DIGITAL SAFETY PLANNING

These 7 steps are designed to improve the digital health and safety of anyone at risk of being harmed online or via technology.

1 USE A SAFE DEVICE

What: If possible, safety plan from a safe device unknown to the attacker.

Concern: Safety planning steps could be exposed on a compromised device.

How: Use a device or computer belonging to a friend, the organization assisting you, etc.

2 CHANGE PASSWORDS

What: Update passwords to each account listed on the Accounts Checklist.

Concern: Compromised passwords can provide unauthorized access to accounts.

How: Use passwords the other party can't guess. Try a password manager to create and store passwords like LastPass or 1Password. Or use a phrase or sentence.

3 2-FACTOR AUTHENTICATION (2FA)

What: A 2nd layer of security in addition to your password. Sends a code to your phone or device that must also be entered to log in.

Concern: If not enabled, a person can log in with only the victim's password.

How: Enable 2FA on each account. If possible, set it up for every time you log in. Links to guides below:

Apple Google Facebook Instagram

4 REMOVE TRUSTED DEVICES

What: These are devices that accounts like Apple and Google recognize and trust.

Concern: Trusted devices won't require 2FA.

How: Log in to Apple or Google to view and remove any devices the victim doesn't trust.

5 LOG OUT OF ALL DEVICES

What: Attacker's device(s) may be still be logged in to victim's accounts.

Concern: Attacker can monitor or make changes to the victim's accounts.

How: Apple & Google allow you to log out all devices.

6 UPDATE CONTACT INFO

What: Email address & phone numbers where security notifications, 2FA codes & password reset links are sent.

Concern: Attacker may change a victim's contact info to a phone number or email they control.

How: Verify & update contact info for all accounts.

7 SECURITY QUESTIONS

What: Password reset questions & the attacker may know the answers.

Concern: The ability to reset a victim's password even after they change it.

How: Don't answer honestly. Change answers to something incorrect.