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

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.

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

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

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

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

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

- Protection & Privacy on Mobile Devices
- Erasing Information from Online Data Brokers

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

Red Flags of Social Engineers and Abusers

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.

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

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.