SCAMS
FRAUD
CONS

LIBRARY FREEDOM PROJECT

What Are Scams?

Scams (AKA Cons, Fraud, etc.) refer to deceptive strategies intended to trick or coerce someone (the "mark") into giving the scammer something of value, usually money

Why Are Scams?

Scamming is a way to get money outside of the formal economy. Most underground economies are shaped by extreme poverty and desperate conditions, and scamming is no exception. Many people engaged in running scams live in the Global South, and a significant number are forced into the work through various mafias of the world.

Scamming online usually has the lowest risk for the highest reward.

Scamming online instead of in-person obviously prevents harm to someone's physical body, but it also carries a lower legal risk than in-person theft; legal enforcement is sparse, and the consumer protection environment is not robust.

While some scam people within their local community, it's more lucrative to scam people in wealthier areas. Class segregation and border policing physically separates the poorest from the wealthiest, so the easiest way to initiate an interaction is through global communication infrastructure (e.g. phones and internet).

How Do Scams Work?

In order to convince you to give them money, banking information, or access to your computer, they need to determine when you already do those things and then artificially replicate those scenarios.

What communication technologies do you use?

Who would you respond to?

Why, or in what situations, do you give access to your computer/phone, sensitive information, or money?

How do you give access, share information, or send money using technology?

Your answers to all of these questions will be avenues scammers may use.

If you use a communication technology, a scam can come through that technology.

If you would respond to any person/organization /system, the scammer could imitate them (especially if their image/ information/voice was easily findable online).

If you see a hyperlink, download, login page, new app, ad for something, computer alert, etc-- these are avenues to access your information, computer, or money.

If you're not sure, don't click. You're better safe than sorry!

ONLINE SAFETY TIPS

- Update software as soon as there are new updates!
- Use different, secure passwords for each account (password managers may help make this easier to do and remember)
- Make backups of devices using cloud storage or external hard drive to prevent loss due to malware
- Practice caution with strange calls, texts, emails, or messages on social media, even from someone you know. Have a safety phrase you can use to check if it's really them.
- Practice caution with links, attachments, downloads, etc. Only download software from trusted locations.
- Stay calm. Hang up the phone, step away from the computer, and tell someone.

How Does Impersonation Work?

Scams of this type rely on social pressure and our obligations to other people, organizations, or systems.

Efforts to impersonate can be aided by technology in increasingly effective ways:

- learning about the mark through social media or data breaches
- using AI voice technology to sound like someone's loved one, often using previously recorded audio available online
- designing authentic appearing websites or mobile apps in which money can be exchanged

However, impersonating someone you know involves the central difficulty of making sure the you don't contact the actual person(/org/system) being impersonated

Persuasive deception works best when people feel a sense of fear, shame, and urgency to make a decision. Those feelings effectively dissuade most people from reaching out to their support networks for help or taking time to fact-check what's being claimed. This is why if you experience a call/text/email/alert/ad/other remote communication that says you must act ***urgently*** (especially if it involves something ***frightening, embarrassing***, or states outright that you should keep it ***secret***): ***before you act you should tell someone.***