The Joy of Scams and Fraud

How to understand and avoid them

Scope of the problem

- 73% of Americans report having been exposed to scam activity and 21% have lost money.
- The average amount of money lost in the US by scam victims is $3520, with similar figures for citizens of Denmark, Switzerland and Singapore. Total amount of money lost worldwide was 1.03 trillion USD, 64 billion in the US alone.
- It is a problem, pretty much equally, for all age and race groups
- Despite increasing awareness of the problem, it is continuing to increase.

Types of scams

Phishing - Fraudulent emails, texts, or messages pretending to be from legitimate companies to steal passwords, credit card numbers, or other personal information.

Vishing - Voice phishing, where scammers call pretending to be from banks, tech support, or government agencies to extract information or payments over the phone.

Smishing - Phishing via SMS text messages, often claiming there's a problem with your account or a package delivery.

Romance scams - Scammers build fake romantic relationships online to eventually ask for money, often claiming emergencies or travel expenses. Also called “pig butchering”

Investment/Ponzi schemes - Promising unrealistic returns on investments, using new investors' money to pay earlier investors until the scheme collapses.

Tech support scams - Fraudsters claiming your computer has a virus or problem, then charging for unnecessary "fixes" or installing malware.

Lottery/prize scams - Telling you you've won something but need to pay fees or taxes upfront to claim it.

Advance fee fraud - Promising large sums of money (inheritance, business deal) if you first pay smaller processing fees. Includes timeshare sales, investment offers

Charity scams - Fake charities, especially appearing after disasters, collecting donations that never reach victims.

Employment scams - Fake job offers that ask for upfront payment for training, equipment, or background checks.

Grandparent scams - Calling elderly people pretending to be a grandchild in urgent trouble needing money.

Cryptocurrency scams - Fake investment platforms, pump-and-dump schemes, or impersonating legitimate crypto exchanges.

What happens when a phishing/smishing attempt succeeds?

- Clicking on link takes you to a site that looks real
- Information you enter there (such as passwords or other personal information) is copied by scammers
- This information can be used to access your contacts to scam them, access your bank account or social security to drain funds, engage in identity theft
- Scammers can install malware on your computer that allows them to access private information including finding passwords for other websites

Simple rules

- Don’t click on links in emails or messages. Go directly to a trusted website to see if any action is needed.
- Beware anyone you don’t know well who tries to make you do anything urgently.
- Call a trusted friend or family member before believing anything about a sick or injured relative. Always verify information.
- Do not trust someone who tells you that you need to do something right away or keep information secret.

Grandparent scams

Artificial intelligence can be used to generate a voice that sounds like someone you know

The story is often that a close relative has been injured and you need to send money right away for an operation or medical care

Instead of relative, this can be a lost pet or another vulnerable individual

Having a “family password” that is based on information a scammer is not likely to have (nicknames of a pet for instance) can make this less successful

If it sounds like an emergency it probably is not

What are some resources for learning more and taking action?

FBI operates the Internet Crime Complaints Center: https://www.ic3.gov/

Scam detector considers themselves the Wikipedia of scams and has various tools including identifying scam websites as well as many informative articles about new, old and upcoming scams. https://www.scam-detector.com/

Who is doing this?

Scams can originate almost anywhere, but Myanmar, Laos and Cambodia have the most significant organized scam farms. Political upheaval and poverty has driven the industry, which funds parts of governments as well as rebel and insurgent groups.

Scammers are often trafficked by being offered legitimate jobs, then trapped in compounds where they are punished if they are not productive. Some scammers take these jobs because of lack of other employment and some are self employed.

There are American scammers, but they tend to focus on specific groups of people such as time-share owners and Medicare recipients.

Glossary of terms

https://www.ftc.gov/news-events/topics/glossary-scams-legal-terms

This is website from FTC discussing some common scams and terms relating to them

https://www.scam-detector.com/romance-scams/

This website from scam detector has many types of common scams

Stay tuned!

Will be starting a discussion group on scams!