# Basic Tech Safety

### 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.

# What is Technology-Facilitated Gender-Based Violence?

Technology-facilitated gender-based violence (TFGBV) is when technology is misused by perpetrators to commit violent abusive acts such as domestic violence, harassment (stalking), sexual assault, impersonation, extortion, and the non-consensual filming and sharing of intimate images. It can include things like receiving threats or harassment over text message or social media, location tracking or surveillance using technology, restricting access to technology, or online sexual exploitation and harassment.

Abusers are increasingly misusing a variety of phone, surveillance, computer technologies, apps, and social media platforms to harass, threaten, coerce, defame, intimidate, and monitor women and girls.

It is common for a perpetrator to misuse multiple technologies at once while also using more traditional power and control tactics such as withholding access to children and/or finances.

## What Does Technology-Facilitated Gender-Based Violence Look Like?

The following is a list of the most common forms of technology-facilitated gender-based violence. This is not meant to be an exhaustive list. For more details on different forms of TFGBV, check out the specific tip sheets and guides in the

Technology Safety and Privacy Toolkit.

**Harassment:** the misuse of technology by a perpetrator to repeatedly contact, threaten or intimidate another person when they do not want them to and it makes them feel afraid.

This may be happening to you if you're:

- Being sent abusive, threatening, or insistent text messages and/or emails.
- Receiving persistent Facebook, WhatsApp, Snapchat, or other online platform messages.
- Continually being tagged on social media such as Instagram or Facebook.
- Receiving posts of abusive and/or continuous comments and replies to social media posts.

**Stalking/Criminal Harassment:** misusing technology to knowingly and/or recklessly harass someone that causes that person to reasonably fear for their safety or the safety of someone they know.

In Canada, this includes:

- Repeatedly following a person from place to place or following anyone known to the survivor;
- Repeatedly communicating, either directly or indirectly, with the survivor and/or anyone known to them.
- Harassing, disturbing, or watching the survivor's house or place where they, or anyone known to them, resides, works, carries out business, or happens to be; or engaging in threatening conduct directed at the survivor or anyone they know.

This may be happening to you if the perpetrator is:

- Using apps, location trackers, or stalkerware to learn your whereabouts and/or follow you from place to place.
- Using technology (e.g. apps, social media, texts, instant messaging) to repeatedly communicate with you directly or indirectly.
- Using webcams, hidden cameras, or apps to watch you at your home, work, or as you carry out your daily business.

**Impersonation:** hiding behind technology to pretend to be someone else as a tactic of further violence and control, for example, to damage a woman's reputation or relationships.

This may be happening to you if:

- You receive replies from strangers regarding an unknown advertisement that links them to you as the person who posted the ad.
- You receive angry responses from friends and family regarding messages, emails, or communications that you did not write.
- Your employer receives an unauthorized resignation email seemingly from you.
- You receive communication from a perpetrator impersonating a new partner or friend to "catfish"/ get close to you and connect with you.
- You receive notifications that your accounts are closed or you've changed passwords or cancelled your utility accounts when you have not made any changes to your accounts.

**Monitoring/Surveillance:** the misuse of technology to learn, know about, or follow another person's communications or activities. This can be possible if a perpetrator has physical or remote access to a device.

This may be happening to you if the perpetrator is:

- Logging onto your smartphone, email, or social media accounts to monitor your activities.
- Using apps, spyware, or key-stroke loggers to learn your location.
- Inserting a GPS tracker into your car or GPS-enabled watches and other accessories.
- Using hidden cameras that have been installed or strategically placed.

**Location Tracking:** using apps or tools to track a person's location, such as stalkerware. It may seem like the perpetrator knows where the person is at all times.

This may be happening to you if the perpetrator:

- Is using apps, location trackers, or stalkerware to learn your whereabouts and follow you from place to place.
- Has access to your cloud accounts and your smartphone has location services turned on.
- Has apps on your phone such as "find my friends" turned on and is a member.
- Gives location tracking technology to your children through a smartwatch, AirTag or Tile, or phone apps.
- Has access to GPS systems in your car.
- Is misusing family and friend location capabilities found on technology-enabled devices.

**Threats:** the use of language threatening to harm, extort, or humiliate someone through the use of technology.

This may be happening to you if you're:

- Receiving threats that the perpetrator will post personal information, photos, videos, or other material unless you comply with their demands.
- Being locked out of social media, email, or other online accounts including banking.
- Receiving threats through text, email, and social media.

**Non-Consensual Distribution of Images:** distributing, sharing, and posting private/intimate photos and videos of a person without their consent.

This may have happened to you if:

- Intimate and private images or videos of you have been posted online without your consent to embarrass, humiliate, harass, degrade, and/or harm.
- Private/intimate photos or videos of you have been sent to your friends, family members, employers/coworkers, and/or strangers without your consent.

**Consent** means an ongoing process of **giving and receiving permission.**

**Doxing:** the publication of private or identifying information of a particular individual on the Internet without the individual's consent.

This may have happened to you if:

- Your personally identifying information (e.g. name, address, phone number, email address, passport/SIN numbers) was posted on social media or websites without your consent.

*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.*

# Is Tech Abuse Happening to You?

## It Can Be Tech Abuse If Someone:

- Controls your phone
- Takes your phone away from you
- Breaks your phone
- Makes you share your phone
- Controls your online accounts
- Stops you from using your online accounts
- Uses your online accounts when you don't want them to
- Shares pictures of you that you don't want people to see
- Tells you they will share pictures of you that you don't want people to see unless you do what they want

## It Can Be Tech Abuse If Someone Watches What You Do Using:

- Your phone
- Hidden cameras
- Apps

## It Can Be Tech Abuse If Someone Uses a Computer, Phone, or Tablet to:

- Repeatedly contact you (if unwanted)
- Say things that hurt you
- Punish you
- Say they will hurt you or a member of your family

## It Can Be Tech Abuse If Someone Uses Apps or Social Media to:

- Say things that make you feel bad
- Say things that make you or your family look bad
- Make threats about things they will do to you or our family

## It Can Be Tech Abuse If Someone Uses Tech to:

- Find out where you are when you don't want them to
- Find out what you are doing when you don't want them to
- Follow you

*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 Is Tech Abuse Happening to You.*

# Technology Safety Plan Tip Sheet

## Prioritize Safety

**Consider using a safer device.** If you think that someone is monitoring your computer, tablet, or smartphone, try using a different device that the perpetrator 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 is one way to reduce the risk of being monitored by a perpetrator.

**Get more information.** Navigating violence, abuse, and stalking can be very difficult and dangerous. Anti-violence workers in your area can tell you about options and local resources, and help you create a plan for your safety. You can call your local anti-violence program to be connected with a support worker near you or find one at www.sheltersafe.ca.

**Trust your instincts.** Perpetrators are often very determined to maintain control over women 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 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 perpetrators 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 behaviour if they feel they've lost control over their current or former partner. Before removing a hidden camera or GPS tracker that you've found, or uninstalling stalkerware, think through how the

perpetrator may respond and plan for your safety. For example, some women choose to use a safer device for certain interactions, but also keep using the monitored device as a way to collect evidence and prevent escalation.

## Identify the Abuse

**Look for patterns.** Take some time to think through what kind of technology may be used to stalk, monitor, or harass you. For example, if the perpetrator 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 being misused can help you create a safety plan and to document the abuse. Read more about Assessing for Technology-Facilitated Violence.

**Document the incidents.** Documenting a series of incidents can show police or the court a pattern of behaviour 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 Documentation Tips for Women Experiencing Technology-Facilitated Violence.

**Report the incidents.** You may also want to report the incidents to law enforcement or seek a Peace Bond or Family Protection Order. If the harassing behaviour is online, you can also report the abuse to the website or app where the harassment is happening. If the behaviour 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 as evidence before reporting it.

## 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 and settings.** Go through your smartphone, apps, and online accounts to 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 is and what it does. 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 is 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 perpetrator 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 when it's not in use. You also might keep the old device so that the perpetrator thinks you are still using it and doesn't try to get access to the new device.

**Protect your location.** If the perpetrator seems to always know where you are, they might be tracking you through your smartphone or vehicle or by using a location-tracking device. You can check your smartphone, 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 wireless provider to ask if any location-sharing services are in use, especially if you were/are on a family plan with the perpetrator. 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 car mechanic may be able to check for you. It's important to safety plan and document evidence before removing a device or changing the perpetrator'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 perpetrator, 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 with a piece of removable tape (although this only addresses the camera, not the spyware on the computer). Remember to make a safety plan and document evidence before removing devices or cutting off the perpetrator's access.

## Steps to Increase Privacy

**Protect your address.** If you're concerned about someone discovering your home address, you could open a private mailbox (PO Box). Note that this is most helpful if you have recently moved or the perpetrator doesn't already know your address. Tell friends and family not to share your address, and be cautious about giving it out to local businesses. Also, look into what information is public in your community if you were to purchase a home so you know your options.

**Limit the information you give out about yourself.** Almost 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 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 and online privacy.** Our Technology Safety and Privacy Toolkit has Online Privacy and Safety Tips including more information about changing settings on your electronic devices, social media accounts such as Facebook and Twitter, and your home WiFi network. Follow those steps to increase your privacy and decrease the risks of the perpetrator misusing those technologies, locating you, or monitoring your activity.

*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 NNEDV's Safety Net project, based on their resource Technology Safety Plan: A Guide for Survivors and Advocates.*

# Assessing for Technology Abuse: Tips for Anti-Violence Workers

## Best Practices for Programs

Women's safety and privacy are often compromised by abusers who misuse technology and survivors' personal information. As frontline workers, it is important that we take the time to educate ourselves and our service users about the various ways stalking, tracking, and monitoring occur through technology.

The following information will help you and the women you support think through how to identify and respond to different forms of technology misuse so you can properly safety plan. Including technology in a safety plan means strategically planning around the continued use of tech. When perpetrators 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 behaviour if they feel they've lost control over their current or former parter. The questions below are only meant to quickly assess what might be an issue; they are not meant to be an exhaustive list of all technology-related safety concerns a woman might face.

Anti-violence workers should follow up with a more thorough conversation about each woman's specific concerns and discuss strategies to increase safety, document incidents, and get additional help. You may find the other resources in our Technology Safety and Privacy Toolkit helpful in this process. Keep in mind that women often attend support groups with little direct and ongoing interaction with anti-violence workers, so consider incorporating this information as a support group topic as well.

## Steps to Assessing Technology Misuse and Safety

- *Prioritize safety planning*: What are your current safety concerns?
- *Narrow down the possible technology that could be used*: What types of things have happened to make you feel unsafe or cause concern?
- *Gauge women's knowledge and understanding*: How do you think this is happening?

These questions open a conversation that will explore and prioritize safety, discuss what types of technology devices or applications could be misused, and identify how to best address their needs and further their knowledge.

Below are sample questions and examples of possible technology misuses to get you started, once you've narrowed down what may be happening:

### 1. Are you concerned about the abuser knowing where you are all the time? Let's explore some common ways tracking can occur:

- Through your smartphone
- Through apps on your phone that use your location
- Through social media
- Through friends and family

- Through your car or some kind of tracking device on the car
- Through a location device such as a Tile or AirTag

## 2. Are you worried that the perpetrator might be able to access your communication with other people? Here are some common communications that can be compromised:

- Email communication
- Smartphone communication (e.g. texts or calls)
- Phone communication
- Private instant or direct messages (PMs and DMs)

## 3. Are you concerned about information that's posted about you online? Let's look at possible ways information about you could be shared online:

- Through your social media accounts
- Through the abuser's social media accounts
- Through your children/family/friends' social media accounts
- What specifically is your concern about those accounts?
  - The abuser is posting terrible things.
  - The abuser is monitoring social media accounts to find information about you.
  - The abuser is accessing online accounts without your permission.
- Is there other information online about you that you are concerned about?
  - Work or school websites
  - Community forums and groups
  - Apps

## 4. Are you concerned about your children/family/friends' use of technology and the possibility it could compromise your safety?

- Are they using specific apps on their smartphones, iPads, tablets, etc. that you're concerned about?
- Are there games they are playing that you're worried about?
- Does the abuser have access to the technology of children and/or other family members?

## 5. Are you concerned about your ability to continue using technology while maintaining your safety and privacy?

- Are there specific devices, such as your smartphone or laptop, that you want to go through to ensure that it is safe and secure?
- Do you need to go through your social network accounts to figure out privacy and security settings?

## 6. What are other concerns that you have about your privacy and safety?

- Do you need to think about other technology to figure out privacy and security settings? If so, what are they?

*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 NNEDV's Safety Net project, based on their resource Assessing for Technology Abuse.

# Documenting Tech Abuse

How technology is misused to harass and control may seem unbelievable. However, it is important to trust your instincts. If you believe that you are being monitored or stalked via technology, you might be. Narrowing down what is happening, including the tactics and technology used, can help to determine if technology-facilitated gender-based violence (TFGBV) is occurring and, if so, how to address it.

It is important to document everything that is happening. Documentation is important for many reasons:

- It will give you a record of what is happening, which may be helpful if you want to pursue legal action.
- It will alert you to any escalation in monitoring and control, which may indicate that the danger is increasing as well.
- It will help you see patterns of technology-facilitated violence and may help determine how the perpetrator is misusing a particular technology.

## Documentation Tips

- **Keep a log of all incidents**, even if you are not sure that you want to involve the police. Some of the information you might want to include is the date, time, location, police officer information (if reported), witnesses (if any), suspected technology involved (e.g. phone, email, etc.) and a brief description of what the perpetrator did.
- **Save everything related to the event or incident.** If you receive a threatening note or a threatening message by email, text message, or voicemail, make sure you save it. Take a photo or screenshot of the message. While it may be tempting to delete it, saving it could show patterns to help you determine safety strategies and provide needed evidence.
- **Think about what technology you suspect the abuser could be using.** In some cases, women have strong suspicions about what technology the perpetrator is using based on the type of abuse, the tactics involved, and what they know about the perpetrator.
- **Think about your safety first.** In some cases, when abusers know that women are documenting the abuse, they might escalate their monitoring, control, or physical violence. You will know best how to assess the situation and what could happen. Trust your instincts and do what is safest for you.
- **Document only relevant information.** Keep in mind that this information could potentially be introduced as evidence or inadvertently shared with the perpetrator at a future time. For example, you may not want to document personal photos that aren't being used as part of the abusive tactic.

## What to Document

### Email

- Emails contain IP addresses, which could reveal the originating IP address and, therefore, the identity of the sender. Because of that, it's important not to delete the email and not to forward the email to someone else.
- If you are saving email content by printing or taking screenshots , be sure to also save the email header (often hidden and can be found in the settings), which is where the IP information is stored. Depending on the email platform you are using (Gmail, Outlook, Yahoo! Mail, etc.), how you access the email header will be different.
- If you're concerned that the perpetrator could access the account and delete emails, then try to print or take screenshots of the content, including the headers. Forwarded emails will lose the identifying information needed for evidence.

## Text Messages

- Text messages that are just stored on a phone may be inadvertently deleted or may be automatically deleted if you run out of space. Take a screenshot or picture of the text messages to retain the evidence.
- Also, take a screenshot of the contact page to show that the harassing messages from the perpetrator are associated with the perpetrator's phone number.
- Text message content is kept by the wireless carrier only for a limited time. If you are working with law enforcement, be sure to ask them to send a preservation letter to the phone company as soon as possible, so the phone company knows not to destroy the data.

## Social Media/Internet Harassment

- To keep evidence of harassment on social media, take a screenshot of the harassment/abuse on your computer or device.
- Some sites offer alternative ways to document activity on the site or on your page. For example, using Facebook's "Download Your Information" (DYI) feature, you can capture all content and save it for later.
- If working with law enforcement, they could send a letter to the social media or website company asking them to preserve the account information or contact the Department of Justice's Mutual Legal Assistance team.
- You may consider reporting the harassment to the social media or website company. However, be sure that you document the abuse first if you want evidence of it. If it violates the site's terms of service or content guidelines, they may remove the content.

## Harassing Phone Calls

- You could consider recording your phone conversations to keep evidence of harassing or threatening calls as Canada allows for one-party consent recording.

## Phone Number/Caller ID Impersonation

- Document your call logs by taking a photograph of the Caller ID. Be sure to include the date and time of the calls.
- Keep your phone records to show the number of the originating call, date, and time.

Our technology-facilitated violence log can help you document what is happening to you. For more information on how to store your digital evidence, see our info sheet "How to Back Up and Store Evidence of Technology-Facilitated Violence."

*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 NNEDV's Safety Net project, based on their resource Documenting Abuse.*

# Stalking and Technology-Facilitated Abuse Log

## What is a stalking and technology-facilitated abuse log?

Stalking and technology-facilitated gender-based violence (TFGBV) is when an abuser usestechnology as a tool to monitor and harm someone. This can include things like tracking location, sending harassing texts, and threatening to share abusive images. Some of the commontechnologies that are used as tools of abuse are devices and accounts.

This handout has a log to write down important details about the abuse. Two logs are provided, in a long and short form, so you choose the one that works best for their situation.

## Why keep a stalking and tech-facilitated abuse log?

- To capture evidence at the time the abuse occurs, making it more reliable in court
- To support the evidence captured
- To help see patterns and escalations of abuse for safety planning purposes
- To provide evidence for police and assist with their investigations
- To give support workers insight into the risks a survivor faces so that they can assist further
- To support you to take back control and be proactive
- To validate experiences. This can help if an abuser minimizes, denies, or gaslights the person they are abusing. Gaslighting is a form of psychological abuse where an abuser pretends the abuse did not occur and may blame a victim for "going crazy."
- To remind you about an abusive person's behaviour. Sometimes memories of abuse can beblurred over time. A log might assist with making statements for court or by helping a survivor decide what to do if an abuser is trying to re-establish a relationship.

## Staying safe while logging abuse

**Think about where you can store the logs safely so that an abuser will not find them. This may be in a locked desk at work, with your support worker, or with a trusted friend. Trust yourself. You know your situation best.**

If you decide to provide your logs to police or other services, they may ask for more details aboutthe person who is abusing you. These items may include information about the abuser's technology, such as their:

- Internet and phone provider and account information;

- Devices, such as phones, computers, tablets, cameras, drones, external hard drives,USBs, children's devices, etc.;
- Accounts or apps that have been used in the abuse such as social media or banking accounts;
- Email addresses, phone numbers, cloud storage accounts, usernames, avatars, pseudonyms, online identities, etc.; and
- any other information that relates to their technology, such as passwords, online associates, tracking devices, ISP addresses, identity theft or fraud, etc.

**Download a blank Stalking and Technology-Facilitated Abuse Log**

*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 Stalking and Tech-Facilitated Abuse Log.*

*This document is part of a series of resources provided through Women's Shelters Canada's Tech Safety Canada project. We encourage you to visit www.techsafety.ca to find additional information and resources about technology-facilitated violence, technology safety planning, and preserving digital evidence. This document, or any portion thereof, may be reproduced or used as long as acknowledgement is included. If you would like to adapt the content, please contact Women's Shelters Canada at info@endvaw.ca.*



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

Women and Gender Equality Canada | Femmes et Égalité des genres Canada | Canada