Baycrest
KOSCHITZKY CENTRE
for Innovations in Caregiving

Petro-Canada
CareMakers
Foundation™

ABUSE AND SCAMS

Learn How to Protect Yourself

Adapted from Constable Mark McCabe's webinar on March 16, 2022

Older adult cyber abuse is often a crime committed against those who hesitate reporting out of fear and shame.

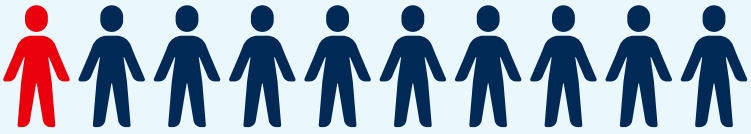
Older adult cyber abuse is perhaps more hidden today than ever before and it is all too often a silent crime committed against a population who tend to hesitate reporting abuse out of fear of embarrassment and shame. Constable Mark McCabe discusses the legal framework currently in place to empower older adults and protect them from cyber abuse. This basic guide will help you to understand how to protect yourself against the most common frauds and scams.

What exactly are scams and fraud?

Fraud occurs when someone is deceived or mislead with the intention of profiting or gaining some unfair or dishonest advantage over them.

Scams are typically fraudulent schemes aiming to cheat or defraud, often with the intent of making a quick profit.

Stigma around fraud, scams and cyber abuse



Only 5% to 10% of frauds are reported

- These are often not reported due to embarrassment
- Frauds and scams are often not perceived as a "real crime" when, in fact, they are a real crime
- Becoming a victim of fraud may leave someone feeling isolated, afraid, or embarrassed
- It is important to speak about it and report it

Common Scams

Grandparent scams

- These scams often involve someone pretending to be your grandchild in trouble
- Here are some things you can do in response to a call like this:
  - Do not say your grandchild's name, stay calm, ask questions, contact other family members to verify information before sending money, and if the caller (who claims to be your grandchild) says they are in jail or the hospital: contact the facility directly to confirm whether this is true or a scam

Social media scams

- As more older adults are present on Facebook, they are being targeted by social media scammers
- Fake pages and advertisements are posted saying things like: "Free $1000 gift card", "You won a free trip", or offering coupon vouchers
- Do not believe everything you see on social media

Canada Revenue Agency (CRA) scams

- CRA scams can be a phone call, text message, email, or letter, and can claim that you are due a tax refund or owe the government money
- Here are some things you can do in response to a call like this:
  - If you receive a refund email or text message without personally signing up for the online option – delete these and do not respond to them, you can also call the official CRA number to ask about the email you received, do not click on the links in these emails or text messages, never give credit card details asked for in these links, legitimate CRA personnel will never ask for personal information by email or text, request payments by prepaid credit cards, nor give taxpayer information to another person without authorization by the taxpayer, nor leave personal information on an answering machine, nor threaten a taxpayer
- It is important to know that scammers can change their caller ID. Call back on the number you trust.

Computer scams

- Below are some examples of different types of computer scams and some tips for how you can respond to them
  - Message pop-ups or warning saying: "Your computer may be infected, call this number" – never call that number. Show it to someone who is tech savvy and can resolve the issue.
  - Do not give a caller or person on the internet access to your computer, they may lock you out and ask for ransom. Never pay the money they as for as there is no guarantee of them doing what they say they will, and they may ask for more and more money
  - Download anti-virus software

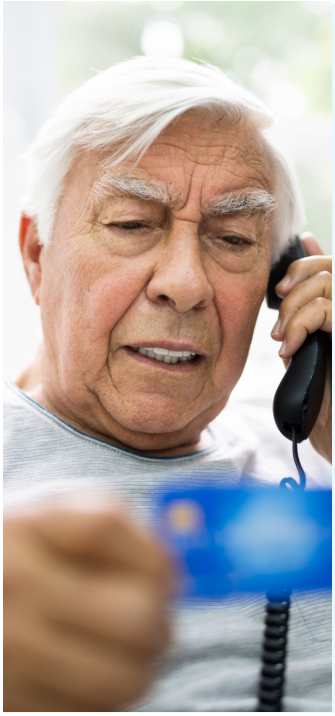
Common Scams

Bank inspector scams

- For these scams the caller typically claims to be a bank investigator who is concerned about fraudulent activity at the individual's branch. It can lead to the individual being asked to withdraw large sums of money and not telling branch staff why
- If you get a call like this, you should call a trusted number from your bank to confirm if the person who called works there. Remember, there is no sense of urgency relayed from legitimate institutions to do everything in the moment or right away. If using a landline, and the individual on the other side asks you to call the number on the back of your credit card to avoid scams, call after at least at least 10-15 minutes, as landline phones sometimes do not disconnect, and you can end up speaking to the scammer who may pretend to be a professional at the bank

Romance scams

- These can occur when someone makes contact through dating websites, apps, Facebook and social media sites, and attempts to start a conversation
- The romantic interest may never show up on video calls or in person
- If you end up speaking with someone in this way you can take the following precautions: never send money or personal information, never give someone your credit card information, cut off contact if someone starts asking you for personal or financial information, ask specific questions about details in their profile as a scammer may struggle to remember the details of a fake profile



Reporting fraud and scams

- Report frauds and scams to the Canadian Anti-fraud Centre: 1-888-495-8501
- Contact the police to report fraud and scams! In major cities in Ontario, Quebec, Nova Scotia, Alberta, British Columbia, Manitoba, Newfoundland and Labrador, and New Brunswick the police non-emergency number can be acquired by calling: 311. Police non-emergency numbers outside of these locations can be found online by region
- In Toronto, you can report scams online if below $5000: www.torontopolice.on.ca/prime/
- You can call the Senior's safety line: 1-866-299-1011
- To report a crime anonymously, meaning without sharing your name, you can call Crime Stoppers: 1-800-222-8477

Where to look to stay informed on new scams

- Canadian Anti-fraud Centre https://www.antifraudcentre-centreantifraude.ca/index-eng.htm
- Canadian Bankers Association https://cba.ca/
- BBB Scam Tracker https://www.bbb.org/scamtracker/detail/fakecheckscam-23225-VA/178083
- The Little Black Book of Scams https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/03074.html

This information is brought to you by the Koschitzky Centre for Innovations in Caregiving, and is generally funded by Petro-Canada CareMakers Foundation.

Baycrest
KOSCHITZKY CENTRE
for Innovations in Caregiving

Petro-Canada
CareMakers
Foundation™