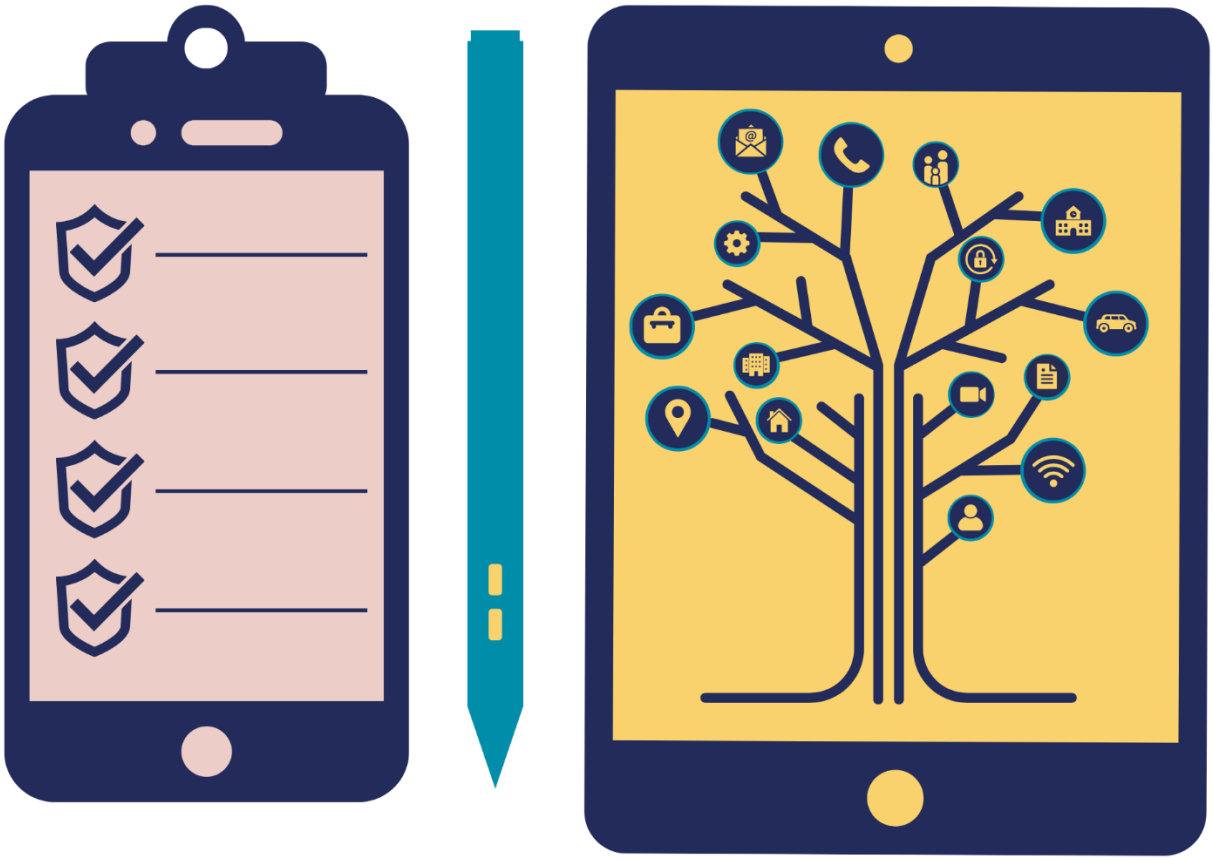
Tech Safety Planning Checklist



A safety planning process helps you think through:

- What is happening
- How you can stay safe
- What to do if the situation escalates
- Who to reach out to for additional support

Technology safety planning should always be done in tandem with more traditional safety planning. Online violence and offline violence are interconnected, and it is important to consider the non-technology-related risks that may be associated with actions you take to protect yourself online or on your devices.

This tech safety planning checklist walks you through various steps you can take to increase your safety online and when using your devices. Not all actions or sections will apply to every person's situation. You can review the checklist and identify the steps that will be most useful to you based on what you are experiencing and what will improve your safety. This checklist is meant to be an addition to a broader safety plan that considers other aspects of your life beyond technology.

Whenever you are safety planning with someone who has experienced technology-facilitated violence, it is important to note that the abuser may have access to their devices or accounts and may be monitoring their communication and movements via these devices and accounts. Making changes to any device, social media account, email, or other technology may alert the abuser that the survivor is seeking help and can trigger additional abuse. Extra safety planning precautions may need to be taken in these situations.

Table of Contents

Passwords 4

Blocking, Deleting, and Unfriending 6

Stalking, Tracking, and Monitoring 7

Alternate Accounts 12

Cloud Storage, Shared Accounts, and Unauthorized Access 12

Search History 13

Intimate Images 14

Google Alerts 16

Reporting Harmful Content to Social Media Companies 16

Software Updates, Firewalls, and Anti-Virus Software 16

Evidence Collection 17

APPENDIX A 19

Devices and Accounts to Consider 19

Passwords

- ☐ Make a list of all of your devices and accounts. **Note which of these the abuser has access to, knows the passwords to, or may know the passwords to.**
    - Devices can include: laptop, cell phone, Fitbit, AirTags, home security system, smart car, Internet-connected devices, Siri/Alexa, Bluetooth-connected sound systems, etc.
    - Accounts can include: social media, email, online shopping, online food services, transportation apps, cloud accounts, fitness trackers, games, etc.
    - See appendix A for a list of potential accounts.

- ☐ Think about what information is included on those accounts. If your former partner has access to your password, they may be able to view information you do not want them to have access to.
    - ***Example:*** *Home address, phone number, email address, credit card information, personal messages, Internet search history, communication about safety planning, etc.*

- ☐ Change all passwords to unique passphrases that the abuser would not be able to guess. Use a different, long password or passphrase for each account.

- Avoid using things like the names of children or pets, important dates, old addresses, or old phone numbers.

- ☐ When you have to create a password, aim for at least 15 characters. A passphrase made from several unrelated words like “tree-sun-happy-glass" can be easier to remember and harder to guess.

- ☐ Do not reuse the same password for multiple accounts. A password manager can create and securely store different passwords for you. Before using one, consider whether the abusive person has access to the device or account where the password manager is stored.

- ☐ Change the password to your home Wi-Fi.

- ☐ For account security questions, make up fake answers or avoid questions the abuser could guess; otherwise, they may be able to access the account.

    - ***Example:*** *Instead of using your mother’s actual maiden name, make up an answer when they ask for your mother’s maiden name.*

- ☐ Make sure you remember your fake answer or record it somewhere the abuser can’t access.

- ☐ Review where your passwords and passkeys are saved and whether they are syncing to any devices or accounts the abusive person can access.

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

- ☐ Review the devices and active sessions signed in to your important accounts. Sign out of devices or sessions you do not recognize or no longer use, but consider your safety before removing a device if the abusive person may notice the change

- ☐ Use two-factor authentication on any app or account that allows for it.

- ☐ Turn on two-factor or multi-factor authentication (2FA/MFA) when it is available. It adds another way of confirming it is really you signing in. Depending on the account, this might use an authenticator app, passkey, security key or a code sent to your phone.

- ☐ Do not use social media accounts to sign in to other accounts

    - ***Example:*** *"Sign in with Facebook" or "Sign in with Google" options.*

- ☐ Remove the abuser's email addresses or devices from shared accounts and as Trusted Devices on your accounts.

Blocking, Deleting, and Unfriending

- ☐ Consider blocking or unfriending the abuser's email address, phone number, or social media profile.

    - Ensure that you have collected all the evidence needed from those accounts before doing this. Certain programs will delete or

not allow you to access conversations and information from the other person's account once they have been unfriended, blocked, or deleted from your account.

- ☐ When deciding to block, delete, or unfriend someone, consider whether this may escalate the abuse.

- ☐ There may be benefits to having access to the abuser's social media (such as knowing their location) that are worth considering.

- ☐ Consider which of your friends and family may have the abusive person as a "friend" on their accounts.

    - Ask friends and family not to post information about you or photos of you online and not to share information with the perpetrator.

Stalking, Tracking, and Monitoring

- ☐ Use a camera cover on all your devices' cameras when you are not using them.

- ☐ If the abuser is tracking your device or accounts, consider using a different device to look up information, connect with resources, and plan changes to your devices or accounts.

    - ***Examples of different devices you could use:*** *a friend's computer, a work device, or a computer at a library.*

- ☐ Consider what personal information is posted online and decide whether to delete that information or make it private.
    - ***Examples of personal information that might be online:*** *home address on a birthday event invitation, phone number in a Facebook post, or a new workplace on LinkedIn, etc.*
        - *Remember that other people could share that information with your perpetrator even if you have blocked them from your accounts.*
- ☐ Turn off or limit the location functions on your devices when not in use.
- ☐ Turn off location functions like Find My.
- ☐ Delete previously-stored location history, especially before and after arriving at domestic violence shelters or other safe spaces.
- ☐ Do not "check-in" to locations on social media.
- ☐ Change your privacy settings on apps and social media to limit who can see your posts, location, personal information, friends or followers, and online activity. Review who currently has access and remove people you do not know or trust.
- ☐ Before changing privacy settings or removing someone's access, consider whether they may notice the change and how they might react.

- ☐ Do not post 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.
- ☐ Remove the abuser's email addresses or devices from shared accounts and remove their device from Trusted Devices on all your accounts.
    - See Appendix A for potential accounts.
- ☐ Check accounts for Last Account Activity or Account Activity to see if any unusual IP addresses are accessing the account.
- ☐ If there is concern that the abuser has access to your accounts, consider using a P.O. Box for an address on online accounts and deliveries.
- ☐ Consider the risk of the perpetrator accessing credit card information or misusing the account if they have access.
- ☐ Untether your phone or other devices from the perpetrator's devices
    - ***Example:*** *Bluetooth stereo in their car or home, fitness notifications to their smartwatch, etc.*
- ☐ Search belongings (e.g. purses, cars, jackets) for GPS tracking devices or other recording devices.

- ☐ Examine any gifts or unusual items in the home, including children's items, for hidden cameras or recording devices.

- ☐ Consider what information is on your children's devices and accounts (e.g. phones, video game systems, social media accounts) and what may be shared with the abuser.

- ☐ Consider whether the abuser may have access to any home security system information, such as access to the cameras or information when people are leaving or entering the home.

- ☐ Consider using a device or program (e.g. network scanners, port scanners, RF signal detectors) that can detect certain hidden cameras to scan your Wi-Fi or home.

- ☐ Look through apps on your phone and delete any unfamiliar ones.

- ☐ If you are concerned that the abuser 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.

- ☐ The Clinic To End Tech Abuse also has resources to help identify spyware on a device.

    - 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 in the software that hackers could misuse.
    - 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, as this may transfer any spyware installed on the previous device.

- ☐ Look for unusual hardware attached to desktop computers.

    - ***Example:*** *Key loggers are often attached between the keyboard and the desktop.*

- ☐ It should be noted that experienced hackers and IT engineers may be able to access the location of a device, even when this feature is turned off in the settings.
    - If your abuser has an IT background, there can be additional challenges to tech safety depending on their skill.
    - You may want to speak with an IT specialist or law enforcement if this is the case.

Alternate Accounts

- ☐ If the abuser has access to your accounts and there is no safe way to remove their access at this moment (e.g. if removing their access will escalate the risk or violence), create an alternate email account or social media account that the abuser does not know about or have access to for sensitive communication.

- ☐ Do not sign into any new accounts on your compromised personal or shared devices.
    - Use a work computer, library computer, or friend's computer to access it.

Cloud Storage, Shared Accounts, and Unauthorized Access

- ☐ Remove the abuser from any shared accounts, devices, or plans if it is safe to do so.

- ☐ Remove Bluetooth connections from the perpetrator's devices.

    - ***Example:*** *if you are connected to their home stereo, car, etc.*

- ☐ Consider what content is being automatically uploaded or connected and whether the abuser could gain access to these accounts or information.

    - ***Examples:*** *Calendars, iCloud storage for photos and texts, Fitbit, smart watches.*

- ☐ Remove all devices except your own devices from Trusted Devices on all accounts.

- ☐ Check 'Last Account Activity' on all accounts to see if an unusual IP address or device has been accessing the account.

Search History

- ☐ If the abuser has access to your device or account, they can check your search history.

- ☐ If you are looking for help or resources, use a computer that is not in the home and that they do not have access to.

- ***Example:*** *A public computer, a friend's computer, or a work computer.*

- ☐ Selectively delete Internet search history. Remove sites that could reveal your plans or location, or that you are seeking out support or planning to leave. Leave other sites in the history to avoid raising suspicion.

- ☐ Use "private" or "incognito" options so the search history is not being recorded.

- ☐ Turn off cookies in the browser settings.

Intimate Images

- ☐ Make a list of images and videos that may exist.

- ☐ Consider using StopNCII.org to prevent other people from uploading sexual images that have been registered and "hashed" with the company.

- ☐ If safe to do so, ask your former partners to delete any intimate images after the relationship ends and tell them that there is no consent to share them. Document this communication.

- ☐ Consider whether the abuser may have been able to capture images without consent.

    - ***Example:*** *hidden camera, screen capturing sex via apps.*

- ☐ Do a reverse image search on Google for images.
- ☐ Search common pornography sites for your name.
    - People are often doxed and named when their images are shared.
- ☐ Set up a Google alert for your name, as this can help alert you when your name is mentioned online if it is posted along with your images.
- ☐ Consider alerting family, friends, and co-workers who may receive the images to reduce the harm.
- ☐ If the image has been shared without consent, see the Cyber Civil Rights Initiative guide for information on getting content taken off the Internet.
- ☐ Report to social media companies or porn companies, as most have policies that forbid non-consensually shared nude images.
- ☐ If images have been released, consider using a reputation service to help get the content removed.
- ☐ If sharing intimate images in the future, consider harm reduction strategies:
- ☐ Avoid images with your face or identifying marks (e.g. tattoos, birthmarks).

- ☐ Avoid images in places that are identifiable (e.g. a recognizable room).
- ☐ Use programs like Signal that allow for disappearing messages.

Google Alerts

- ☐ Set a Google alert for your name so you are notified when your name appears online. This will not find all places where your name is posted, but can alert you to some instances.
- ☐ Make a Google alert for all versions of your name (e.g. Victoria Chan, Vickie Chan, Vicky Chan)

Reporting Harmful Content to Social Media Companies

- ☐ Gather evidence (e.g. screenshots) of the harmful content before reporting, as it may be deleted by the social media company if it violates their policies.

Software Updates, Firewalls, and Anti-Virus Software

- ☐ Update your software regularly.
    - This includes your mobile phones.

- These updates often patch any insecurities found on the software that hackers could misuse.

- ☐ Enable firewalls and anti-virus software on all devices.

Evidence Collection

- ☐ Create a log of all experiences of technology-facilitated violence and include information such as the time, date, abuser, evidence gathered, and other useful information.

- ☐ See WSC's Sample Technology-Facilitated Violence Log.

- ☐ Take screenshots or make recordings of abuse.

- ☐ Consider whether the app alerts the other person if someone else takes a screenshot.

    - If it does, it may not be safe to screenshot and it may be better to take a photo or video of it with a second device.

- ☐ Ensure you include the profile and other identifying information about the abuser in the evidence.

- ☐ Ensure it shows the date of the abuse.

- ☐ If the abuse is happening via email, keep the original email as it contains metadata such as the IP address of the sender.

- ☐ If the abuse was posted by someone else, capture it before they have a chance to delete it.

- ☐ Store copies of the evidence in a secure location that the abuser cannot access. Back up the information in at least one other location.

- ☐ If the abuser has access to the device or cloud storage where the evidence is stored, they could delete the evidence.

- ☐ Have both printed copies and electronic copies of the evidence.

APPENDIX A

Devices and Accounts to Consider

Social Media Accounts	Communication
☐ Facebook	☐ Smart Phone
☐ Twitter	☐ Computer
☐ Instagram	☐ Gmail
☐ Snapchat	☐ Personal and work email
☐ TikTok	☐ Messenger
☐ Pinterest	☐ WhatsApp
☐ WeChat	☐ Signal
☐ YouTube	☐ Slack
☐ Tumblr	☐ QQ
☐ Reddit	☐ Viber
☐ LinkedIn	☐ Telegram

- ☐ Instant, Direct (DMs), or Private Messages on online platforms

Video Conference

- ☐ Zoom
- ☐ MS Teams
- ☐ Skype
- ☐ FaceTime
- ☐ Video calls on online platforms

Cloud Storage

- ☐ iCloud
- ☐ Dropbox
- ☐ Google Drive
- ☐ Amazon Drive

Childcare and pets

- ☐ Shared calendars
- ☐ Child tracking apps
- ☐ Baby monitor
- ☐ Photo sharing
- ☐ Scheduling apps

Finances

- ☐ Bank accounts (including credit cards)
- ☐ Investment accounts (e.g. stocks, investments, retirement, education, etc.)
- ☐ PayPal
- ☐ Apple wallet

- ☐ Animal camera
- ☐ Animal tracker (e.g. GPS device in collar)
- ☐ Bitcoin Wallet
- ☐ OXF

Bills and Utilities

- ☐ Phone plans
- ☐ Electricity
- ☐ Gas
- ☐ Internet/Cable

Government Accounts

- ☐ Canada Revenue Agency
- ☐ Appointment booking apps
- ☐ Student Loan Account
- ☐ My Account (CRA)
- ☐ Provincial Services Account

Food Delivery Services

- ☐ SkipTheDishes
- ☐ Uber Eats
- ☐ DoorDash

Transportation Apps

- ☐ Uber
- ☐ Lyft
- ☐ Taxi apps

- ☐ Foodora
- ☐ Other restaurant accounts
- ☐ Waze
- ☐ Google maps
- ☐ Public transit apps

Shopping Apps

- ☐ Amazon
- ☐ Grocery points card
- ☐ PC Optimum
- ☐ Coffee points card
- ☐ Real Estate apps
- ☐ Account/reward apps at stores you shop at or online

Entertainment

- ☐ Spotify
- ☐ Netflix
- ☐ Crave
- ☐ Disney+
- ☐ Amazon Prime Video
- ☐ Apple Music and TV
- ☐ iTunes
- ☐ Podcast apps
- ☐ Audible
- ☐ PornHub

Gaming

- ☐ Discord
- ☐ Twitch
- ☐ Switch
- ☐ Steam
- ☐ Xbox Live
- ☐ PlayStation Network
- ☐ Origin
- ☐ Smartphone games

Health and Fitness

- ☐ Fitbit
- ☐ Apple Watch
- ☐ Distance tracking (e.g. Strava, MapMyRun)
- ☐ GPS devices (e.g. Garmin, hiking apps)
- ☐ Period or fertility apps
- ☐ Diet or calorie counters
- ☐ Medical tracking apps
- ☐ Therapy apps

Travel

- ☐ Travel points cards (e.g. Aeroplan, Air Miles)
- ☐ Airbnb
- ☐ Expedia
- ☐ TripAdvisor
- ☐ HostelInternational
- ☐ Airlines
- ☐ Trains

Smart Home Devices

- ☐ Amazon Echo
- ☐ Google Nest
- ☐ Alexa
- ☐ Siri
- ☐ Sonos One
- ☐ The Ring
- ☐ Home security systems
- ☐ Smart thermostat
- ☐ Smart lighting
- ☐ Smart lock

Smart Portable Devices

- ☐ Smart car
- ☐ GPS in car
- ☐ Bluetooth in car
- ☐ Tracking app for bike
- ☐ Tiles
- ☐ Find my phone

Education and Learning

- ☐ School email
- ☐ School online assignment platform
- ☐ Library card
- ☐ Language apps

Technology-Facilitated Gender-Based Violence (TFGBV) is part of a continuum of violence that can be both online and in-person. If you or someone you know is experiencing TFGBV, you are not alone. You can use sheltersafe.ca to find a shelter/transition house near you to discuss options and create a safety plan. You don't need to stay in a shelter to access free, confidential services and support.

We gratefully acknowledge Suzie Dunn, PhD Candidate at the University of Ottawa, for the creation of this information sheet.

Adapted from BCSTH's Technology Safety project, based on their resource [Technology Safety Planning Checklist](#).