

Fraud Prevention

Ways to prevent fraud



YOUR MONEY SENIORS



YOUR MONEY SENIORS

Want more information about financial fraud?

Sign up for the CBA's free Fraud Prevention Tip newsletter at cba.ca/fraudpreventiontips

Fraud Prevention

Ways to prevent fraud

Don't be a victim: 10 ways to prevent fraud



- 1 Protect your personal and financial information.
- 2 Destroy all your financial documents before putting them in the recycling.
- 3 Never give personal or financial information over the phone - unless you initiated the call.
- 4 Report lost or stolen credit/debit cards, driver's license, social insurance card, passport, etc. immediately.
- 5 Consult with a trusted and knowledgeable financial advisor.
- 6 Review your financial statements monthly.
- 7 Never share your PIN or passwords with anyone and choose PINs and passwords that are hard to guess.
- 8 Keep anti-virus and anti-spyware up to date on your computers, tablets and mobile devices.
- 9 Visit websites that you are sure are legitimate and shop online with only reputable businesses.
- 10 Change your password or passphrases every couple of months.

Remember: Your bank will never send you an e-mail asking you to disclose personal information such as your credit card number, online banking password or your mother's maiden name.

Watch out for these top scams:

The Romance Scam

A criminal will target an individual through a social networking or online dating site and will build a romantic relationship over time - sometimes many months. Once the scammer has a victim's trust, he or she will begin to ask for money.

Visit the CBA's YouTube page to view fraud scenarios that explain how it works and what it looks like in action: [youtube.com/user/cdnbankers/videos](https://www.youtube.com/user/cdnbankers/videos)

How not to choose your online password or PIN

When choosing online passwords, verification questions and credit and debit card PINs, avoid choosing something that would be easy to guess or information that could be obtained by others. And never use any of the following:

- Your name or that of a close relative
- Your birth date, year of birth, telephone number or address, or that of a close relative
- Your bank account, debit card or credit card number
- A number on any other identification that you keep with your debit and credit cards in your wallet, such as a driver's license or social insurance number
- A password or PIN used for other purposes

Phishing and Vishing

When criminals send emails and create websites that look like they are from a legitimate company you might deal with (i.e. your bank or cable company). Vishing (or voice phishing) is the same thing, except that scammers contact you via phone instead.

The Grandparent Scam

Involves a criminal calling and claiming to be your grandchild. He or she will ask for money to help them out in an emergency - a car accident or problem in a foreign country. They'll ask you to send money through a transfer service - urgently and with little time to think twice. And they'll tell you not to tell their parents.

Where to get help

- Your financial institution
- Your local police department
- The Canadian Anti-Fraud Centre
Toll free: 1.888.495.8501
antifraudcentre.ca

Find out more

The Canadian Bankers Association (CBA) website has extensive information on fraud prevention at cba.ca/fraud. The CBA also distributes a regular, free fraud prevention tip by email.

Sign up at cba.ca/fraudpreventiontips.

Never share your debit or credit cards, PINs and passwords with others - not even family members.

