Technology Safety Plan
A Guide for Survivors and Advocates

Prioritize Safety

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.

Get more information. Navigating violence, abuse, and stalking can be very difficult and dangerous. Victim advocates in your area can tell you about options and local resources, and help you create a plan for your safety. You can call the National Domestic Violence Hotline at 800-799-7233, the National Sexual Assault Hotline at 800-656-4673, or the National Human Trafficking hotline at 888-373-7888 to be connected with an advocate near you. More information about technology, harassment, and abuse is in our Survivor Toolkit at TechSafety.org.

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.

Identify the Abuse

Look for patterns. Take some time to think through what kind of technology may being used to stalk, monitor, or harass you. For example, if the abusive person has hinted that they are watching you, think about what they know. Do they only know what you are doing in a certain area of your home? If so, there may be a hidden camera in that room. If you suspect you're being followed, is it just when you're in your car or is it also when you are on foot? If it's just in your car, then there may be a device hidden in your car. If it's everywhere, it may be something you are carrying with you, such as your phone or a tracker in your bag. Narrowing down the potential source of technology can help you create a safety plan and to document the abuse. Read more about Assessing for Technology Abuse.

Document the incidents. Documenting a series of incidents can show police or the court a pattern of behavior that fits a legal definition of stalking or harassment. Documentation can also help you see if things are escalating, and help you with safety planning. For more information, check out our Documentation Tips for Survivors.

Report the incidents. You may also want to report the incidents to law enforcement or seek a protective order. If the harassing behavior is online, you can also report it to the website or app where the harassment is happening. If the behavior violates the platform's terms of service, the content may be removed or the person may be banned. It's important to recognize that reporting content may remove it completely so it should be documented prior to reports for evidence.

Steps to Increase Security

Change passwords and usernames. If you think your online accounts are being accessed, you can change your usernames and passwords using a safer device. Once you've updated the account information, it's important not to access those accounts from a device you think is being monitored. You can also consider creating brand new accounts, such as a new email address with a non-identifying

username instead of your actual name or other revealing information. It's important to not link these new accounts to any old accounts or numbers, and not to use the same password for all of your accounts. Read more tips about Password Safety.

Check your devices & settings. Go through your mobile device, apps, and online accounts, and check the privacy settings to make sure that other devices or accounts aren't connected to yours, and that any device-to-device access, like Bluetooth, is turned off when you're not using it. Make sure you know what each of your apps are and what they do. Delete any apps on your device that you're unfamiliar with or that you don't use. Look for spikes in data usage – these may indicate that monitoring software such as spyware may be in use.

Get a new device. If you suspect that your actual device is being monitored, the safest thing may be to get a new device with an account that the abusive person doesn't have access to. A pay-as-you-go phone is a less expensive option. Put a passcode on the new device, and don't link it to your old cloud accounts like iCloud or Google that the person might have access to. Consider turning off location and Bluetooth sharing. You also might keep the old device so that the person thinks you are still using it, and doesn't try to get access to the new device.

Protect your location. If the person seems to always know where you are, they might be tracking you through your mobile device, your vehicle, or by using a location tracker. You can check your mobile devices, apps, and accounts to see if location sharing is turned on, and update the settings to best suit your needs. You can also call your mobile phone provider to ask if any location sharing services are in use, especially if you were/are on a family plan with the person. Location tracking through your car might be through a roadside assistance or safe driver service. If you are concerned about a hidden tracking device in your car or other belongings, a law enforcement agency, private investigator, or a car mechanic may be able to check for you. It's important to safety plan and document evidence before removing a device or changing an abusive person's access to your location information.

Consider cameras and audio devices. If you suspect that you're being monitored through cameras or audio recorders, it may be happening through hidden devices, gifts received from the abusive person, or even everyday devices like webcams, personal assistants (such as Google Home or Alexa), or security systems. If you're concerned about hidden cameras, you may consider trying a camera detector, though some will locate only wireless cameras, not wired cameras, or vice versa. Everyday devices or gifts may be able to be secured by changing account settings or passwords. Built-in web cameras can be covered up with a piece of removable tape (although this only addresses the camera, not the spyware on the computer). Remember to consider making a safety plan and documenting evidence before removing devices or cutting off an abusive person's access.

Steps to Increase Privacy

Protect your address. If you're concerned about someone finding your address, you might 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.) Tell friends and family not to share your address, and be cautious around giving it out to local business. Also, look into what information is public in your state if you were to purchase a home so you know your options.

Limit the information you give out about yourself. Most everything we do these days asks for personally identifying information—whether it's to make a purchase, open a discount card, or create an online account. The information we provide is often sold to third parties, and later ends up online in people-search engines and with data brokers. When possible, opt out of information collection, or only provide the minimum amount necessary. You can get creative – for instance, instead of using your first and last name, use your first and last initials. You can also use a free virtual phone number, such as Google Voice, to give yourself an alternative number to share when you need to.

Control your offline & online privacy. Our Survivor Toolkit at TechSafety.org has Online Privacy & Safety Tips, including more information about changing settings on your mobile devices, social media accounts such as Facebook and Twitter, and your home WiFi network. Follow those steps to increase your privacy and decrease risks for an abusive person to misuse those technologies, locate you, or monitor your activity.

Supported by US DOJ-OVC Grant #2017-TA-AX-K015. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of DOJ. We update our materials frequently. Please visit TechSafety.org for the latest version of this and other materials.