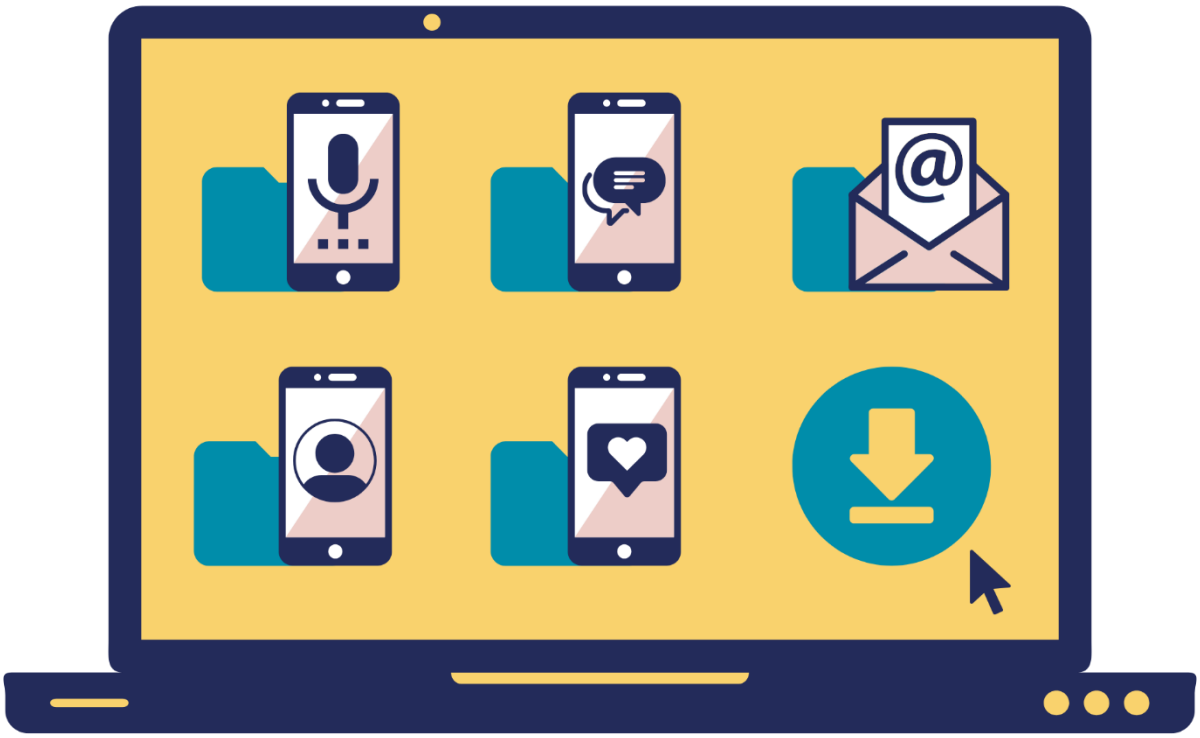
Documenting Tech Abuse



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 your current/former partner 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:

- 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 abuser did.

Save everything related to the event or incident.

If you receive 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, survivors have strong suspicions about what technology the abuser is using based on the type of abuse, the tactics involved, and what they know about the abuser.

Think about your safety first.

In some cases, when abusers know that survivors 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 abuser 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 abuser 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 abuser are associated with the abuser'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.

For more information on dealing with harassing and threatening messages see our short video here.

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,
    - send a letter to the 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.

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.