CYBER SAFETY IN DATING RELATIONSHIPS

Computers, tablets, and smartphones store personal information, including email and social media accounts, calendars, and even biometric data such as fingerprints and facial scans. While this technology makes our daily lives convenient, abusers and stalkers can use this information to monitor, control, and harass victims. This guide outlines steps you can take for safer use of your accounts and devices if you are in an abusive relationship.

SAFETY TIPS

- Password protect your devices and accounts so no one but you can access or make changes to them. Do not share your passwords with anyone.
- Change passwords frequently, choosing sequences that are not easy to guess. Use a mix of numbers, letters, and symbols.
- Turn off GPS location sharing in your device's settings.
- Turn off location settings for all social media accounts so your posts do not reveal your location. Do not "check in" to places and events.
- Create a new email account and do not share the password with anyone.
- Clear internet data (browser history, cookies, stored passwords) regularly.
- Use "SOS" phone settings for quick access to emergency services like 911.
- Check for spyware; if you suspect your device has spyware installed, do not use it for searching the internet or communicating about your safety or situation.

Social media has the awesome power to connect people across the globe. Social media can also unfortunately be used by abusers to track victims. The following tips can make your use of social media more private, and ultimately safer.

If you are being abused or are in transition, ***consider suspending or deleting your social media accounts*** altogether until you are in a safer situation. Talk to an Interval House advocate about best practices.

RULES OF THE ROAD FOR SAFER SOCIAL MEDIA

- Password protect all devices you use to access social media. Lock your screen when not in use.
- Change your app passwords frequently and enable two-factor authentication. Sign out when not using the apps.
- Block the accounts of anyone else who makes you feel unsafe.
- Consider changing your account name and profile picture to something an abuser will not recognize.
- Set your account to "Private" so you are able to approve or deny users and limit incoming messages to followers only. Don't accept messages from people you don't know IRL.
- Report any threatening content aimed at you to TikTok and tell a trusted adult what is going on.
- Disable location services for all social media apps. Do not "check in" to events or places that will reveal your location. Do not post pictures or videos that reveal your location (pay attention to the background of your images).
- Turn off any functions that allow other users to find you using your mobile number.
- Routinely check for security updates to all social media apps you use.
- If you think your account has been hacked, immediately change your password and report it to the social media platform.

INTERVAL HOUSE
working to end domestic violence