Fraud prevention tips

Fraudsters 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.

This tip sheet provides you with some common characteristics of scams to help you identify if something is amiss, along with helpful tips if you think you've spotted a scam. By learning how to avoid a scam, you'll ensure your money is safe and out of the hands of a fraudster.

What's a scam?

Scams are schemes perpetrated by individuals to illegally obtain money or information, often by tricking the victim into giving them up. Fraudsters will develop trust, instill a sense of urgency and a need for discretion to get people to hand over their money. Scams make people believe they're benefiting from the scenario, but in fact it's the opposite – they give away their money and don't get anything in return.

Common characteristics of a scam:

Unusual payment method

Many scams involve a request for payment by wire transfer, pre-loaded cards, e-transfer, or using cryptocurrency. These untraditional forms of payment are often difficult to trace back to the recipient or get back, making it a preferred form of payment for fraudsters.

Sounds too good to be true

Whether it's a guaranteed high return investment or winning a contest, stop and think if the offer actually makes sense. Fraudsters often require some sort of payment or tax up front before the funds can be released.

Urgent and secret

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.

Unexpected call, text, email or letter

Fraudsters use different ways to reach out to people in order to get a response. If you receive a call saying you won a contest that you don't remember entering then chances are it's a scam.

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.

If you've come across any of these common characteristics and think you've spotted a scam, stop any communication, don't send money, and investigate the situation further by taking these steps:

Take your time

Think about the situation you're in and avoid making any quick decisions. Ask yourself whether the situation you're in makes sense and question whether it could be a scam.

Do your research

Research the person you're talking to and the situation that you're in, using online resources. If other people have been in the same scam situation, you may find more information online to confirm it isn't legitimate.

Talk to someone you trust

Ask for advice about your situation from a person you trust, such as family member or friend. Getting an outside perspective on your situation will help you identify whether it may be a scam.

If you may be a victim of fraud, report it

Report your situation to CIBC by calling 1 800 465-2422 or by visiting your local banking centre.

To learn more about how to spot different types of scams and ways to protect yourself, visit **cibc.com/fraud**.
You can also visit the Canadian Anti-Fraud Centre website or contact them at **1 888 495-8501**.

To learn more about tax scams, visit the Canada Revenue Agency website or contact them at **1 800 959-8281**.