Technology Safety Plan

Understand that there is no way to go unmonitored on the internet or on your cell phone.It should be noted that experienced hackers and IT engineers may be able to access the location of a device, even when it is turned off in the settings. If your perpetrator has an IT background, there can be additional challenges to tech safety depending on their skill.

Trust your instincts. Abusers, stalkers, and perpetrators are often very determined to maintain control over their victims, and technology is one of many tools they use to do this. If it seems like the person knows too much about you, they could be getting that information from a variety of sources, like monitoring your devices, accessing your online accounts, tracking your location, or gathering information about you online.

Strategically plan around your tech. When abusers misuse technology, it's often a natural reaction to want to throw away devices or close online accounts to make it stop. However, some abusive individuals may escalate their controlling and dangerous behavior if they feel they've lost access to the victim. So before removing a hidden camera that you've found, or a GPS tracker, think through how the abuser may respond and plan for your safety. For example, some survivors choose to use a safer device for certain interactions, but also keep using the monitored device as a way to collect evidence.

Check your cell phone settings. If you are using a cell phone provided by the abusive person, consider turning it off when not in use. Also many phones let you "lock" the keys so a phone won't automatically answer or call if it is bumped. When on, check the phone settings; if your phone has an optional location service, you may want to switch the location feature off/on via phone settings or by turning your phone on and off.

Consider using a safer device. If you think that someone is monitoring your computer, tablet, or mobile device, try using a different device that the person hasn't had physical or remote access to in the past, and doesn't have access to now (like a computer at a library or a friend's phone). This can hopefully give an option for communication that cannot be monitored by this person.

Create a new email account. If you suspect that anyone abusive can access your email, consider creating an additional email account on a safer computer. Do not create or check this new email from a computer your abuser could access, in case it is monitored. Use an anonymous name, and account, and do not provide detailed information about yourself.

Change passwords & pin numbers. Some abusers use victim's email and other accounts to impersonate and cause harm. If anyone abusive knows or could guess your passwords, change them quickly and frequently. Think about any password protected accounts - online banking, voicemail, etc.

Minimize use of baby monitors. If you don't want others to overhear your conversations, turn baby monitors off when not in use.

Get a private mailbox and don't give out your real address. When asked by businesses, doctors, and others for your address, have a private mailbox address or a safer address to give them. Try to keep your true residential address out of national databases.

Make a list of all devices. (e.g. laptop, cell phone, Fitbit, AirTags, home security system, smart car, Internet-connected devices, Siri/Alexa, Bluetooth-connected sound systems, etc.) and accounts (e.g. social media, email, online shopping, online food services, transportation apps, cloud accounts, fitness trackers, games, etc.).

Change the password to your home Wi-Fi.

Security questions on accounts. Make up fake answers or do not use questions that the perpetrator would be able to guess; otherwise, they may be able to access the account (e.g. instead of using your mother's maiden name, make up an answer when they ask for your mother's maiden name and answer with something different. Just make sure you will remember your fake answer).

Turn off all automatically saved passwords on all devices and accounts.

Sign out of all accounts and devices when not using them.

Two-factor authentication. Use on any app or account that allows for it. Two-factor authentication requires you to enter a password that is sent to your phone or email to confirm that it is actually you accessing the account.

Cameras. Cover on all your devices' cameras when you are not using them.

Delete. Remove previously-stored location history, especially before and after arriving at domestic violence shelters or other safe spaces.

Do not post photos. Photos on social media containing metadata or background information that could alert the user to your location. One way to remove location-based metadata on a photo is to take a screenshot of the photo and post the screenshot rather than the original photo that contains the metadata.

Check accounts. Last Account Activity or Account Activity to see if any unusual IP addresses are accessing the account.

Spyware. If you are concerned that the perpetrator may have installed spyware on your devices, you may want to have an IT specialist or law enforcement check the device for spyware. Remember that if spyware is installed on the device, the perpetrator may be able to see whatever is being done on the device, which may escalate the abuse.

Signs that a device may have spyware on it:

- Device running slowly
- Battery draining
- Data being used up
- Device getting hot
- Device lighting up when not in use
- Clicks or odd sounds on calls
- Takes a long time to shut down

Keep your devices' operating systems up to date. These updates often patch any insecurities found on the software that hackers could misuse and spyware. Double-check your privacy settings after an update to make sure the update did not change any of them.

Consider replacing devices entirely. If you decide to do this, you should not back up your devices from previous devices. This may transfer any spyware installed on the previous device.

Look for hardware such as key loggers.