Technology-facilitated abuse guide.

A TELUS Wise® guide for adults of all ages.



This resource is intended as a supplement, not a replacement for professional support from trained domestic violence advocates. If you're in immediate danger, call 9-1-1.

TELUS® Wise

© TELUS 2026. 26-0872

Contents

What is technology-facilitated abuse? 1

Why technology makes abuse easier 1

Who is affected? 1

The Power and Control Wheel 2

Warning signs of tech abuse 3

Is this really abuse? 4

Types of tech abuse 5

Surveillance and stalkerware 5

GPS and location tracking 5

Image-based abuse (non-consensual intimate images) 6

Smart home and Internet of Things (IOT) 6

Online harassment and cyberstalking 7

Digital financial abuse 7

Safety planning 8

Covering your digital tracks 8

Quick safety check list 9

Get help 10

Crisis and support lines 10

Organizations and resources 10

This guide was created in collaboration with The Today Family Violence Help Centre; whose expertise, guidance, and insights helped shape this resource.

What is technology-facilitated abuse?

Technology-facilitated abuse (TFA), also called tech abuse or digital abuse, occurs when someone uses digital technology as a tool to monitor, control, harass, intimidate or harm another person.

Technology itself is not the problem. Abusers weaponize everyday devices and apps, smartphones, smart home devices, social media, GPS and more, to extend their power and control beyond physical spaces.

Tech abuse is not a separate form of abuse, it's a tactic used within a broader pattern of coercive control. It often accompanies physical, emotional, financial and sexual abuse.

Why technology makes abuse easier:

- Technology is embedded in every part of daily life, including home, work and social connections
- Many monitoring tools are marketed as "family safety" apps, making abuse easy to disguise
- Abusers can monitor victims remotely and in real time, 24 hours a day
- Digital evidence of abuse can be hard to document and easy to delete
- Victims may not recognize tech-based tactics as abuse
- Leaving an abuser does not automatically stop tech abuse; it can escalate after separation

Who is affected?

Tech abuse can happen in any relationship regardless of gender, age, sexuality or background. It's especially common in:

- Intimate partner relationships (current or former)
- Family relationships (parents, siblings, adult children)
- Situations where one person controls shared accounts or devices
- Relationships with significant power imbalances

According to research by the Government of Canada, tech abuse disproportionately affects women, LGBTQ+ individuals, immigrants, people with disabilities and Indigenous Peoples, though anyone can be a victim.

Youth are also particularly susceptible. They are growing up in a digital age where the sharing of location, personal information, passwords and social media access among peers is normalized from a very young age. This may make it harder to recognize the risks associated with those behaviours.

The Power and Control Wheel

Just as the Duluth Model - a foundational framework in domestic violence advocacy and social work - describes physical and emotional abuse tactics, tech abuse fits into the
same framework of power and control:

Surveillance: tracking location, reading messages or monitoring calls

Isolation: blocking contacts and controlling access to devices

Intimidation: threatening to share private images or information

Economic control: controlling online banking, shared accounts or workplace accounts

Coercion: demanding passwords or forcing sharing of location

Minimizing and denying: “I’m just keeping you safe” and “You’re paranoid.”



The following sections explore how these tactics manifest through specific digital technologies.



Warning signs of tech abuse

You may be experiencing tech abuse if your partner or family member does any of the following:

Tracks your location: constantly knows where you are without you telling them; demands you share your location at all times.

Demands passwords: insists on having all your passwords, PINs and account access, and gets angry if you change them.

Monitors your messages: reads your texts, emails, and social media messages; demands to see your phone at any time.

Threatens to share private images: has shared intimate images of you without your consent (image-based abuse).

Controls smart home devices: uses smart locks, cameras, thermostats or speakers to monitor or control your environment.

Controls your online accounts: manages your email, social media or banking; prevents you from accessing your own accounts; or prevents you from accessing your workplace accounts to undermine your reputation with colleagues or damage your work in an effort to get you fired (a form of economic control). May also use access for illegal activity, blackmail, or criminalization.

Accesses personal information: may access online health records, Canada Revenue Agency files or other sensitive documents as a form of surveillance or intimidation.

Records without your consent: records your conversations, takes photos or videos of you without permission or installs spyware.

Isolates you online: blocks your contacts, controls who you can follow or talk to, or posts things to damage your reputation.

Controls finances: controls online banking and e-transfers or prevents you from accessing money through digital means.

Creates fear and anxiety: you feel anxious using your phone or devices; you self-censor out of fear of being monitored.

Continues after separation: harassment, monitoring, or threats continue via technology even after you have left the relationship.

Creates fake profiles: creates fake accounts to monitor or impersonate you, or contacts people in your life.

Is this really abuse?

Abusers often frame tech monitoring as care or safety. Ask yourself:

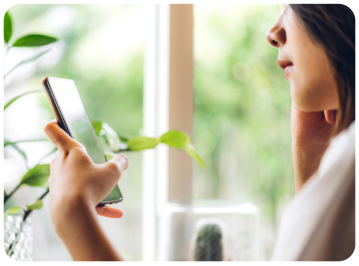
- Do I feel afraid or anxious when I use my devices?
- Do I hide who I talk to or what I do online?
- Did I agree to this monitoring, or was it demanded?
- Does my partner use information from my devices to punish or control me?
- Would my partner be angry if I changed my passwords or turned off location sharing?

REMEMBER: Healthy relationships are built on trust and mutual respect, not surveillance. You have the right to privacy, even in a relationship.



Types of tech abuse

1. Surveillance and stalkerware



What it is: software secretly installed on your device to monitor calls, texts, location, photos and app activity without your knowledge.

Signs your device may be compromised:

- Battery drains unusually fast
- Phone feels warm even when not in use
- Data usage is higher than expected
- Device is slow or behaves strangely
- Your partner knows things you never told them

CAUTION: Do NOT delete suspected stalkerware without first speaking to a domestic violence advocate. Deleting it may alert the abuser and put you at greater risk. An advocate can help you plan safe removal strategies without detection.

2. GPS and location tracking



What it is: apps, devices or hidden GPS trackers that monitor your physical location.

Common methods:

- Built-in phone location sharing (Find My, Google Maps sharing)
- Shared family plan location features
- Hidden GPS trackers placed in vehicles, bags or belongings
- Smart car apps that report driving data
- AirTags or Tile trackers hidden without consent
- Children's devices and apps with location-sharing features
- Pet trackers and collars with location features

3. Image-based abuse (non-consensual intimate images)



What it is: taking, sharing or threatening to share intimate images without consent, sometimes called “revenge porn” (though this term minimizes the harm).

Examples:

- Sharing or threatening to share intimate images with family, employers or publicly
- Recording sexual activity without consent
- Using images as blackmail to control behaviour
- Deepfake images created using AI

Image-based abuse is a crime in Canada. The non-consensual sharing of intimate images is illegal under the Criminal Code of Canada. You can report this to the police.

4. Smart home and Internet of Things (IOT)



What it is: using connected home devices to monitor, control or intimidate.

Examples:

- Smart locks: locking and unlocking doors remotely to control movement
- Smart cameras: monitoring inside the home
- Smart speakers: listening to conversations
- Thermostats: controlling temperature as punishment
- Baby monitors: using to spy on victims
- Smart doorbells: monitoring who visits

TIP: If you’re leaving the relationship, check all smart home devices. Change passwords and remove shared access from all accounts before or after leaving safely.

5. Online harassment and cyberstalking



What it is: using digital platforms to harass, intimidate or control.

Examples:

- Sending threatening or abusive messages repeatedly
- Creating fake profiles to monitor or impersonate you
- Creating fake text or email threads or AI-generated deepfakes to incriminate you or manipulate court proceedings
- Posting false or damaging information about you online
- Contacting your friends, family or employer online
- Flooding you with calls, texts or emails
- Hacking into your accounts

Online harassment and cyberstalking are crimes in Canada. Learn more about criminal harassment laws.

6. Digital financial abuse



What it is: using technology to control or restrict access to money.

Examples:

- Controlling all online banking access
- Monitoring all purchases and transactions
- Preventing you from setting up your own accounts
- Running up debt in your name using your digital identity
- Controlling cryptocurrency or digital assets
- Accessing or controlling sensitive financial and legal documents (tax returns, mortgages, loans, insurance, wills, investments)

Safety planning

Your safety comes first. Before making any changes to devices or accounts, please speak with a domestic violence advocate. Some actions, like deleting spyware or changing passwords, can alert an abuser and increase danger.

Important: Safety planning should always be done with the support of a trained advocate who understands tech abuse. The steps below are general guidance only. While these steps may help improve your safety, they can't eliminate risk. Safety planning is a risk-reduction strategy, and no single plan works for everyone.

Covering your digital tracks

If you need to research help on a shared or monitored device:

- Use private or incognito browsing mode (Ctrl+Shift+N or Command+Shift+N)
- Clear your browser history after each session
- Use a Virtual Private Network (VPN) if available
- Use a library computer or a friend's device
- Search using DuckDuckGo, which does not save search history
- Call crisis lines from a payphone or a friend's phone

Note: Incognito mode doesn't hide your activity from your internet service provider or from monitoring software installed on your device.

Step 1: Use a safe device

If possible, use a device your abuser does not have access to - a friend's phone, a library computer or a new prepaid phone - for sensitive communications and searches. Ask your local family violence organization about accessing a safe phone. Some organizations have prepaid phones available.

Step 2: Check for tracking apps

Ask an advocate or a trusted tech-savvy person to help check your device for stalkerware. Don't delete it without guidance as it may alert your abuser. For a step-by-step guide, refer to MediaSmarts' resource on securing your devices.

Step 3: Secure your accounts

When safe to do so, change passwords on a safe device, enable two-factor authentication on a number or email your abuser can't access and review account recovery options.

Step 4: Review location sharing

Check all apps for location sharing settings. Look for AirTags or GPS devices in your vehicle, bags and belongings.

Step 5: Document the abuse

Take screenshots of threatening messages, save records of calls, and note dates and times of incidents. Store evidence on a safe device or with a trusted person.

Step 6: Adjust social media privacy

Review privacy settings on all social media. Consider making accounts private, removing location tags from posts and blocking the abuser on all platforms.

Step 7: Smart home devices

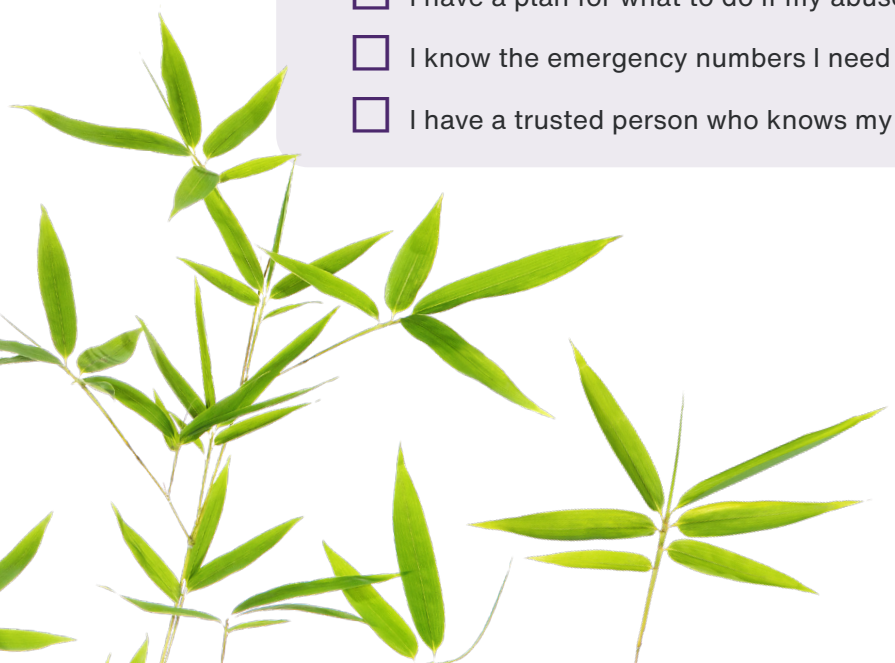
If safe to do so after leaving, change all smart home passwords, remove the abuser's access from all apps and consider a factory reset of devices.

Step 8: Create a new email address

Set up a new email account on a safe device for communications with shelters, lawyers and support services. Don't access it from a device your abuser may monitor.

Quick safety check list

- ☐ I have access to a safe device for sensitive communications
- ☐ I have spoken with a domestic violence advocate about my tech safety
- ☐ I know how to clear my browser history if needed
- ☐ I have documented evidence of tech abuse safely
- ☐ I have a plan for what to do if my abuser discovers I'm seeking help
- ☐ I know the emergency numbers I need (police, shelter, crisis line)
- ☐ I have a trusted person who knows my situation



Are you new to using digital technology?

Our TELUS Wise online basics video series covers everything you need to know, from connecting to the Internet to keeping your devices and accounts safe, including passwords, privacy settings and social media security.

To learn more, visit telus.com/**WiseOnlineBasics**



Get help

Don't face this alone. Here are trusted organizations and resources to help:

Crisis and support lines

- Ontario: Assaulted Women's Helpline: 1-866-863-0511 (24/7, 200+ languages)
- Alberta: Family Violence Info Line: 1-780-310-1818 or Text 310-1818
- BC: VictimLinkBC: 1-800-563-0808 (24/7)
- National: Dial 2-1-1. This is a national service available in most provinces that can connect you to community, social, and government services, including support for men experiencing abuse.

Organizations and resources

- Ending Violence Association of Canada (EVA)
- Canadian Women's Foundation
- Canadian Center for Women's Empowerment (CCFWE)
- For Survivors - Tech Safety Canada
- Stalking and Technology-Facilitated Abuse Log - TechSafety
- Reclaim Your Digital Space
- Security in a Box
- Technology Safety – New Beginnings
- Resources-Survivors — Safety Net Project
- Digital Smarts Program Resources for Survivors