The Dementia Society
Ottawa and Renfrew County

40 Years of Community
40 ans de communauté

Protecting Yourself and Older Adults from Fraud

Canada Revenue Agency (CRA) reported over 100,000 incidents of fraud to Canadians in 2021, noting fraud is the number one crime against senior Canadians.

Older adults are prime targets, often due to limited knowledge of technology, lack of awareness, and sometimes simply because they are home alone during the day to answer the door or phone. High levels of trust make it easy for people to take advantage of older adults.

Fraud is occurring on all platforms—by mail, phone, email, and text, not to mention internet ads and internet sites dressed up to look legitimate. Typically, **a fraudster is seeking personal information—most of all financial information like your banking and credit card details—ultimately to part you with your money.** To do this, they create emotional and too-good-to-be-true stories to entice you to provide them with the information they need to steel and profit from your identity.

Be Alert to Common Fraud Scams

Identity Theft

Stealing your personal information for criminal purposes—like purchasing items on your credit without your knowledge or consent, or impersonating you to make financial transactions or other representations—is identify theft.

> **What to know:** Identity theft can occur by postal mail; email, called 'phishing'; or computer software, through the use of 'spyware'; to gain information to allow scammers to conduct fraudulent activity in your name.
>
> **What to do:** If you find suspicious activity happening on your credit card, contact your bank immediately and have your card blocked. Check your credit score and bank accounts regularly.

If you suspect fraud, report it immediately to your local police and the Canadian Anti-Fraud Centre (1-888-495-8501).

Call the Canadian Anti-Fraud Centre (1-888-495-8501) or 911 if you sense you are in danger.

In cases where you become concerned for your personal safety, such as if someone tries to scare you via email or by phone claiming you are suspected of fraud or that a

This information was compiled from the following sources: Canada Revenue Agency, Elder Abuse Prevention Ontario, Canadian Anti-Fraud Centre.

relative/loved one is in danger – try to stay calm. Do not react or follow the scammer's instructions, and do not share sensitive personal information—like your address, or bank or credit card information.

If you suspect a call may be fraud or it makes you feel uncomfortable, tell the caller to call back later and immediately seek help from someone you trust.

Grandparent Fraud

You receive a phone call from someone claiming to be your grandchild. The caller says that they have been arrested and they urgently need you to send money or gift cards to pay for their bail.

The fraudster will make it difficult for you to understand what they are saying or to recognize the voice to get you to fill in the blanks as to who they are. They can be incredibly convincing and count on your emotional reaction. Victims of this crime report that the fraudster lead them to believe that a 'Gag Order' was put into place to protect the identity of the police officer collecting payment. This fake secrecy demand puts victims in an awkward position; making it difficult to tell anyone about the demand for money from a family member.

What to know: Police never ask for money for bail from family members, nor do they issue 'Gag Orders'. Bail Hearing in Canada takes place in Court and does not necessarily involve money. If there is a financial penalty involved, it is not paid up front to a police officer, by pre-paid gift cards or via transfer to someone's bank account.

What to do if you get a call like this:

- Never confirm any personal information over the phone.
- Always verify who is calling. Ottawa Police recommend that if it is a family member—as they claim—tell them you will call them back and use the number you have for this person. Do not use a number given by the caller. Use 411 or the Internet to get the phone number if you don't have it.
- Don't be pressured. Take some time to process what you have been told, to see if it makes sense. Ask a trusted friend or family member for their opinion, or if in doubt, call your local police service.

Prize Scam

You receive a call or an email claiming you have won a lottery, or offering a prize such as money or a car, or even both. However, to obtain the prize you must submit a payment to cover costs such as taxes or shipping.

What to know: Scammers may ask for payment in e-transfer or gift cards, or even cash. This is likely a fraud.

What to do: Do not share your address, bank details, purchase and send gift cards or e-transfer money in response to such requests. End the call immediately; this is not the time to be polite!

This information was compiled from the following sources: Canada Revenue Agency, Elder Abuse Prevention Ontario, Canadian Anti-Fraud Centre.

Tax and Fine Fraud

Someone contacts you alleging they are from a government agency, like CRA or a law enforcement agency, asking for sensitive data like your Social Insurance Number, and/or credit card details (including the CVV—those three digits printed on the back of a credit card, above the signature box). A scammer will typically say you need to provide this information because you have funds owing to the government or law enforcement, for example, taxes or duties, overdue fines or that you have a warrant outstanding and if you do not pay them you will be arrested. This is a scam. Do not provide any information; simply hang up.

What to know: Government agencies like CRA or law enforcement never call to ask for private data, nor rush you to share information. Never share your SIN, credit card or its CVV number in a phone call or with a person you don't know and trust.

What you can do: Resist acting on the callers' demands. If you find a call to be suspicious, ask the caller to call back later when you know there will be someone there to help you. Or, email or call the company's official number to ask if they had called to ask for details.

Payment Fraud: Prepaid Cards, BitCoin, and e-Transfers

Beware of suspicious requests asking for immediate payments. The caller might ask you to withdraw a sum of money in cash or to make an e-transfer, or to purchase store gift cards (i.e. pharmacy or grocery cards loaded with large sums), or to purchase cryptocurrency like Bitcoin to make payments. These are all non-traceable forms of payment. Once transferred or sent to the scammer, there is no way for the authorities to trace and recover your funds.

Keep It to Yourself

- Social Insurance Number (SIN)
- Bank account and banking passwords
- Credit card details
- PIN numbers
- Social media and email passwords
- Your birthdate
- Your address
- Your living situation (i.e. "I live alone")

Avoid sharing with people you do not know or trust.

What to know: Never provide any personal information like financial details (i.e. banking, credit card, etc.), your address, or living situation (i.e. do not say if you live alone).

What to do: Ask the caller to call again later; usually, a scammer will not call you back. If they do, hang up or better, screen your calls and only answer calls from people you know and trust. You can also call the company's official number

This information was compiled from the following sources: Canada Revenue Agency, Elder Abuse Prevention Ontario, Canadian Anti-Fraud Centre.

available on their official website to confirm if there is a pending payment, or to verify whatever the caller said.

Fraud via Text Message

Text message scams are on the increase. Beware of text messages from unknown individuals or numbers that ask you to click on links, ask you for payments, or claim that you have won a prize, or about a random package delivery.

What to know: These types of scams are also lures to get more information and money from you. Unless perhaps it's your birthday, deliveries for items you did not order are likely not real. And generally, you should not have to provide money to redeem a prize. And just like they will not contact you by phone or email for personal information, government agencies do not ask for personal details over text.

What to do: If you click on the link and find it suspicious, or if does not take you to an official website, close the tab and do not go further, and do not share any personal information. Better yet, don't click, just delete the text altogether.

A scammer may try to entice you with the promise of a great prize, a story of a personal or family emergency—theirs, or a fictitious story involving yours, or they may want you to believe you've done something incorrect or even illegal—just to get sensitive information to take advantage of you and your money.

Organizations you would want to do business with do not operate this way.

Be Fraud Aware: Recognize The Signs

- The communication is unexpected.
- The request makes you feel pressured to act immediately.
- You are randomly offered cash or a prize.
- You are told you are lucky and that such offers are rare.
- You receive bills, subscription messages and delivery tracking links from companies you did not sign up for, nor did you make a purchase from them.
- You receive unsolicited emails from individuals or organizations prompting you to click on an attachment or link. Check the sender's email id and the link. Often, scammers have completely different email addresses than the organization they purport to represent.
- You are asked to send money via wire transfer service, courier, BitCoin, e-transfer or prepaid cards—all non-traceable means of acquiring funds.
- You are asked not to discuss the purchase/offer details with others, so the scam is not discovered by family members, neighbours, etc.

This information was compiled from the following sources: Canada Revenue Agency, Elder Abuse Prevention Ontario, Canadian Anti-Fraud Centre.

Scam situations can be overwhelming and scary. But there are ways to protect yourself and the older adults in your life. Don't shy away from asking for help if you need it.

Tips to Stay Alert and Stay Safe

Say NO—don't hesitate to assert yourself. And there's no need to be polite.

- No pressure. Never make a decision that feels immediate, sudden or uncomfortable.
- Don't share. Never give out personal information or financial details regardless of the situation even if someone claims the information is necessary for medical information like vaccinations, medicine or prescriptions, insurance or government institutions such as the Canadian Revenue Agency (CRA), or Immigration and Citizenship Canada (IRCC).
- Keep an eye on your credit. Check your credit card statements, bank accountand credit report regularly.
- Be Safely Social. Review your privacy and security settings on all your social media platforms and Web services, including email like Gmail or Yahoo!
- Watch where you click. Never respond to or click a suspicious link or attachment on any of your devices, this can lead to hackers taking over your computer to steel sensitive information. Similarly, don't respond to suspicious texts or pop-up windows. Delete immediately!
- Who's there? Make sure to read the sender's email address (see the "sent from" name in your email), and make sure it is from the legitimate company or government email. For example, it says from apple.com and not no_reply@email.apple.com.
- Don't get personal. Never give out personal information (such as your birthdate, address, a Social Insurance Number, credit card number, bank account number or passport number) by telephone, email or text.

Be alert that frauds exist and could happen to anyone, including you.

What to Expect from Government Communications

- Government communications typically come by postal mail. Government departments and agencies like CRA will not contact you to request information by email or by text.
- Government agencies will never threaten or ask you for immediate payment, payment by credit card, or via a money wiring service.
- Consider that the "government employee" asking for your personal information over the phone should already have certain personal information, like a SIN number, on your file.

This information was compiled from the following sources: Canada Revenue Agency, Elder Abuse Prevention Ontario, Canadian Anti-Fraud Centre.

- There is no need to take immediate action, contact the real agency before you give out your personal information.
- If you suspect someone is posing as a government representative for the purpose of committing fraud, contact 1 800 O-Canada (1-800-622-6232) to verify the validity of any communication you have received (including government websites).
- Contact 1-800-959-8281 if you suspect scammers impersonating the CRA are contacting you.

Keep Informed

The following trusted resources can help you to report a fraud crime and learn more about what you can do to protect yourself and senior adults in your life.

Canadian Anti-Fraud Centre

If you suspect or are experiencing a fraud/scam, report it.

1-888-495-8501 or www.antifraudcentre-centreantifraude.ca

Competition Bureau

File a complaint about false or misleading advertising at:

1-800-348-5358 or www.competitionbureau.gc.ca

Crime Stoppers

Report crimes anonymously.

1-800-222-TIPS (8477) or www.canadiancrimestoppers.org

Ottawa Police

911 or report online at https://www.ottawapolice.ca/en/contact-us/find-a-police-station.aspx

Seniors Safety Line (SLL)

1-866-299-1011 or www.awhl.org/seniors

To learn more about fraud in Canada, prevention and tips to stay safe, please visit the links below:

Canada Revenue Agency

Canadian Antifraud Centre

Elder Abuse Prevention Ontario's Scam Brochure

Elder Abuse Prevention Ontario's Financial Abuse Brochure

Connected Canadians– article about "phishing" email scams for seniors, available in over 200 languages.

Royal Canadian Mounted Police – Seniors guidebook to safety and security

This information was compiled from the following sources: Canada Revenue Agency, Elder Abuse Prevention Ontario, Canadian Anti-Fraud Centre.

Canada Employment and Social Development: Learn about fraud scams
https://www.canada.ca/en/employment-social-development/corporate/portfolio/service-canada/fraud.html

This information was compiled from the following sources: Canada Revenue Agency, Elder Abuse Prevention Ontario, Canadian Anti-Fraud Centre.