Digital Financial Abuse: Safety Planning Tips for Anti-Violence Workers

This resource is intended to help anti-violence workers discuss digital financial abuse with survivors. With financial technology evolving quickly, digital financial abuse is becoming a common tactic of technology-facilitated gender-based violence.

If the person you are working with has experienced digital financial abuse, this should be considered carefully in their safety plan.

This resource contains:

- question prompts,

- tech safety strategies, and
- document links that you can use to guide your safety planning conversations with survivors.

You may also find these companion resources about TFGBV and safety planning helpful:

- Is Tech Abuse Happening to You?
- Is Digital Financial Abuse Happening to You?
- Technology Safety Planning Checklist
- Conversation Starters for Tech Safety Planning
- 6 Tips for Securing Your Online Financial Information

Safety Planning: Personally Identifying Information

Personally identifying information (name, birthdate, SIN, address) can be misused by a current or former partner to open accounts, log in to financial apps, and restrict access to money.

ASK:

- 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?
- Does your current or former partner know the account numbers, passwords, and PINs to online banking, other financial apps, and accounts you may have?
- Do you have access to your and your children's personal identifying information (name, birthdate, SIN), documents or financial statements?
- Are you restricted from accessing your documents?

    - Example: No Wi-Fi at home to make a replacement request, current or former partner has hidden the documents from you.

SUGGESTED STRATEGIES:

- Gather documents, make copies, and store them in a safe place.
- Replace any missing documents and send them to the address of someone you trust.
- Change passwords to ones that have a mix of numbers, letters and symbols and are lengthy.
- Example: $ummer1$myFavouriteeaon
- Change PINs to a new combination of numbers you have never used.
    - Choose a random sequence of numbers and avoid using numbers that your current or former partner could guess easily.
    - Example: Do not use your or your children's birthdates, your favourite number, house number, etc.
- Don't save new passwords and PINs to your device unless you know your device or account is not being monitored or used by others.

Safety Planning: Ownership of Financial Accounts and Access

ASK:

- In general, who controls the finances in your household?
- Do you have a bank account?
    - If yes, is it joint or individual?
- 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?

SUGGESTED STRATEGIES:

- Change your individual accounts' PINs, mailing addresses, contact information, and passwords.
- Do not change account information unless it is safe to do so.
    - Instead, record or take screenshots or photos to regularly capture the account's balance and transaction history.
    - Focus on documenting dates, balances, and key transactions.
- Open a new account at a different bank that the abuser doesn't know about.
    - Learn more about how to do so safely in our resource, Safeguarding Against Digital Financial Abuse When Opening a New Bank Account.

Safety Planning: Harassment and Threats

ASK:

- Have you received threats through the "optional message" section when you receive an e-transfer from your current or former partner?
- Does your current or former partner demand to know your log-in ID and passwords for your online banking?
- Does your current or former partner send constant requests for money?
- Has your current or former partner damaged your credit by applying for credit cards, loans, or government benefits under your name?
- Has your current or former partner located your whereabouts by logging in to financial accounts online?

- Has your current or former partner withdrawn access to finances by cancelling or putting bank and credit cards on hold?

SUGGESTED STRATEGIES:

- Report any abuse or suspicious activity to your bank or credit card company.
- Preserve evidence of harassment, threats, and monitoring by taking screenshots or video screen recordings.
- If comfortable, contact law enforcement.
- Withdraw cash from a bank machine further away from where you work or live.
- Change passwords and PINs to ones that are hard to guess.
- Request a free credit report from Equifax.

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. For more information about digital financial abuse, see our full Digital Financial Abuse Toolkit.

Adapted for Canada from the New York City Domestic Violence Economic Justice Taskforce's Financial Development Subcommittee, based on their resource *Financial Safety Planning: Best Practices for Domestic Violence Service Providers*.

This project was funded by TD Bank Group, through its corporate citizenship platform, the TD Ready Commitment.