Tech Safety Canada

6 Tips for Securing Your Online Financial Information

If you're trying to protect your finances from a current or former partner, here are six tips to help you secure your financial identity online.

1. Check Settings

Check the settings of your online banking account and any other online account or app that stores financial information.

If you are concerned about a current or former partner gaining access to your account, consider:

- Increasing password security by changing your password on a device that is not being monitored.
- Implementing multi-factor authentication.

You can also familiarize yourself with the actions you can take beyond changing passwords, such as:

- restricting access to cards,
- locking credit cards, and
- setting up alerts to get notified by text or email about purchases, low or high balances, failed login attempts, or other changes.

Contact your bank or credit card company for guidance.

2. Secure Your Accounts, Devices, and Networks

Use secure accounts, devices, and networks such as a library computer or a friend's device to access your financial information.

If you are concerned that your abuser is monitoring your devices, this can help ensure your abuser is not aware of any new passwords, accounts, or other changes you are making to your financial accounts, providing their email is not set up to be notified of changes.

To prevent unauthorized access:

- secure your accounts with a PIN or password known only to you and

- ensure only you have access to your email for authentication.

3. Review Publicly Available Personally Identifying Information

Review, secure, and/or remove personally identifying information (name, birth date, SIN, address, etc.) publicly available online.

Personally identifying information such as your name, address, email address, phone number, and other data may end up online in a few different ways.

For example:

- you may share it voluntarily,
- someone else may share it on your behalf, or
- it may be obtained in a data breach.

There are various ways to manage your digital fingerprint, some free and some requiring one-time payment or a monthly fee.

A simple way to see what's publicly available about you online is by using a search engine (e.g. Safari, Firefox, Chrome) to look up your name and see what information appears in the results. This will primarily show information you or someone else has shared, as information released in a data breach is not typically easily accessed through online searches.

There are several free and paid options to determine if your information has been compromised in a data breach and what information may be exposed. One free option is have i been pwned?, which will search known data breaches for your email address and allow you to sign up to receive notifications of future breaches.

Steps to take if you find your personal information online:

Information Shared by You:

- If you come across information you previously shared that you wish to remove, you can manage or remove this yourself if you still have access to the account.
- If you no longer have access to the account, it may take additional steps to regain access to the account from which you shared the information.

Information Shared by Someone Else:

- If you see information someone else shared about you that you do not want to be shared, check out the National Network to End Domestic Violence's Safety Net resource on removing sensitive information from the Internet for more information.

Information Shared in a Data Breach:

- Once you know that your information has been involved in a data breach, it's crucial to:
    - update passwords,
    - secure any current accounts, and
    - not reuse a leaked password for any other accounts.

Remember, only share sensitive financial information with applications (apps) and organizations you trust.

- Your data is a valuable commodity for many websites and apps.
- Websites and apps will request sensitive information about your financial identity for a variety of reasons.
- Some will allow you to import banking information for various purposes, such as payment processing, rental applications, and tracking expenditures.
- Sharing this information can help you achieve your financial goals more quickly, but it can also place your privacy at risk if the app or institution is not guarding your information adequately.
- Shared information can also pose a risk if an abuser has access to a non-financial account that contains financial information you don't want them to have, such as credit cards and banking information.

Questions to Consider

To help you decide which websites or apps to trust with your information, here are some essential questions to consider:

Who is your information being shared with?

- Will your information be shared with others once you share it with this institution or app?
- Can you choose who else this information is shared with?

Consider this for both your bank and credit accounts and the apps you share this information with. This information should be included in the privacy policy governing your account or application usage, but these documents are often overlooked when opening a new account or are too long to read and understand in one sitting.

How is your information being used?

- What is the purpose of collecting your information?
    - Before sharing, consider whether this information is necessary to achieve your goals in using the app features or account services.
- Is there another way to achieve these goals without sharing this information?
    - For example, could a potential landlord review paystubs or another form of income verification rather than requesting sensitive banking information?

What protections or measures are in place to protect your personal information once it's entered into the application?

- If an app requests access to sensitive financial identity information, the app should be transparent about how your information is being used and protected.
    - The Apple and Google app stores provide users with an overview of how each app handles data written by the developer, which can be reviewed before downloading the app.
- You can also review user ratings to see if other customers had security issues with the app.
- Additionally, anti-virus programs like Norton 360 can help you determine whether an app is reputable, what information it collects, and with whom it is shared.

  - These programs can be helpful tools in determining whether an app meets your privacy needs, but they usually require a fee or paid subscription and may not be accessible to all survivors.

4. Use a Credit Card

If you have access to credit, one way to protect your finances is to **use a credit card instead of a debit for routine purchases.** Using a credit card will protect cash assets against instant withdrawal if someone gains access to your card and uses it for an unauthorized purchase.

Also, most credit cards offer some level of protection against unauthorized purchases. They will not hold the cardholder liable for fraudulent charges, although it can take time to dispute them and get them cleared from an account. Ideally, use a credit card that has never been shared with the abusive person so that your purchases cannot be monitored.

If you have multiple credit cards, using specific cards for specific types of purchases (e.g. groceries, gasoline, etc.) can help make fraud or other unauthorized spending easier to detect if it occurs.

5. Monitor Your Credit Report

Monitor your credit report and track any new inquiries or changes in your credit score.

There are several free and paid options for monitoring changes to your credit report. Some consumer reporting agencies will let you sign up for an account and receive additional copies of their report. It's important to note that while credit reports will show active and closed credit accounts, how much debt you have, and payment history, they may also include a credit score. Credit scores are determined based on the information in your credit reports, so if you find fraudulent activity or errors in your credit report, it can impact your credit score.

If you find fraudulent activity in your credit report:

- Dispute the issue with the credit bureau(s) (e.g. Equifax Canada, TransUnion Canada) that shows the incorrect information.
- Notify the bank, credit card company, or institution reporting the error.
  - They are legally required to investigate and correct inaccuracies.
- File a Fraud Alert or Credit Freeze with Equifax and TransUnion to warn lenders to take extra steps to verify your identity.
- Consider requesting a credit freeze to prevent new accounts from being opened in your name without your consent.

6. Use Fraud Alerts

Utilize fraud alerts to protect your financial identity and credit.

Fraud alerts notify potential creditors that you have been or may be a victim of fraud and encourage them to take additional steps to verify your identity before extending a new line of credit.

There are two types of fraud alerts: Initial and Extended.

Initial

- You can request an initial fraud alert for any reason, and it will remain on your credit report for one year.
- Initial fraud alerts can be renewed annually as needed.

Extended

- An extended fraud alert is only available to victims of fraud with certain types of documentation, such as a police report or Affidavit of Fraud confirming fraud and/or identity theft.
- This type of fraud alert will:
    - remain on your credit report for up to seven years unless you opt out earlier, and
    - will stop you from receiving any pre-screened credit card and insurance offers for 5 years.

Both types of fraud alerts will also allow you to request additional copies of your credit report free of charge for credit monitoring purposes. You only need to request a fraud alert through one of the three nationwide credit bureaus (Experian, TransUnion, and Equifax), who will then communicate with the other two on your behalf.

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 with permission from NNEDV’s Safety Net project, based on their resource *Financial Abuse and Technology*.

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