Recognize Fraud

March is Fraud Prevention Month

Everyone plays a role in the fight against fraud. Learn to recognize, reject and report it.

Over the phone: Legitimate telemarketers have nothing to hide. Criminals will say anything to get your personal information or money. They might pretend to be a family member in an emergency. They might tell you that you have won a vacation, or have a hot new investment to sell. They pressure you to make a quick decision.

In a Text Message: Many businesses are turning to text messaging as a way of communicating with their customers and clients. Criminals are also sending texts about fake job offers, tax refunds, or promoting offers via links to click on. They may sound official, but legitimate organizations will not request for personal or financial information via text. If unsure, always call the organization back at a listed business phone number to confirm the legitimacy of the text.

At your Door: The aim is to convince you into purchasing a product or services you do not need. Some common door to door scams include: services for home repairs or maintenance, utility company scams, impersonating a charity, surveys, fake investment opportunities, and free home inspections.

In the Mail: Letters advising of a large inheritance, a lottery prize winning or fake cheques. Legitimate lottery companies will never request money up front in order to receive a prize. Never deposit a cheque and send a portion of the money on to a third party. Businesses can be targeted by phony past-due invoices demanding payment for a service they never requested.

In an Email: Also called *phishing*, these email messages contain links to fake websites that look like the real sites. Criminals hope you will click on the link and provide personal information and financial information. Sometimes these emails contain attachments that when opened can infect your computer with malicious viruses or spyware. Often the email looks like it came from a friend or someone in your contact list. If you are not sure, do not reply to the email, click on any links, or open any attachments. Contact the company or your friend first to verify the nature of the email.

Online scams: Ads for free trials or free gifts after completing a survey may look like a good offer. But you may be signing up for something and not know it, leading to an unexpected bill in the mail. Exercise caution if you are required to provide credit card information to pay for the free trial shipping and handling. Read the fine print before signing up for a free sample.

Criminal may post phony online classified ads or impersonate a real online store. They might sell knock-offs, or ask you to wire money somewhere to pay for an item. Before placing an order, review the website's "About Me" page, search for it on the web or on social media. Its credibility should be ascertained before placing an order.

It is important to be protective of your personal and financial information. Ask yourself:

- ***Can the offer or company/organization be verified with a credible source?*** The *Better Business Bureau* or industry registration or licensing bodies can provide consumer based information about a business. Charities can be verified through the *Canada Revenue Agency Charities Listings* at *www.cra-arc.gc.ca/chrts-gvng/lstngs/menu-eng.html*
- ***Have you had enough time to make a decision?*** Legitimate businesses will allow you time to review a contract and provide opportunities to ask for additional information.
- ***Is the risk you are taking reasonable for the expected return?*** In general, low-risk investments are in the range of current GIC rates offered by banks. If the expected return is higher than these rates, you are taking a greater risk with your money. Make sure you understand and can afford the amount of risk you're taking on. Understand the investment fully before signing any contract.
- ***Is the method of payment secure?*** Look for the "http***s"*** in the URL when using online payment platforms. Exercise caution when e-transfering funds to e-mail addresses not associated with a business domain.
- ***What happens with my personal information?*** When providing personal information, what will the organization do with the information and do they require it for the relationship you maintain with them?