



AN OUNCE OF PREVENTION: PROTECTING AGAINST FRAUD

Most Canadians have pretty good instincts when it comes to telling when something just isn't right. With March being Fraud Prevention month, there's no better time to hone your instincts and protect yourself and those you love against fraud.

You've probably been targeted at least once by a fraudster. They may have come to your door or called you. "But the Internet and advances in digital communications have opened other ways for scammers to steal your personal information and gain access to your money," says Bessie Calabria, CIBC Senior Director, Fraud Risk Management.

What does a fraud scam look like?

An interaction may appear to be legitimate on the surface. For instance, someone contacts you pretending to be the government, a potential love interest reaches out, or someone is selling something of interest to you. Fraudsters may threaten you, encourage you to act quickly and advise you to keep the transaction details from loved ones.

Some examples include:

1) Income tax fraud

You receive a text message, email or phone call from someone claiming to be from the Canada Revenue Agency (CRA) notifying you that you're entitled to an extra refund, or you owe money. All you need to do is provide your banking details, or make a payment using Bitcoin or gift cards. This is what a tax scam looks like. Corporal John McMath of the Royal Canadian Mounted Police says that tax fraud is one of the more prominent types of fraud.

To protect yourself, remember:

- The CRA doesn't make threatening phone calls.
- The CRA won't solicit personal information over the phone or by email, or demand payment with Bitcoin, gift cards or other unusual methods of payment.
- 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.

2) Romance schemes

Look out for potential scammers who try to appeal to your romantic and compassionate side. "The number one sign of a romance scam is that you're asked to send money, and it can be for any number of reasons," says Detective Sergeant Cathy Kehoe of the Ontario Provincial Police. They may tell you they'd like to see you but can't afford the trip. They may also ask for a loan for a health emergency.

To protect yourself, remember:

- Never send money to someone you've never met.
- Always meet in person, but only if you feel comfortable doing so.
- Don't share personal information, like your email or phone number.



3) Online purchase scams

Today, you can buy or sell almost anything over the Internet. While this is convenient, it can also be dangerous. Keep in mind, fraudsters remain anonymous on the Internet which means they can more easily take advantage of you.

For instance, scammers may sell a product—often at a very cheap price—so they can steal your payment card or personal information. They may also take your money and send you a worthless item, or nothing at all.

If you're selling an item, a fraudster may "accidentally" overpay you for it and then request you send them back the overpayment. In return, they promise you a small payment for your trouble. In these instances, the method of payment, usually a cheque, is worthless which leaves you out of the money you sent back to the fraudster and the item you were selling.

To protect yourself, remember:

- Buy from reputable companies or individuals you know.
- Be wary of websites that contain spelling mistakes and grammatical errors.
- If an offer sounds suspicious or too good to be true, it probably is.

Protecting your digital assets

Any information that you store electronically—from photos to text messages and emails, to legal documents—are your digital assets. This includes information and data you store on a computer, a flash drive, or a phone, or that you store electronically in a cloud.

Your digital assets are valuable to you. If you lost your phone, you'd probably be more upset about losing the information and pictures that are on it than the device itself. Consider these tips to protect your digital assets:

Expert insights on fraud prevention

"By managing your personal information wisely and being aware of potential scams, you can help guard yourself against fraud," says Calabria. "Always shred receipts, copies of credit applications, insurance forms and the like." She also recommends you check out the Canadian Edition of [The Little Black Book of Scams](#), for insights on fraud prevention.

"Your credit rating can indicate if your personal information has been misused," continues Calabria. Check your credit rating regularly through CIBC Online Banking's Check Your Credit Score link. You can also order a copy of your credit report from Equifax Canada, by phone at 1-800-685-1111 or 1-800-465-7166, or through their website. Other agencies, such as TransUnion Canada, also provide credit report information.

Receive real-time CIBC fraud alerts via phone or email. Make sure your contact information is up to date on CIBC Online Banking.

Back up your data. This is a great way to protect stored photographs and documents. You can use a cloud-hosted service, use regular backups that come with your devices, or invest in a portable drive.

Treat your passwords with care. Your passwords are the key to your life online. Don't use passwords that are easy to guess and don't write them down. Use different passwords for your banking, your email and other online accounts. Also, 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.

*Contact us anytime if you have questions about protecting yourself against fraud or spotting fraudulent schemes.
We're always happy to help.*