Conversation Guide: Securing Personal Information Online

What is personally identifying information?

Personally identifying information is any information that can be used to create accounts or verify one's identity. It is important to keep this kind of personal information safe as it can be misused by a current or former partner to gain access to the survivor's existing accounts or to impersonate them for the purpose of creating new accounts in their name.

The misuse of personally identifying information can look like:

- Opening bank accounts or taking out loans in the survivor's name
- Logging in to the survivor's financial apps to gain information about their finances or transfer money out of their accounts
- Restricting a survivor's access to money by putting holds on or closing accounts
- Abusive partners can also use this information to locate a survivor's new address, contact them after they have changed their number, or even find out personal things about their life.

Examples of personally identifying information are:

- Full name
- Home address
- Phone number
- Email address
- Birthdate
- School name
- Social media usernames (e.g., usernames like "Kate1981" could reveal personal details like someone's name and year of birth
- Credit card or banking details such as account numbers, PINs and passwords.
- Social Insurance Number

Conversation Starters with Survivors:

Before getting started, remind yourself of the foundational principles of survivor centered tech safety support, see The 4 Core Principles of Tech Safety.

Step 1: Understand what is happening

Start by asking questions to learn how the abuser may be misusing the survivor's personal information. This helps determine the level of risk and financial harm and helps identify the most effective steps to take. Questions you can ask include:

- Does your current or former partner have access to your and your children's personally identifying information (name, birthdate, SIN, address), documents, or financial statements?
- Do you have access to your and your children's personal identifying information (name, birthdate, SIN), documents or financial statements?
- Does your current or former partner know the account numbers, passwords, and PINs to online banking, other financial apps, and accounts you may have?
- Has your current or former partner accessed your financial accounts or opened an account under your name in the past?
- Are you restricted from accessing your documents (e.g. no Wi-Fi at home to make ID replacement request, current or former partner has hidden the documents from you etc.)?

Step 2: Understand what the survivor wants to do

Each survivor's needs and goals will be different. Instead of assuming what should happen next, ask:

- What would you like to see happen? What do you want?
- Do you want to involve the financial institution?
- Do you want law enforcement involved?
- Do you want to keep a record of what has happened?

Step 3: Identify strategies that will match the survivor's goals

Once the survivor's goals are clear, help them develop a plan to secure their online accounts and reduce further harm. Here, we are focused on technological strategies and responses. You should also take whatever other steps you would normally recommend if, for example, an abuser is breaching a peace bond or court order or if you have immediate or urgent concerns about the survivor's safety.

Some strategies for different scenarios include:

If the survivor does not have access to their documents/information or is concerned about losing access, encourage them to:

- Gather documents of financial accounts, make copies, and store them in a safe place.
- Replace any missing documents and send them to the address of someone they trust.

If the abuser has had access to accounts previously or has the information needed to access them in the future, encourage the survivor to:

- Change passwords to ones that have a mix of numbers, letters and symbols and are lengthy, like $ummer1$myFavouriteeaon on a device their current or former partner does not have access to if it's safe to do so.
- Change PINs to a new combination of numbers they have never used. Choose a random sequence of numbers and avoid using numbers that their current or former partner could guess easily. For example, they should not use children's birthdates, their favourite number, house number, etc.
- Update the security question answers on their accounts (the ones used to reset a password if you forget it) with new responses that their abuser won't be able to guess. Answers don't have to be truthful—survivors just have to make sure they remember what they set.

- Don't save new passwords and PINs to their device unless they are sure their device or account is not being monitored or used by others.

For more information see our What to Do if You're a Victim of Financial Fraud tip sheet.

If the survivor wants to pursue legal action:

Survivors might not be sure if they want to go to the police or they may know they don't want to involve law enforcement right now. However, if the evidence isn't preserved when the abuse happens, they may not be able to access it later if they change their mind about involving law enforcement. Encourage them to preserve evidence so they have proof if they ever need it later. Here are some suggestions:

Here are some suggestions:

- Consider notifying law enforcement if it feels safe to do so. Let the survivor know that reporting to the police could lead to an investigation to see if the abuser broke any laws.
- Plan for safety, especially if they go to the police station, as the abuser may realize that they are reporting if a location tracker is still on the survivor's belongings or vehicle.
- Seek legal support. Survivors can reach out to a civil attorney or legal aid organization. The survivor may also consider applying for a civil protection order independently or with the support of an advocate or attorney.
- Keep a record of financial documents, make copies, and store them in a safe place. See Women's Shelters Canada's (WSC) Sample Technology-Facilitated Violence Log for guidance.
- Check online accounts if they track where and when someone logged into your accounts and cross reference it with your location and schedule. Most online accounts give an option to download this information that can be used as evidence.
- Store the evidence in a safe place. Back it up somewhere else, too, just in case.

Understanding personally identifying information (PII) and how it can be misused is essential for supporting survivors of technology-facilitated gender-based violence. By having informed conversations, identifying safety strategies, and preserving digital evidence, anti-violence workers can help survivors regain control over their personal information and financial security. Every survivor's situation is unique, and a survivor-centered approach ensures that their choices, needs, and safety remain the top priority.

Suggested Resources

- What is Tech-Facilitated Gender-Based Violence?
- Is Tech Abuse Happening to You (Poster)
- Tech Safety Planning Conversation Starters
- Tech Safety Planning Conversation Starters for Anti-Violence Workers Supporting Indigenous Survivors
- Your Safety, Your Voice: Protecting Your Personal Information Online- Video for Survivors
- Passwords: Simple Ways to Increase Your Security
- Safety Planning Check List
- Digital Financial Abuse Toolkit
- Preserving Digital Evidence Toolkit

Technology-Facilitated Gender-Based Violence (TFGBV) is part of a larger pattern of violence that can happen both online and in person. As a support worker, it's important to let survivors know they are not alone. For guidance on addressing TFGBV, you can refer to our comprehensive techsafety.ca website.

This project was supported by a grant from CIRA's Net Good Program.