Conversation Guide: Securing Online Bank Accounts

What is digital financial abuse?

Digital financial abuse is the misuse of online financial tools such as online bank accounts to harm a survivor financially and/or restrict their access to money and resources.

This could look like:

- Logging into the survivor's bank account without permission to take or track money.
- Moving money between accounts to confuse or control the survivor's finances.
- Opening credit cards, loans, or bank accounts in the survivor's name without them knowing.
- Changing passwords or security questions to lock the survivor out of their own bank account.
- Setting up automatic payments or transfers to steal money.

- Turning off banking alerts so the survivor doesn't see what's happening.
- Removing the survivor from a shared account so they lose access to their money.
- Using mobile payment apps or e-transfers to take money secretly.
- Threatening to report fake fraud to ruin the survivor's financial reputation.
- Using cryptocurrency or digital wallets to hide money.

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 is controlling or accessing the survivor's finances. This helps determine the level of risk and financial harm and helps you identify the most effective steps to take.

Consider asking:

- Has anyone accessed your bank accounts or credit cards without your permission?
- Who controls the finances in your household? Is your account joint?
- Can your current or former partner physically or electronically access your bank account or statements?
- Do you have a safe place to save money without your current or former partner accessing it?
- Have you noticed money missing, strange transactions, or new accounts in your name?
- Have you been locked out of your bank accounts or had passwords changed?
- Are you receiving alerts or statements about accounts you don't recognize?
- Do you feel pressured or afraid to make financial decisions?

- If the survivor is unsure, suggest checking their online banking history, credit report, or speaking with their bank to identify any unusual activity.

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 finances 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 wants to secure their online accounts, encourage them to:

- Change passwords and security questions if it is safe to do so (if doing so will not escalate the risk of harm). Make sure to avoid answers the abuser might guess.
- Enable two-step verification for extra security by turning on the option within the settings.
- Review bank account settings to remove unauthorized users or devices.

If the survivor wants to monitor and protect their finances, encourage them to:

- Check bank statements and credit reports for unusual activity.
- Set up transaction alerts to stay informed of any changes through account settings.
- Freeze or close compromised accounts.
- Increasing Privacy and Safety.
- Use a new email address and phone number for banking if the abuser has access to your existing email account and phone number.
- Request paper statements or change the account email if the abuser has access to the survivor's email.
- Consider opening a separate bank account at a different financial institution so that the abuser does not have access to the survivor's bank account.

If the survivor needs additional support, encourage them to:

- Contact the bank's fraud department for help reversing charges or securing accounts.
- Speak with a financial counselor about the options to recover credit or consolidate debt.
- If safe to do so, report identity theft or fraud to authorities.

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:

- 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 assistance from 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. Document any suspicious activity.
- Store the evidence in a safe place. Back it up somewhere else, too, just in case.

Every survivor's situation is unique, and their choices should guide the response. By providing information, options, and support, frontline workers can help survivors regain financial control while prioritizing their safety.

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: Securing Online Bank Accounts from an Abusive Partner- Video for Survivors
- Is Digital Financial Abuse Happening to You?
- Safety Planning Check List

- 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