Tech Safe BC

# Safely Preserving Digital Evidence of Technology-Facilitated Violence

**Complied by Tech Safe BC**

**Last Updated:** February 9, 2026

Tech Safe BC

# Table of Contents:



**If something in this guide is no longer up to date, or you have any questions, please reach out to techsafe@bcsth.ca with your concerns.**

# 1 Start with Safety

Before collecting any digital evidence, take time to think about your safety. Saving evidence can sometimes increase risk if the person causing harm is watching your devices, accounts, or online activity.

### Consider these safety questions:

- Could the person causing harm see what I save on my phone, computer, or tablet?
- Do they have access to my cloud accounts, email, passwords, or shared accounts?
- Is there a chance they could delete evidence if they notice I'm saving it?
- Does my device feel unsafe, slow, or like someone else might be monitoring it?

If you have any concerns, it's helpful to connect with a local anti-violence program to create a technology safety plan. They can also help you plan how and where to safely save evidence.

### Safety Tip:

If your current or former partner might be monitoring your phone or accounts, collect and store evidence on a different device or ask a trusted friend to help.

# 2 Understand What Counts as Evidence

Digital evidence can come from many places. You may have:

- Evidence you can directly see.
    - Examples: Texts, emails, social media posts, DMs, call logs, photos, online threats.
- Evidence you cannot directly access, such as:
    - Content shared in group chats you are not part of.

    - Photos or messages visible to friends of the abuser.
- Evidence the abuser controls, such as content on shared accounts.
- Evidence requiring technical help, like checking for spyware.
- Evidence needing a court order, such as information from service providers or websites.

# 3 Plan and Document

Before saving anything, create a simple plan to stay organized and reduce risk.

## Step 1: Create a Log

A log helps you track what happened, when it happened, and what evidence you collected.

Include:

- Date and time of the abuse.
- Date and time you collected the evidence.
- What happened and its impact (emotional, financial, safety-related).
- Who you think was involved, and why.
- Any witnesses or other relevant information.
- Any missing pieces you still need to collect.

A simple word document, notebook, or printed form can work.

Some organizations use a Technology-Facilitated Violence Log template.

### Safety Tip:

Log entries themselves can be evidence, showing timelines and impacts.

# Step 2: Document What Happened

Try to capture evidence as soon as possible as online content can disappear or be deleted.

## When documenting, try to include:

- The full message or post.
- Usernames, phone numbers, or profile links.
- Timestamps.
- Metadata if available (e.g., url, date stamps, email headers).
- Enough surrounding conversation to show context.

## Guidance for common platforms:

**Texts / Messaging Apps**

- Screenshot or screen-record the full conversation.
- Overlap screenshots so nothing is missing.
- Capture contact details and timestamps.

**Social media** (e.g., Instagram, Facebook, Snapchat, TikTok, X, etc.)

- Screenshot or screen-record posts, comments, and profiles.
- Include usernames and dates.
- Capture full threads, including replies and likes.
- For Snapchat and other apps that alert the sender: use a second device if possible so the abuser is not notified.

**Emails**

- Capture the “To/From/Subject/Date” fields.
- Do not forward the email to yourself as this removes metadata.
- Save attachments.

**Voicemails / Calls**

- You may record calls in Canada as long as you are part of the conversation.
- Save call logs and voicemail audio.
- Write down the date, time, and what was said.

**Websites**

- Save as PDF or screenshot.
- Capture URL, date, time, and identity of poster.
- Double-check PDFs created through "Print Page" functions.

If police are involved, they can send "preservation letters" to platforms to prevent deletion of evidence.

# 4 Store Evidence Safely

Where and how you store evidence depends on your situation and your safety plan.

## Option A: Internal Storage

Use this only if your current or former partner cannot access your device.

- Save evidence to a secure folder.
- Delete "Recently Deleted" folders when necessary.
- Turn off password saving features in browsers.
- Change passwords to accounts used to store evidence.

### Safety Tip:

Change passwords on a device the abuser cannot access, especially if spyware is suspected.

## Option B: External Storage Device

An external storage device is safer if your current or former partner can access your device.

**Examples**: External Hard Disk Drives (HDDs), External Solid-State Drives (SSDs), USB Flash Drives (Thumb Drives), Memory Cards

- Transfer files to a secure laptop or desktop first.
- Use a USB or USB C Key the current or former partner does not know about.
- For iPhones, you may need an adapter or specific app.

Keep a record of when and how you transferred evidence (helpful for court authenticity questions).

## Option C: Remote External Storage

Remote external storage is useful when physical safety is a concern or you cannot hide an external storage device.

**Examples**: Google Drive, iCloud, Dropbox, PCloud

- Use a separate email account the abuser cannot access.
- Avoid downloading cloud apps unless you normally use them.
- Access cloud accounts through a browser and clear history afterward.
- Consider using web-based versions instead of apps.

### Safety Tip:

Use a dedicated email only for storing evidence. Delete browser history after accessing it.

## Option C: Decoy Apps (Use with Caution)

Some apps hide files behind fake icons (like a calculator), but they still store files on your device. They can be discovered, especially if spyware is present on your device.

## 5 Be Cautious About Sharing Evidence Online

Some survivors share screenshots or videos publicly. While understandable, this can sometimes:

- Alert your current or former partner.
- Lead them to delete or hide evidence.
- Negatively affect legal cases.

Speak with an anti-violence worker if you are unsure.

## 6 Get Support

If you're unsure how to collect or store digital evidence safely:

- Connect with a local anti-violence worker.
- Ask about technology safety planning.
- Request support accessing legal help or police if you choose to involve them.

Support workers can also help determine:

- Safer methods of documentation.
- Storage plans.
- When and how to collect evidence without tipping off the abuser.

*If you are experiencing tech abuse, you are not alone. Find support in your community by connecting with a BC Society of Transition Houses Member Program or check out our other safety resources at techsafebc.bcsth.ca.*