TECHNOLOGY SAFETY PLAN: A GUIDE FOR SURVIVORS AND FRONTLINE WORKERS

techsafety.org.au

Please note that the contents of this document should not be regarded as legal advice. The information contained within is relevant as of January 2025.

This document contains general information, tips and suggestions about safety planning around technology abuse with victims of domestic and sexual violence, stalking, and trafficking. For more specific safety planning strategies, please consult one of our safety planning guides for a particular technology or situation, and speak with a local support worker, frontline worker or DFV practitioner 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 and stalkers can be incredibly persistent and creative in maintaining control, and technology is another tool for abuse.

Get more information

Navigating violence, abuse, and stalking is very difficult and can be dangerous. Work with a victim advocate to discuss your options and to help you plan for your safety. You can call 1800 RESPECT on 1800 737 732 or visit www.1800respect.org.au.

Look for patterns to identify misused technology

Take care to try to identify which technology is being used to harass, stalk, or monitor you. For example, if you suspect you're being watched, is it in one particular room? If you suspect you're being followed, is it just when you're in your car or is it all the time? Keep in mind that, rather than using expensive or highly technological methods, abusers usually opt for the cheapest and simplest ways to perpetrate tech abuse. Narrowing down the potential source will build your confidence in creating a solid safety plan.

General safety tips

If it seems like the person knows too much about your activities, it could be that the information is gleaned from a variety of technology sources. The abuser could be monitoring your computer or smartphone, accessing your online accounts or

gathering information about you online. In addition to physically stalking you, a stalker might be monitoring your location through devices, apps or online accounts.

Use a safer computer/device

If you suspect that the abusive person is monitoring your online activities, try using a secure Wi-Fi network, computer, or other safe device to prevent the abusive person from seeing what you're doing. If you don't have access to a secure Wi-Fi network or a safe device, then use non-tracking Incognito, In Private or Private browsers that don't store your browsing history, and consider using a reputable VPN (Virtual Private Network), a password-protected screensaver and a privacy screen protector, if it is safe to do so.

Change passwords and usernames

Change the login credentials of your online accounts on a safe device while using a secure Wi-Fi network. Make your new password a unique, long, and strong 'passphrase' and avoid logging into accounts on compromised devices or networks. Consider creating brand new accounts, such as a new encrypted email or chat service, then protect devices, accounts and apps with 2-step verification or multi-factor authentication, if it is safe to do so. Use non-identifying usernames and provide fake answers to security questions so that they cannot be easily guessed.

Check your smartphone settings

Go through your phone's settings to ensure that other devices aren't connected to it via subscriptions, in-built device apps or family sharing tools. Check that Bluetooth and location access is limited or turned off in 'Settings' and within individual app permissions. Familiarise yourself with each app downloaded on your phone; if you don't use it regularly or don't know what it is, uninstall it and delete the app. Take note of excessive battery or data usage, unexplained increases on your screen time reports, or your device acting strangely, as those issues may indicate a hidden program is running. Call your phone carrier to ask about location settings or third-party applications.

Get a new smartphone

If you suspect that your smartphone is being monitored, consider getting a secondary phone under a new account or a new provider that the abusive person won't have access to. A prepaid phone is an inexpensive alternative. Put a passcode or use biometric authentication for privacy, secure location services, Wi-Fi and Bluetooth settings, manually enter a few select contacts, and resist uploading compromised accounts or apps onto the new device.

Have your car checked

If the abusive person knows your whereabouts whenever you are in your car, it may be worth having it professionally swept for hidden tracking devices. Review your Bluetooth and Ultra-Wideband (UWB)-enabled device connections and ask a trusted mechanic or service to check the car thoroughly.

Limit the information you give out about yourself

Most things we do these days ask 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 and enter an email and password combination rather than use your Google or Facebook account to automatically log in - you don't know who else they may be sharing your information with. If available, use the 'Hide my email' function.

Get a PO Box

If you're concerned about someone finding out where you live, you can open a Post Office Box to protect your physical address. You can also apply to become a 'silent elector' on the electoral roll and request an unlisted/silent service option with your telco provider. These actions will reduce the risk of the abuser coming across your information.

Check for hidden cameras

If you suspect there are hidden cameras in your home, determine where they might be based on the information shared by the abusive person (for example, they may describe precise details of what you are doing or wearing when you're in a specific room). Look for out-of-place or new objects, and check things like smoke detectors, grills and light fittings. It can be expensive to have a home 'swept', but it may be possible to locate infrared cameras using a smartphone camera app, and some camera detectors can locate hidden cameras also. If a camera is located and it is safe to do so, you might choose to alert police to its whereabouts and have them remove it. Alternatively, you may limit what you do in view of it. You might consider disabling built-in cameras via the settings of computers, smart TV's and mobile devices, and powering off devices or pulling out wall plugs when not in use. Covering in-built camera lenses with removable tape can also provide some additional privacy when you cannot disable a camera.

Document the incidences

If possible, document the stalking or harassing behaviour in chronological order. You can record these details on a stalking log, a journal, or, if your device is not compromised, in an app developed specifically for this purpose. It can help to

record how the incident made you feel at the time too. Sometimes, a harassing or stalking incident by itself may seem minor; but a series of incidents will show a pattern of behaviour that can be proved as criminal stalking or harassment.

Report the incidences

If you feel safe in doing so, report the incidents to the police and ask for a police report. If the harassing behaviour is online, report it directly to the online platform too. Many sites have links where you can report online abuse.

Think about your safety

Oftentimes, many victims want to stop the abusive behaviour by getting rid of the technology. For some abusers, however, this may escalate their dangerous behaviour if they feel their power and control over the victim is threatened. Think about what may happen if you remove the smartphone, camera or the GPS tracker, and incorporate those risks into your safety planning. For example, some survivors choose to secretly use a safer computer, mobile device or new accounts while continuing to use the monitored devices or accounts to minimise the risk of the abuser's violence escalating.

Additional Resources

- Read Documentation Tips for Survivors of Technology Abuse and Stalking
- Learn more about creating a strong, secure password Password Safety
- Read Dealing with harassing calls, texts, and messages
- Consider using our Stalking and Technology-Facilitated Abuse Log
- Learn about Mobile Spyware
- Learn about Securing Your Home Wi-Fi Network/Router
- View our video on How to take a screenshot on a computer and smartphone
- Read about Increasing Privacy and Security when Using Google
- Review access to your iPhone using the Apple Safety Check Feature available on an iPhone with iOS 16 or later

Acknowledgement

This handout has been created by Wesnet under licence from the National Network to End Domestic Violence.