



Survivors' Guide to Phones: Increasing Privacy & Responding to Abuse

Our smartphones store sensitive information, track location, and are how we access our personal accounts. It's incredibly important that survivors of abuse have the tools to increase privacy and respond to tech abuse. Here are some steps and considerations for survivors.

Prioritize Safety

Use a safer device. If you think that someone is monitoring your phone, use a different device that the person cannot access (and that they have not had access to in the past) such as a computer at a library or a friend's phone.

Get more information. Navigating violence, abuse, and stalking can be difficult and dangerous. Advocates can help you figure out options and local resources and help you create a plan for your safety. You can [contact a national helpline](#) to be connected with local resources.

Part 1: Is Your Phone Being Used Against You?

Unfortunately, conversations and information on phones can be misused to monitor, stalk, control, or harass. *Trust your instincts.* If you suspect that someone is monitoring your phone, but you're not sure, you can [read more about how to figure out what's going on](#). Meanwhile, here are some questions to consider.

Is there a pattern?

Does the person seem to know everything—who you've spoken to, the content of conversations you've had either on your phone or near your phone, texts you've written and received, where you go—or just pieces of that information?

Narrowing the possibilities of how your activities are being tracked will help you determine how you are being monitored, and which safety strategies to consider.

What does the person seem to know?

If the person knows that you had a conversation, but not specifically what you said, wrote, or shared, then they may be looking at your call log, billing records, or other account information. They also could have talked with the other person you were communicating with.

If the person knows the content of your messages, then they may be using other devices that are linked to your accounts, monitoring your device, or the other person shared or forwarded the messages.

If they know the content of voice or video conversations, but they were not nearby to simply overhear the conversation, and they weren't told of the conversation by the person you were speaking with, then they may be using stalkerware. **Caution:** anything you do on the phone, including looking up information or looking for the stalkerware could likely be seen. [Read more about stalkerware](#) on a safer device.

Has the person monitoring you had access to your phone?

Most monitoring requires physical access to the phone. The person might regularly scroll through the phone to see who called and texted you or may have installed stalkerware on the phone allowing them to view your activity from another phone or computer. With physical access to your phone, they could also download apps or change account and security features to make your phone more vulnerable.

Does the person have access to your online or cloud account?

Another way someone can monitor your phone use is if they have access to your account with the phone company and/or the cloud account your phone is linked to (Google or Apple). If their name is on the phone account or they can convince the phone company they are you or an authorized account holder, they may have

the ability to turn on features such as location services or access your billing records online and see your call logs and other information.

Do they know your location?

Phones and apps can share your location. Check the settings on your phone and in apps to limit location sharing. Most phones also have a feature to help you find a lost phone which can reveal your location if the other person has access to your phone or account. Learn more about [Location Tracking](#) beyond phones.

Are you concerned about spyware?

[Read more about stalkerware](#) on a safer device.

Part 2: If Your Phone is Being Monitored

There are steps you can take to secure your phone, apps, and accounts. There isn't one "right" way to respond. What works for someone else may not work or be safe for you.

CAUTION: Making changes will often alert the other person. They might force you to unlock your phone or share your passwords. They might become more abusive. Making changes might also erase evidence.

1. Reset Phone & Accounts.

- Doing a factory reset of the phone may uninstall any stalkerware that was installed without your permission or knowledge. It would be important to avoid reconnecting the device with a backup, however, so the stalkerware wouldn't be reinstalled.
- You can also uninstall any unfamiliar apps and check for apps and settings that are allowing location sharing. Call your cell phone provider to make sure that no other location sharing service is enabled.

- Reset passwords on phone billing, cloud, and other connected accounts to remove any possible access the person might have.

2. Replace your current phone. If you are able to, and you feel safe, you could replace your phone or set up a second phone. Here are a few options:

- Purchase a new phone, and consider switching carriers and getting a new phone number. Ask if there are additional security you can set up for your account, such as asking the company to note in your account that you are the only authorized account holder or set up notifications if changes are made to your account, including adding or removing features.
- Purchase a pay-as-you-go phone with cash.
- Depending on your income or circumstances, you may qualify for discounts on phones or service. An example is the Lifeline program, which offers a discount for individuals who qualify as low-income.
- A trusted friend or family member might be able to give you an old phone. Be sure to wipe the phone's memory and do a "factory reset" to remove any of their information from the phone.

Important: Don't connect the new phone to any old accounts, especially cloud accounts like Google or iCloud, and don't use your old number. Don't move data from your old phone to the new phone using a memory card, SIM card, your cloud account, or backups. Doing so could reinstall stalkerware.

2. Strategize about the monitored phone. Some abusive people may escalate their abuse when their access and control are cut off. You can reach out for help with safety planning. You may also want to keep the monitored phone for evidence. If you keep the phone, decide how you will store it. You could turn it off, remove the battery, or cover it in foil. Remember that once you turn the phone back on, your location will be visible if someone is monitoring your location through the cell signal or the WiFi. You may also consider keeping the

phone on and use it strategically to prevent raising the suspicion of the abusive person. These are all options to consider and to talk through with an advocate.

- 3. Talk to friends and family.** Family and friends can inadvertently share your location, who you're talking to, or what you're doing through social media posts or with other people. If you have children, teach them how to avoid sharing your location or information about your personal activities.
- 4. Document what is happening.** You can document what is happening, if it feels safe, by taking screenshots and creating a log of what's happening before you make any changes. You have the option to share this with law enforcement, an attorney, or save it for later. Documenting the abuse can also help you make or update a safety plan. Read more about [Documenting Abuse](#).

Part 3: Ways to Increase Safety & Privacy

- 1. Put a passcode on your phone.** Most phones ask for a 4-digit passcode, but some will allow you to set up a more complex passcode, a pattern, or a biometric lock using your fingerprint or facial recognition. If you're not able to put a passcode on your phone or the abusive person demands that you share your passcode, consider borrowing someone else's phone to look up safety information or to [call a hotline](#).
- 2. Secure your phone's online accounts.** Phones usually have an online account with the phone company and a cloud account to store personal data (most likely a Google or iCloud account). Review the security settings and consider changing passwords to your phone and cloud accounts to ensure that someone else can't access your information.
- 3. Use anti-virus and anti-spyware software on your phone.** You can research reputable programs online and find them in app stores. Many have free

versions and the services can protect against stalkerware and other malicious apps from being downloaded on your device.

- 4. Turn off location sharing.** Phones have built-in GPS that can pinpoint your location and some phones and apps give you the option to share that information. You can manage your location sharing within the phone settings, where you can choose which applications can access your location or you can turn off the location sharing altogether. Some apps let you manage your location sharing within the app's settings as well.
- 5. Check your privacy & security settings.** Most phones have settings that will help you manage your privacy and security. You can find these controls through the phone settings or app settings. For more information, read [Online Privacy & Safety Tips](#), and check out our guides on [Facebook](#) and [Twitter for more information about their privacy and security settings](#).
- 6. Log out of apps and accounts.** Consider logging out of accounts so that others can't access them if they have access to your phone. You might not be able to log out of some apps without removing them from your phone. It may be more inconvenient to access the account through the browser instead, but make your decision based on your own privacy and safety risks.
- 7. Review downloaded apps.** If you find an unfamiliar app on your phone, delete it. Apps are easy to download and easy to forget, and some apps could be gathering your private information. However, be cautious before removing an app if you're worried it may be spyware or stalkerware. [Read more about spyware](#) on a safer device.
- 8. Avoid unlocked or "jail-broken" phones.** Removing the manufacturer and phone carrier's restrictions makes these phones more vulnerable to spyware

and malware. Knowing if your phone has been unlocked or “jail-broken” can also be a clue to whether or not someone may have installed a monitoring app on your device.

- 9. Use virtual phone numbers.** Consider using a virtual phone number, which will allow you to screen calls, receive voicemails, and make calls or send texts without sharing your device’s phone number. Virtual numbers can be linked to a cloud account, for example Google Voice, so be sure that online account is also secure.
- 10. Try not to store sensitive information on your phone.** The less sensitive information you have on your phone, the less likely someone else can access it. You may want to delete certain text messages or voicemails from your phone and from connected cloud accounts (like Google or iCloud).
- 11. If you’re considering a safety app...** There are many “personal safety apps” available that offer to increase users’ personal safety; some are developed or advertised specifically for survivors of violence. [Read more in our App Safety Center](#) about how to figure out if these apps are right for you.

© 2021 National Network to End Domestic Violence, Safety Net Project. This product was supported by cooperative agreement number 2019-V3-GX-K017, awarded by the Office for Victims of Crime, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this product are those of the contributors and do not necessarily represent the official position or policies of the U.S. Department of Justice. We update our materials frequently. Please visit TechSafety.org for the latest version of this and other materials.