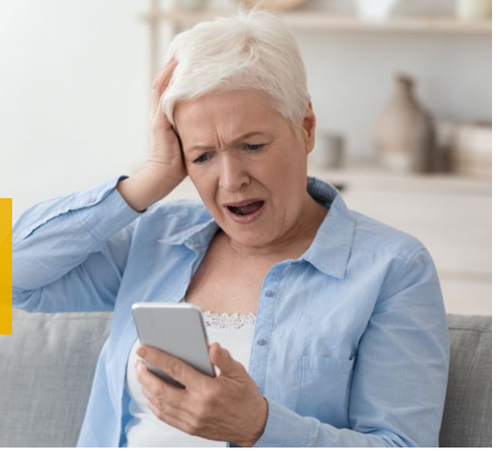
Old Dogs, New Tricks

Staying Safe in the Digital World



Written By: Brett Leclaire

Scams and fraud have been around forever – the dishonest merchant placing his thumb on the scale when weighing out goods, get rich quick schemes, vendors selling magic cure-alls, or the guy who wants to "sell" you the Brooklyn Bridge. There will always be con artists, snake oil salesmen, swindlers, hustlers – these folks aren't new; they've just learned new methods for the same old tricks.

Technology (think computers, cell phones, iPads, etc) plays a big role in our daily lives from catching up with friends, to online shopping and banking. And while there are a lot of great things about technology, there can be a shadier side. Scams. Most of us have encountered scammers through spam calls or odd emails; and with advancing technology new ways to scam people will continue to evolve. When we share social media profiles, take quizzes online that seem fun, or throw away papers with personal information on it, we are exposing ourselves to potential harm. Scams have become more sophisticated and widespread, making it easier for scammers to gather our personal information and play on our emotions. It is essential for us to stay vigilant and informed about the latest tactics to protect ourselves from falling victim.

So, where to begin? It is most important to note that while the methods and technology may have evolved over the years, the underlying principles of scams remain similar: enticing victims with false promises like offering deals or promotions on items, exploiting trust by asking more invasive questions throughout a conversation, and attempting to deceive for financial gains through asking for payment for items or services.

Staying safe from scams begins with staying informed about the latest scam tactics and understanding how scammers operate. Keep yourself updated on the latest scams and fraud schemes through a reliable source such as the Canadian Anti-Fraud Centre (https://www.antifraudcentre-centreantifraude.ca/index-eng.htm). This Government of Canada website not only has a comprehensive listing of scams, but also provides a place to report any fraud or scam activity you might have experienced.

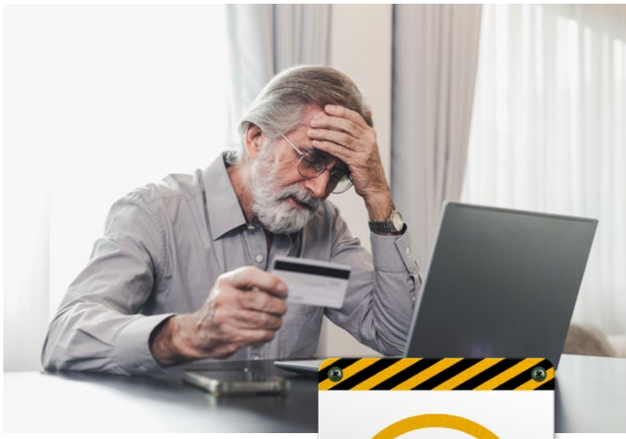
Here are some tips:

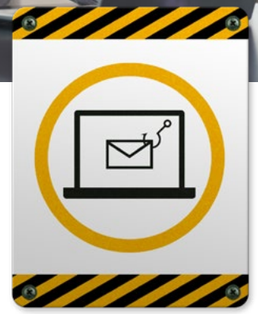
- **Be cautious with personal information and never share sensitive data with unsolicited callers or emails.** If you receive a call from someone claiming to be from your bank or a government agency asking for personal information, hang up immediately. Look up the official contact number for the organization, call them directly, and inquire about the purpose of the call. Banks, government departments, and other legitimate companies respect your right to safety so explaining to them your intentions will always be understandable.
- **Be aware of any unexpected offers or requests, especially if they involve financial transactions.** Be equally cautious when receiving emails with urgent requests to update your account information, change your password, or verify personal details. It's best not to click on any links from unfamiliar sources; however, sometimes the emails LOOK official. A good trick for this is to first check the actual email address (not just the name of the sender) to be sure it is familiar. Next hover/hold (but don't click) your mouse over any links to check the actual name of the site and make sure it matches the official website.

- **Use strong passwords for online accounts and keep your devices updated with security software.** Create unique passwords for each online account that have a combination of letters, numbers, and symbols like question marks and exclamation marks. Avoid using easily guessable information, such as your name or birthdate. Consider using a note pad to keep track of websites and corresponding passwords. Install reputable antivirus software on your computer and keep it up to date.

It can be a rollercoaster of emotions for people who have found themselves victims of a scam. Feelings of frustration, anger, regret, or shame can come from being taken advantage of. These feelings are valid, but it is important to find the right avenue to receive help as soon as possible. Talking to family members and loved ones about what happened is the first step. They can help navigate next steps to mitigate loss and damage and help identify solutions to protect yourself moving forward.

Second, be sure to report scams and fraudulent activity to the Canadian Anti-Fraud Centre (listed previously). Be sure to document the way you were contacted, what they knew about you, and any communications you still have access too. Lastly, contact your financial institutions and secure any information that may have been compromised by the scam (ie: change/update passwords). Doing so can stop any further funds from being taken from your account.





By adopting these practices and seeking advice from trusted sources, such as family members or friends who are knowledgeable about online security, you can shield yourself from scams and enjoy the digital world with confidence and peace of mind. Remember that vigilance and knowledge are your strongest allies in staying safe from fraudulent activities. This is their job so they will work hard to get what they want so we need to be careful. If it seems too good to be true, then most likely it is.

Common Scams

Watch out for these **red flags**!

- "Government" officials threatening fines or arrest.
- Utility companies claiming unpaid bills.
- "Banks" claiming overdrafts on accounts that need to be settled.
- A company claiming you have a delivery notice or unpaid invoice that you did not order/purchase
- Tech support companies claiming they need to fix an urgent issue on your computer
- A person claiming to be a relative reaching out through new numbers or email addresses asking for money.
- What looks like either your bank or the CRA requesting you to share login/any information.
- What looks like your friend/family member asking for money/wire transfer or for you to check out a link
- A random stranger or company saying you won a prize/money or an inheritance or offering an unsolicited home service or repair
- A new/newer relationship (romantic or otherwise) where the person has an "emergency" and needs your financial help
- An email claiming to have embarrassing personal/private videos/photos/information about you that they are threatening to release
- A website selling a too-good to be true or cure-all product