



## Conversation Starters for Tech Safety Planning

### A Note on Language



In this toolkit, we will sometimes use the word woman/women and feminine pronouns for simplicity and to recognize the significant impact technology-facilitated violence has on women and girls. We recognize that TFGBV also impacts trans, non-binary, and Two-Spirit people. We hope that all people impacted by TFGBV will find these documents useful.

### How to Use This Resource

This resource is to help anti-violence workers discuss technology-facilitated gender-based violence (TFGBV) with survivors. TFGBV is a common tactic of domestic violence. If the person you are working with has experienced TFGBV, it should be considered carefully in her safety plan. This resource contains question prompts, tech safety strategies, and document links that you can use to guide your safety planning conversations with survivors experiencing TFGBV.

You can also review the companion resources— [‘Is Tech Abuse Happening to You?’](#) and [“Technology Safety Planning Checklist”](#).

### Some Initial Considerations:

- The following tech safety strategies may not suit every situation. Meet your client where she is at and start the conversation with the form of tech abuse that she identifies may be happening. This is not meant to be a checklist but rather suggestions on how to incorporate technology into safety planning.
- 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 your client is seeking help and can trigger additional abuse. Extra safety planning precautions may need to be taken in these situations.

### Does Anyone Control, Take, Break, or Make You Share Your Phone?

- Do you have your own phone? What do you use your phone for?
- Does anyone keep you from talking to your family or friends?
- Do you share your phone with someone else or does anyone else look at your phone?
- Have you ever needed to use your phone but could not use it? Can you tell me more about what was going on?
- Does anyone know how to unlock your phone or do they make you unlock it?

### Suggested Tech Safety Strategies:

- If you determine that it is not safe to stop using a phone that the abuser is monitoring or accessing, use your phone normally, but find another way to safely talk about private things and plan for safety.
- Let people know when you see them that your phone is not private. Use a code word that can let the other person know if someone is listening to your call or reading your texts.
- Write down the numbers of people on your phone and keep them somewhere safe in case your phone is taken from you or smashed.
- For more tips, check out our [Technology Safety Planning Checklist](#).

### Does Anyone Access, Control, or Lock You Out of Your Accounts (Email, Banking, Social Networks, etc.)?

- Do you share accounts with anyone? Do they set it up or make decisions for you about your account?
- Does anyone have access to your email accounts, bank accounts, GooglePlay, Apple ID, or iCloud account?
- Are the things you do on your phone or accounts private or does anyone else see them?
- Does anyone know your passwords or go into your accounts?
- Has anyone ever locked you out of your accounts or made changes to them?

- Does anyone make accounts in your name or lie about you wanting an account?
- Do you have your own bank account or do you share one with someone?

### **Suggested Tech Safety Strategies:**

- Use a [long password](#) with a mix of numbers and symbols that is hard for someone to guess.
- Use 2-step verification or multi-factor authentication if safe to do so.
- Use a different password for every account.
- Consider changing account passwords or setting up new accounts.
- Set up new "safe" accounts on a safe phone or library computer. Use those accounts only on a device the abuser does not have access to.
- For more tips, check out our [Technology Safety Planning Checklist](#).

## **Does Anyone Shame, Humiliate, Threaten, or Impersonate You Using Social Media, Apps, Text, Email, or Phone?**

- Does anyone say bad things about you on social media?
- Do other people start saying things to hurt you or "like" mean things about you that others have posted?
- Does anyone make you feel afraid to use social media? What do they do?
- Has anyone tricked you or acted like they were you or someone you know on social media?

### **Suggested Tech Safety Strategies:**

- Keep a record of social media posts, who posted them, and who received them (use the "download data" feature, take a screenshot or photo with another "safe" device, or copy, print, or put them on a USB).
- Adjust security and privacy settings (including tagging) on social media apps. Block the abuser if it is safe to do so.
- These behaviours may be against the law and help can be sought from a lawyer or police.
- For more tips, check out our [Technology Safety Planning Checklist](#).

## **Does Anyone Harass, Abuse, Punish, or Threaten You Via Text, Communication Apps (Whatsapp, Viber, Skype, Facetime), Email, Or Phone?**

- Has anyone said things using a phone to hurt you or scare you?
- Do you have to do things with your phone so you do not get in trouble?
- Does anyone send you messages all the time or get angry if you do not write back?

### **Suggested Tech Safety Strategies**

- Write down what was said in phone calls and keep the call history logs, sometimes called "recents" (screenshot, take a photo with another "safe" device, or print). Call history and text logs can also be accessed through mobile providers.
- Keep the text messages (copy, screenshot, take a photo with another "safe" device, print, or save on a USB).
- Turn Wi-Fi and Bluetooth off and then switch the device to Flight or Airplane Mode to preserve the call history and text messages on the device.
- Take the device and any copies, screenshots, printouts, or USB to your lawyer or police to have evidence formally documented, as these behaviours may be against the law.
- For more tips, check out our [Technology Safety Planning Checklist](#).

## **Does Anyone Share or Threaten to Share Images Without Your Consent ([Image-Based Abuse](#))?**

- Does anyone have private photos or videos of you with or without your consent?
- Have they shared those photos or said that they will share them?
- Did they say these things to you in person or send them to you?

### **Suggested Tech Safety Strategies**

- Ask for the person to take the image down and delete it.
- Report the image to the social media company
- The sharing of intimate images without consent is against the law and help can be sought from a legal advocate, lawyer, or police.
- For more tips, check out our [Technology Safety Planning Checklist](#).

## **Does Someone Know Where You Are, What You Do, or Stalk You Using Location/GPS Tracking, Monitoring, Spyware/Keystroke Logger Apps, or Hidden Cameras?**

- Does anyone use your phone to watch you or know where you go?

- Does anyone know things that you have not told them? How do you think they found out about this?
- Does anyone seem to know some things but not others? What are the things they know? Where does that information "live"?
- Do weird things happen with your phone, car, or home that do not make sense?
- If your client suspects that her location is being monitored or if she is being stalked, her devices, home, car, belongings, or her children's devices or belongings may be compromised.
- **All stalking should be taken seriously**

## Suggested Tech Safety Strategies:

- Consider using a "safe" device (e.g. new phone or a trusted family/friend's phone) for safety planning activities and/or leaving it with trusted family/friends.
- Figure out if there is a pattern related to what someone knows. Do they know where you go all the time or just when you drive your car or use public transport? Consider mapping what the person knows and where that information can be found. This can help narrow down where the person is getting the information. For example, if they have access to where you go using a rideshare app but not other forms of transport or other information, it may be that specific ridesharing app that is compromised.
- Check global location settings on the phone and for each app as some apps may collect and share location information. Also check for location-tracking tools like the Tile or AirTags.
- Stalking behaviours may be against the law and help can be sought from a lawyer or police.
- For more tips, check out our [Technology Safety Planning Checklist](#).

*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 or call/text the Kids Help Phone to discuss options and create a [safety plan](#). You don't need to stay in a shelter to access free, confidential services and support.*

*Adapted for Canada with permission from WESNET's Technology Safety project, based on their resource [Tech Abuse: Client Conversation Starters & Safety Planning](#).*

---

© Copyright 2024 Women's Shelters Canada | All Rights Reserved

This project is made possible through funding from the department of Women and Gender Equality (WAGE) Canada.