Technology Safety Plan
A Guide for Survivors and Advocates

This document contains general information about safety planning with victims of domestic and sexual violence, stalking and trafficking in situations of technology abuse. As an overview, this document provides general tips and suggestions. For more specific safety planning strategies, please consult one of our safety planning guides to a particular technology or situation and please contact a local victim advocate who can help you with a more thorough safety plan.

Trust your instincts. If you suspect that the abusive person is harassing, stalking, or monitoring you using technology, it is possible and likely. Abusers, stalkers and perpetrators can be incredibly persistent and creative in maintaining control and technology is another tool for them to misuse.

Get more information. Navigating violence, abuse, and stalking is very difficult and dangerous. Work with a victim advocate to discuss your options and to help you plan for your safety. You can call the National Domestic Violence Hotline at 1-800-799-7233, the National Sexual Assault Hotline at 1-800-656-4673, or the National Human Trafficking hotline at 1-888-373-7888.

Look for patterns to identify misused technology. Carefully try to figure out how or which technology is being used to harass, stalk, or monitor you. For example, if you suspect you’re being watched, is it in a particular room in your house? If you suspect you’re being followed, is it just when you’re in your car or wherever you go? Narrowing down the potential source of technology will help you create a more precise safety plan.

General safety tips. If it seems like the person knows too much about your activity, it could be from a variety of sources. The abuser could be monitoring your computer or cell phone. The perpetrator could be accessing your online accounts or gathering information about you online. Or the stalker could be monitoring your location.

Use a safer computer/device. If you suspect that the abusive person is monitoring your computer activities try using a safer computer, tablet, or device to prevent the abusive person from seeing what you’re doing.

Change passwords and usernames. Change the usernames and passwords of your online accounts on the safe computer. Don’t use the new username and password on the computer that is being likely monitored. Consider creating brand new accounts, such as a new email address. Also consider using a non-identifying username instead of your actual name and don’t use the same password for your accounts.

Check your cell phone settings. Go through your phone’s settings to ensure that other devices aren’t connected to the phone and that Bluetooth and location access is limited or turned off. If your phone allows apps to be downloaded, make sure you know what each of the apps do; if you don’t use it or don’t know what it is, delete the app. Pay attention to excessive battery or data usage as that may indicate that a program may be in use on your phone constantly. Call your phone carrier to ask about location settings or third-part applications.
Get a new cell phone. If you suspect that your cell phone is being monitored, the safest thing is to get a new phone with an account that the abusive person doesn’t have access to. A pay-as-you-go phone is an inexpensive alternative. Put a passcode on your phone and ensure that location settings and Bluetooth settings are turned off.

Have your car checked. If the abusive person knows where you are whenever you are in your car, you may consider having your car checked for hidden location devices. Ask a trusted mechanic or law enforcement to check the car thoroughly.

Limit the information you give out about yourself. Most things we do these days asks for personally identifying information—whether it is to make a purchase, open a discount card or create an account. Limit the information that you provide since you don’t know who else they will share your information.

Get a P.O. Box or inquire about Address Confidentiality Programs. If you’re concerned about someone knowing your actual address, you can open a private mail box or if your state has an address confidentiality program, check to see if you can be a part of that program. (Note that this is most helpful if you have recently moved or the abusive person doesn’t already know your address.)

Hidden cameras. If you suspect cameras in your home, figure out where the camera is hidden based on the information shared by the abusive person (for example, the abusive person seems to know details of what you’re doing when you’re in the living room) or gifts to you or members of your household from the abusive person. Some camera detectors may be helpful in locating the cameras, but remember that some detectors will only locate wireless cameras or wired cameras. Either remove the camera or, if that may be dangerous, limit what you do in the room that is being monitored. If your computer/tablet has a built-in web camera, consider disabling the camera when you aren’t using it. Or you can cover the camera with a piece of removable tape.

Document the incidences. If possible, document the stalking or harassing behavior. Check out NNEDV’s stalking log for an example. Sometimes, a harassing or stalking incident by itself may seem minor. But a series of incidences will show a pattern of behavior that can be proved as criminal stalking or harassment.

Report the incidences. If you feel safe in doing so, report the incidences to law enforcement and ask for a police report. If the harassing behavior is online, report it to the website. Many sites have links where you can report abusive content.

Think about your safety. Oftentimes, many victims want to stop the abusive behavior by getting rid of the technology. However, for some abusive individuals, this may escalate their controlling and dangerous behavior if they feel their control is threatened and you are removing all access. Think about what may happen if you remove the camera or the GPS. Incorporate that into your safety planning. For example, some survivors choose to use a safer computer, device or phone, but not disabling to the monitored device to continue collecting evidence.