PROTECT YOURSELF *from* ABUSE

Red Flags of Social Engineers and Abusers

Social Engineers exploit people's empathy and desire to help by manipulating them into doing questionable things or sharing confidential information.

Social engineering attacks have 3 phases

1. *Gather information about their victims.*
2. *Develop a relationship with the victim.*
3. *Use the relationship to exploit their victim.*

Protecting Yourself from Social Engineering

Digital hygiene is critical to keeping yourself safe, and it's often ignored. This isn't extensive, but:

- *Passwords should be unique and complex*
- *Use two-factor authentication (2FA)*
- *Use different passwords for each site and adopt a password manager like LastPass*
- *Update your software as soon as possible*
- *Encrypt all your devices*
- *Search with DuckDuckGo instead of Google*

Protection & Privacy on Mobile Devices

Cell phones are a beacon tracking your exact location in real-time. You call and text messages can also be accessed by abusive partners.

- *Delete unnecessary apps on your phone*
- *Be wary of giving apps permissions (such as Contacts or Location)*
- *Use an encrypted messenger like Signal*
- *Use an Ad Blocker (Better for iOS, Adblock Plus for Android)*
- *Use a passcode on your phone- not Face ID*

Erasing Information from Online Data Brokers

A lot of your personally identifiable information (PII) is available online for two reasons.

Data brokers (Spokeo, Mylife, Intelius, Acxiom, BeenVerified, Lexis Nexis, TruePeopleSearch) harvest your information. Opting-out individually takes time and diligence.

Social media encourages people to share unsafely. Don't geotag your images. Turn up your privacy settings, and delete old posts from time-to-time.

LIBRARY FREEDOM PROJECT EST 2015

Learn new ways to protect your privacy at
https://libraryfreedom.org