# Conversation Starters for Tech Safety Planning

## 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 their safety plan.

Inside, you'll find question prompts, tech safety strategies, and helpful links to guide your safety planning conversations.

For additional support, see the companion resources: Is Tech Abuse Happening to You? and the Technology Safety Planning Checklist.

### Initial Considerations:

- Meet the survivor where they are and start a conversation to understand more about the tech abuse that may be happening.
- Whenever you are safety planning with someone who has experienced TFGBV, it is important to note that the abuser may have access to their devices or accounts and may be monitoring their communication and movements through them.
    - Making changes to any device, social media account, email, or other technology may alert the abuser that the survivor is seeking help and can escalate 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?
- Who owns your phone and account?
- 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

- Encourage them to keep using that phone as usual to avoid raising suspicion, but use a separate, safer device or method for private conversations and safety planning.
- Remind them to tell trusted contacts in person that their phone isn't private.
- Help the survivor come up with a simple code word they can use to signal when someone is listening to their calls or reading messages.
- Suggest they write down important contact numbers and store them somewhere safe in case their phone is taken or destroyed.
- Support them in contacting the wireless provider to ask about options for leaving an account controlled by the abuser or setting up a new phone or number.

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? Have access to your password manager?
- 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

**To help improve account security:**

- Support the survivor in creating long, hard-to-guess passwords using a mix of numbers and symbols.
  - If it's safe, help them turn on two-step or multi-factor authentication.
  - Encourage using a different password for each account to reduce risk if one is compromised.
  - Discuss whether it's safer to change passwords or set up entirely new accounts.
  - Help them create new "safe" accounts using a secure device—like a library computer or a phone the abuser can't access—and avoid logging into those accounts on any monitored device.

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

**If the survivor is experiencing social media abuse:**

- Help them keep a record of harmful posts, who posted them, and who saw them.
  - If possible, use the "download data" feature, take a screenshot or photo with a safe device, or copy, print, or save the content to a USB.
  - Assist with adjusting privacy and security settings on their social media accounts, including tagging settings.
  - If safe, support them in blocking or muting the abuser.
  - Let them know that some of this behaviour may be illegal, and they can consider talking to police or a lawyer.

For more tips, check out our Technology Safety Planning Checklist.

## Does Anyone:
## Harass, Abuse, Punish, or Threaten You Via Text, Communication Apps (WhatsApp, 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 your abusive partner doesn't get upset or angry?
- Does anyone send you messages all the time, or get angry if you do not write back?

### Suggested Tech Safety Strategies

**To help document phone and text-based abuse:**

- Support the survivor in writing down what was said during calls and keeping a record of call logs (often listed under "Recents").
- If safe, they can screenshot, photograph with a safe device, print, or save the logs to a USB or a new email address.
    - Some call and text records can also be requested from mobile providers.
- Help them preserve abusive text messages using similar methods—copy, screenshot, photograph, print, or save.
- To protect existing data, suggest turning off Wi-Fi and Bluetooth, then switching the phone to Airplane Mode.
- If the survivor chooses to involve police or a lawyer, they can bring the phone and any saved records to help formally document the abuse, which may be illegal.

For more tips, check out our Technology Safety Planning Checklist.

## Does Anyone:
## Share or Threaten to Share Images
## Without Your Consent?

- 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

**If an intimate image is being shared without consent:**

- Support the survivor in asking the person who shared the image to take it down and delete it, if it's safe to do so.
- Help them report the image to the social media platform or website where it was shared.
- If they are worried that the image will be shared on any of these platforms you can prevent the image from being shared on these platforms by starting a case with StopNCII.org
- Let them know that sharing intimate images without consent is illegal. They can consider speaking with a legal advocate, lawyer, or police for support.

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 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? When do they know where you are?
  Where does that information "live"?
- If the survivor suspects that their location is being monitored:
  - their devices, home, car, belongings, or their children's devices or belongings may be compromised.

### Suggested Tech Safety Strategies

**If the survivor is worried about being tracked or followed:**

- Support them in using a "safe" device, such as a new phone or one borrowed from a trusted friend or family member, for safety planning.
  - They may also choose to leave that device with someone they trust.
- Help them look for patterns in what the abusive person seems to know.
  - For example, do they always know where the survivor is, or only when they use certain transportation methods?
  - Mapping what the abuser seems to know and where that information might come from can help identify possible sources of tracking.

    - For instance, if location details match rideshare trips but not other travel, a rideshare app may be compromised.
- Go through the phone's location settings and app-specific settings to check what's sharing location info.
    - Also, check for physical tracking devices like AirTags or Tiles.
- Let them know that stalking and unauthorized tracking may be illegal.
    - They can consider speaking to the police or a lawyer for further help.

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 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.*