etc.
- Scammer offers to help



Romance Scams

- Scammer pretends to be in romantic relationship
 - Often using fake profiles and fabricated stories
 - May spend time to gain trust / build emotion
- Warning Signs:
 - Rapid declarations of love
 - Requests for money
 - Excuses to not meet in person



Investment Scams

- Pretend to have an investment opportunity
 - Often supported by websites showing fake “returns”
- Warning Signs
 - Requests for money
 - Promise of unreasonable returns
 - Excuses for not meeting in person



Work From Home Scams

- Pretend to have a job opportunity
 - Often supported by a website, a work account, bosses
- Job needs your crypto
- Warning Signs
 - Any request for crypto related to a job
 - Promise of unreasonable returns
 - Excuses for not meeting in person



Fear-Based Scams

- Pretend you are in trouble or have a problem
- Need you to move your money to solve it
- Warning Signs
 - Sense of urgency
 - Threat of consequence to you or relatives unless transaction occurs
 - Threat to expose you or your relatives to ridicule or criminal prosecution
 - Promise to “protect” your money once the transaction occurs



Fear-Based Scams

- Can be very sophisticated
 - May use the name of real law enforcement official, employee of your bank, or other trusted person
 - May use non-public knowledge from data breaches / social engineering
 - May use fake voices of persons you know
 - May even spoof their real phone number
- E.g. relative bail money, identity thief
- E.g. terror/CSAM financing

Safety Tips

- Who do you know only via phone, email or text?
 - Never send money to someone you don't know in person
 - Scammers will impersonate real people and people you know
- Skepticism of any claim to need money right away
- Invest in person at financial institutions you trust
- Be especially wary of “new” investments like crypto
- If it's too good to be true, it probably is



Safety Tips

- Crypto ATMs
- Other methods to be wary of:
 - New crypto “exchanges”
 - Cash courier



If You've Been a Victim

- Recognize that you are a scam victim
- Stop sending money
 - Beware “recovery” scams
- Report to Law Enforcement ASAP
 - Local Police Department – In Person
 - Tell them to contact Cal DOJ Cybercrime Unit for assistance if they do not know what to do to investigate these crimes
 - FBI: <https://www.ic3.gov/>
- Seek Help and Support from People you Know



How to Help Others and Prevent Scams

- Talk about scam awareness with friends and family
- Create in person communities as a sounding board
- Discuss the potential that it may be a scam in person with a trusted person before any financial decision
- Don't blame or shame victims
 - Help, counsel, and support them

Contact Information

Address: Public Inquiry Unit
Office of the Attorney General
P.O. Box 944255
Sacramento, CA 94244-2550

<https://oag.ca.gov/contact/general-contact-form>

