



AN OUNCE OF PREVENTION— DON'T LET FRAUD WIN

Around the globe, scammers are focused on finding increasingly deceptive ways to exploit both you and the latest technologies. Their goal—to get your personal information.

Learn how to protect yourself by identifying common fraud characteristics and using a healthy level of scepticism when things don't sound quite right.

Fraud characteristics

We're exposed to fraud on a regular basis, so it's important to be able to identify scam characteristics and take action to protect yourself. Scams may appear as something that's too good to be true, require immediate action and may be accompanied by threats. Fraudsters may also ask you to not share the details with loved ones. They're persistent and creative in designing schemes.

Tips

- Ask yourself if the request makes sense and take your time—don't be rushed into taking action.
- Do your research, speak to friends or family members.
- Don't rely on the phone number on your call display as it can be 'spoofed' (changed to look like another number), and don't divulge personal information if it's not required.

Tax scams

Have you ever received a text message, email or phone call from "the Canada Revenue Agency (CRA)" claiming that you're entitled to an extra refund? — All you need to do is provide your banking details. Perhaps you've been notified that you owe the CRA money and payment is required in Bitcoin or gift cards. Have you been threatened with fines, imprisonment or deportation? If you receive a call, letter or email from the CRA, check your CRA account online or call them directly at 1-800-959-8281.

Tips

It's important to keep in mind that the CRA will never:

- ask for information about your passport, health card, or driver's license;
- demand immediate payment by Interac e-transfer, bitcoin, prepaid credit cards or gift cards from retailers;
- use aggressive language or threaten you with arrest or sending the police;
- leave voicemails that are threatening or give personal or financial information.



Identity fraud

Identity fraud occurs when fraudsters use personal information to access a victim's bank accounts, open new bank accounts, make purchases or apply for mortgages or loans. They do this by collecting information that we post online, leave behind in our recycling bins or give away when tricked by a fake website.

Tips

Keep your personal and financial information safe.

- Shred personal and financial documents before putting them in the garbage — trash bins are a goldmine for identity thieves.
- Never click on a link that asks you to enter your online banking account information and password. Always go to the trusted website directly or call a valid phone number.
- Be aware of where you're sharing personal information and how it could be used; for instance, your Social Insurance Number shouldn't be required to enter a contest.
- Check your bank statements and credit reports regularly, and report any irregularities to your banking centre or the credit bureau.

Password hygiene

It seems like everything requires a password these days and it's difficult to remember them all. We're living in a world of frequent data breaches. If you use the same username and password across sites, fraudsters may run your exposed credentials on a multitude of sites. You could lose Air Miles, collector points and worse, your savings.

How difficult is it to guess your passwords? Online lists of some of the most-used passwords of 2019 include: 123456, Password, qwerty.¹ Think twice when creating or updating yours!

Tips

- Set complex passwords, don't share or reuse them, and use different passwords for your banking, email and other online accounts.
- Never write down your passwords or carry them in your wallet.
- Always shield your PIN when keying it in.

At CIBC your security comes first. [Visit CIBC.com](https://www.cibc.com) to find out how we help protect you from fraud, and how you can help protect yourself.

¹Are you using one of the top 10 most-used passwords? <https://cba.ca/are-your-pins-and-passwords-safe>