Banking that fits your life.

Fraud Prevention Tips*

Scammers are sneaky and sly. They don't discriminate. They target everyone, from youngsters to retirees, from individuals to businesses. No one is immune to fraud.

Learn how to protect yourself. This tip sheet provides you with some of the common characteristics of fraud along with some examples. Ideally you will read this before sending money to someone you don't know, responding to an urgent request from someone you do know, paying taxes with Bitcoin or iTunes cards, or paying to collect on lottery winnings or an inheritance.

We're here to help.

Red Flags

Learn to recognize the signs that something is amiss.

Transfer method

Many scams involve a request to wire money electronically using a money transfer service, like MoneyGram and Western Union, or using cryptocurrency, such as Bitcoin. Once the money is sent it's usually impossible to get it back.

Sounds too good to be true

Everybody loves unexpected money, a large windfall from an unknown relative, or winning a contest. But promises of an overseas inheritance or winnings from contests you don't remember entering may signal that the offer isn't quite what it seems. These types of scams often require some sort of payment or tax up front before the funds can be released.

Urgency/secrecy

Urgent requests with a need for secrecy are the hallmarks of a scam. Fraudsters will encourage immediate action so that you don't have time to think rationally or to investigate the legitimacy of the request. Take your time and speak with a trusted contact.

Personal information request

Fraudsters may ask potential victims to provide more personal or financial information than would be required for a legitimate transaction or discussion such as PINs, passwords, SIN, Driver's License Number, Passport number etc.

Spelling mistakes

Be skeptical of emails, messages or website addresses that contain misspelled common words; grammatical errors that make the message difficult to read, or expressions that are used incorrectly or sound odd.

Romance Scams

Who is behind the keyboard?

Keep your guard up and look out for potential scammers who will try to lower your defenses by appealing to your romantic and compassionate side. They operate on popular, legitimate dating sites as well as on fake ones.

On a dating site, a scammer might send you a few messages and a good-looking photo of themselves, or of someone they claim to be. Once you are charmed, they will start asking you to send money. They may say they have a very sick family member or a desperate situation that only you can help with. Once you give them money, they will request more for a variety of hardships they have recently experienced. Once you have exhausted all funds available to you, the fraudster will request you deposit cheques on their behalf. The cheques will be negotiated based on your good relationship with the Bank, however after you have sent the money to the fraudster the cheque will be returned and you will now owe the Bank.

These types of scams can ruin the victim financially, emotionally and physically.

Tip

Don't send money to someone you have never met.

Emergency Scams

Caring grandparents, don't act too quickly!

Emergency frauds usually target loving grandparents, taking advantage of their emotions to rob them of their money.

The typical scam starts with a grandparent receiving a phone call from someone claiming to be their grandchild. The "grandchild" goes on to say they're in trouble—common misfortunes include having been in a car accident, getting jailed, or trouble returning home from a foreign country—and they need money immediately!

The caller will ask you questions, getting you to reveal personal information. They'll also swear you to secrecy, saying they are embarrassed and don't want other family members to find out what's happened.

One variation of this ploy features two people on the phone, one pretending to be a grandchild and the other a police officer or lawyer. In other cases, the scammer will pretend to be an old neighbour or a family friend in trouble.

Tip

Before sending any money call your grandchild, neighbour or friend at a number that you have, not one provided by the caller, to confirm the story. Don't be shy to discuss the situation with a trusted friend or family member before sending any money.

Tax Scams

Got a call or email from the CRA? Make sure it's real!

You get a text message or an email from the Canada Revenue Agency (CRA) claiming you're entitled to an extra refund and all you need to do is provide your banking details. Watch out— this wonderful-if-true situation is exactly what a tax scam looks like.

Another variation is that they call you to say that you owe the CRA money and that you need to pay right away, or else they will report you to the police, or come to your home and arrest you.

In any case, if you do receive a call, letter, email or text saying you owe money to the CRA, you can double check online via "My Account" or call 1-800-959-8281.

Tip

The CRA will never:

- use aggressive or threatening language threaten you with arrest or send police
- ask for payments via prepaid credit cards or gift cards, such as iTunes, Home Depot, etc.
- collect or distribute payments through Interac e-Transfer®
- use text messages to communicate under any circumstances ask for financial information