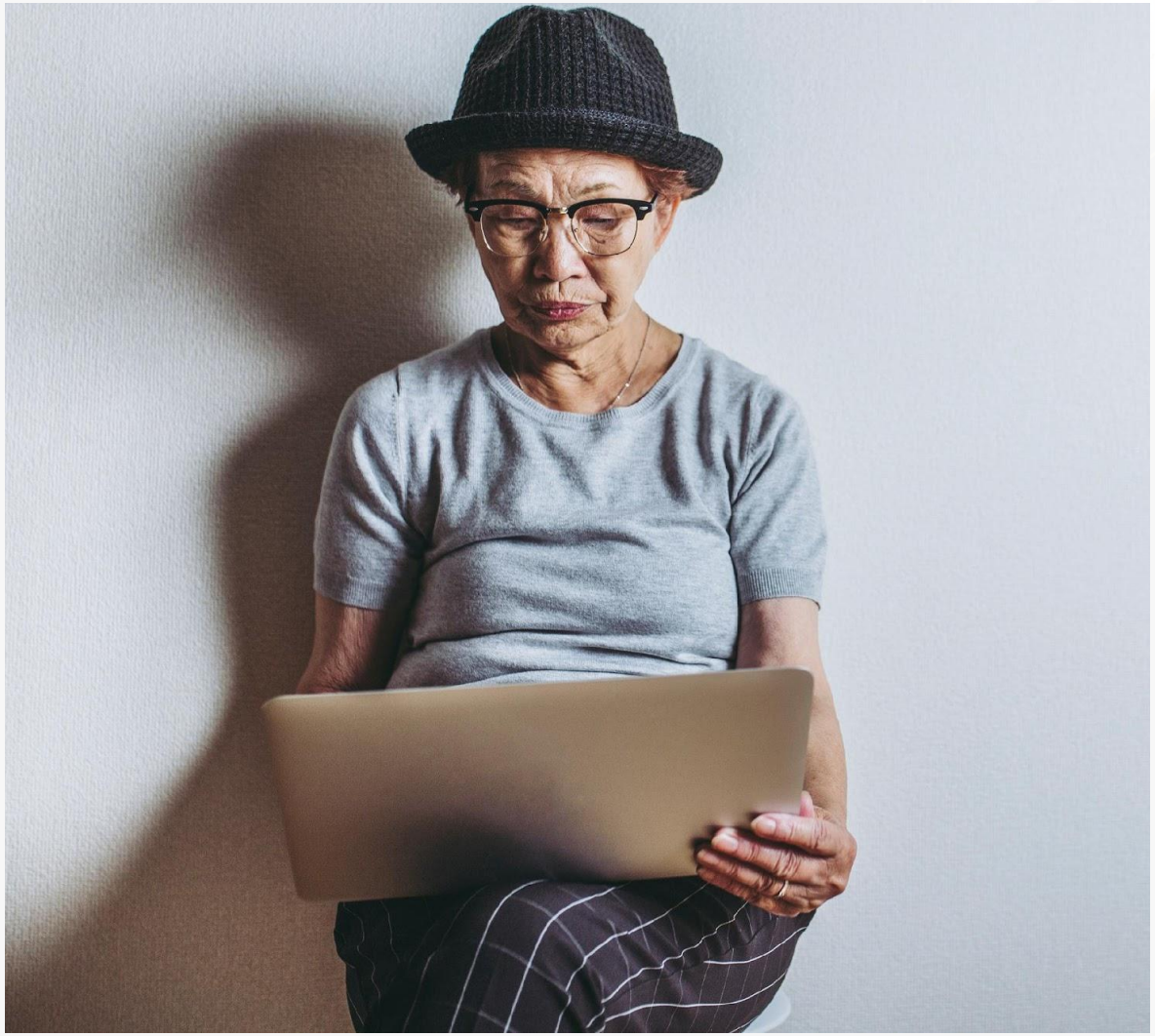
International Women in Cyber Day - Sept 1st Symposium 2022

‘Education, Safety, and Security of Women and Girls’

Digital Safety for Older Women: Preventing Cyber-Crimes and Scams



Advancing and retaining women in cybersecurity!

Digital Security for Older Women: Preventing Cyber-crimes and Scams

- ❑ Technology as a tool of abuse against older women
- ❑ Key tactics fraudsters use - Be aware!
- ❑ Types of cyber frauds and scams
- ❑ Safety tips
- ❑ What to do & Who to report to
- ❑ Talking with older adults about frauds & scams
- ❑ Resources for Support

Technology as a tool for abuse against older women

- **Gender-Based Violence** (in a relationship)
- **Financial abuse** (family, friends)
- **Frauds and Scams** (usually by strangers)

Financial Abuse

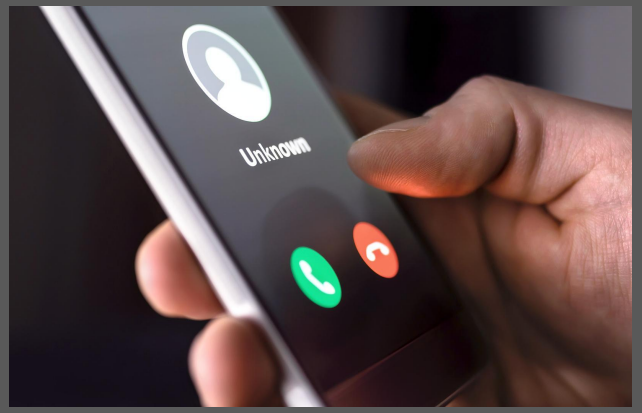
Elder Financial Abuse :

persuading, intimidating, harassing or tricking older adults out of their money, property, or possessions that results in a monetary or personal gain to the abuser and/or monetary or personal loss for the older adult.

Misusing a power of attorney is a common form of financial abuse.

A national Canadian study revealed that in situations of financial abuse, the perpetrator was an adult child or grandchild in 37% of incidents. (Mustel Group, Metro Vancouver and the Capital Regional District 2017)

SCAMS & CYBERCRIMES CAN HAPPEN TO **ANYONE**, ANYWHERE, AT ANY TIME



#TippingTheScale

Scammers' key tactics

Scammers know how to tap into our vulnerabilities

- **Create a sense of urgency:** whether it is a limited time offer, a deadline you cannot miss, or an emergency affecting your "Grandchild'', the clock is always ticking and they require you to make a decision in the moment.

- Often, this will be associated with **pressure, sometimes threats** of consequences if you don't.

- Alternatively, sometimes consecutively, they will also **build an emotional connection**. For potential victims who are lonely or isolated, this can be alluring and may lead you to trust a stranger.

- **Ask to send money** by wire transfer or money transfer service (MoneyGram and Western Union), or cryptocurrency, such as Bitcoin.

FRAUD IS UNDER REPORTED

It is estimated that **less than 5%** of fraud is reported to the cafc.

TOP 10 FRAUDS BY NUMBER OF REPORTS

Fraud Pitch	Reports	Victims	Dollar Loss
Extortion	30, 292	9650	$16.4 million
Personal Info	9706	5619	N/A
Phishing	6942	1638	N/A
Merchandise	6249	4811	$14.2 million
Job	4429	1793	$4.4 million
Service	3593	2031	$6.3 million
Sale of Merchandise	3571	2119	$5.5 million
Spear Phishing	1680	794	$29.9 million
Romance	1531	991	$27.8 million
Emergency	1301	407	$1.4 million

CAFC, 2021

TOP 10 FRAUDS BY DOLLAR LOSS

Fraud Pitch	Reports	Victims	Dollar Loss
Investments	487	449	$38M
Romance	332	251	$19.1M
Service	1525	1051	$4.9M
Extortion	2483	391	$4.5M
Bank Investigator	858	339	$2.5M
Prize	580	165	$2.5M
Timeshare	30	25	$2.1M
Foreign Money Offer	112	13	$2M
Emergency	573	181	$1.9M
Grant	227	117	$1.5M

Main forms of scams

- ★ Romance Scams
- ★ Grandparent Scam
- ★ Phishing and Smishing
- ★ CRA Scams
- ★ Spoofing
- ★ Identity Theft
- ★ Subscription Traps & Health and Medical Scams

ROMANCE Scam

Fraudsters quickly profess their love to gain their victims' trust, affection, and money.

Canadians lost

$43M

from romance scams in 2021.

*Reported by the Canadian Anti-Fraud Centre

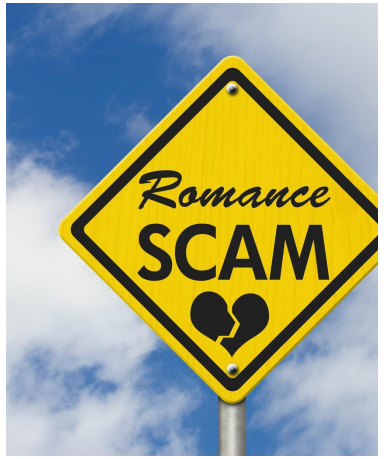
ROMANCE Scam

- Prey on you on popular, legitimate dating sites as well as on fake ones.
- Send a few messages and a good-looking photo of themselves, or of someone they claim to be.
- Once trust is quickly gained, scammers begin to ask you to send money. They may claim to have a very sick family member or a desperate situation with which they need your help. Once you give them money, they often disappear.
- To keep you writing back and paying, the scammer may hook you in with vague emails about their love and desire for you.

ROMANCE Scam

Protect Yourself:

- Make sure you only use legitimate and reputable dating sites
- Never send money or give financial details on a dating site.
- Beware of individuals quickly professing their love for you.
- Never send intimate photos or video of yourself as they may be used to blackmail you.
- Remember that it's very unlikely that someone will declare their undying love to anyone after only a few letters, emails, phone calls or pictures.



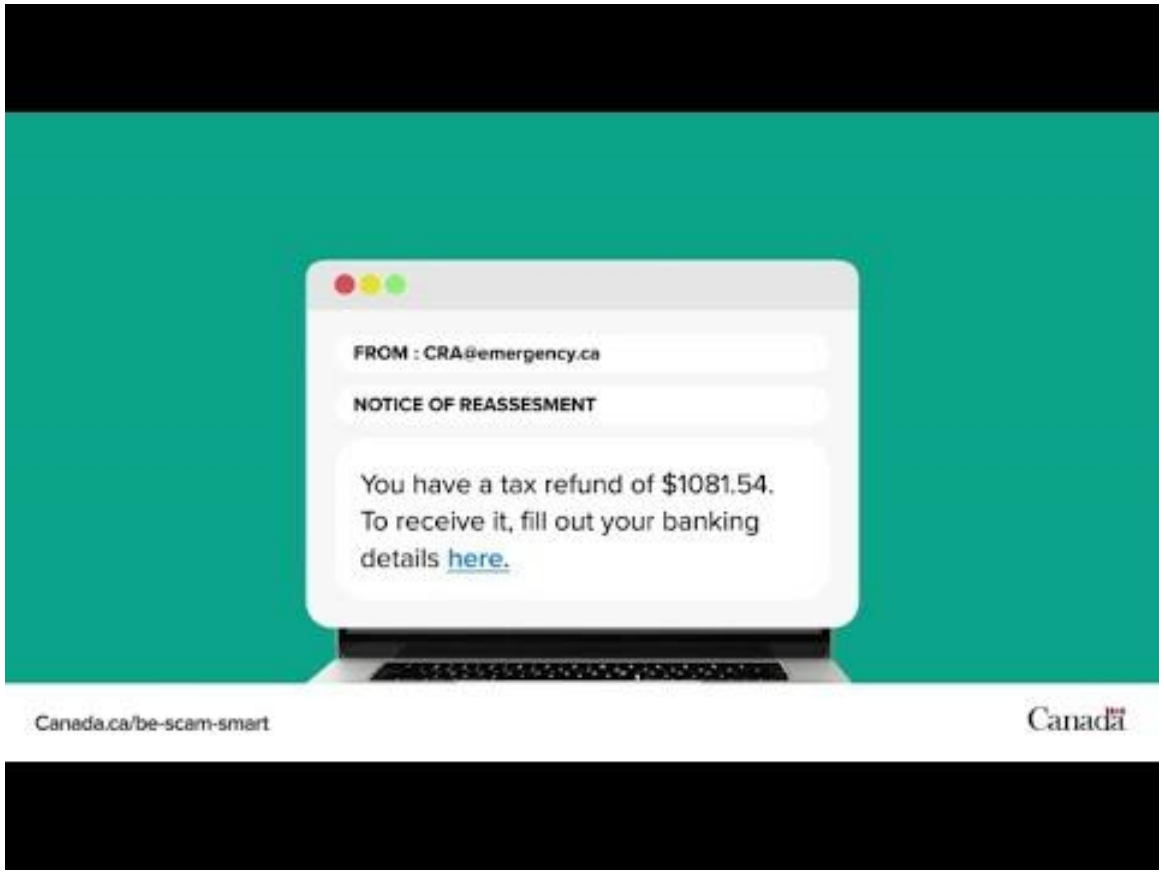
Source [The Litltle Black Book Of Scams]

Emergency or “Grandparent” Scam

This occurs when someone posing as a family member or friend contacts you in urgent need of cash because of an accident or arrest while travelling abroad. **They ask you to wire or transfer money.**

The scam is often targeted to older adults in late evening or very early in morning. Scammers use social media (facebook), the internet and phones to target potential senior victims.

Request payment methods in form of Gift cards (iTunes, Google Play) Money transfers such as Western Union, MoneyGram or Bitcoin.


FROM : CRA@emergency.ca
NOTICE OF REASSESMENT
You have a tax refund of $1081.54. To receive it, fill out your banking details here.
Canada.ca/be-scam-smart
Canada

PHISHING AND SMISHING

Phishing messages will direct you to click a link to capture your personal and/or financial information on-line.

Smishing - via text messages

Source [The Litltle Black Book Of Scams]

Canadian Anti-Fraud Centre
July 20 ·

We have received reports of phishing emails impersonating the CAFC. The emails look like the automated emails sent when we receive a file through our Fraud Reporting System. The email asks you to click on a link to view your report. The CAFC DOES NOT provide links to submitted reports. DO NOT CLICK ON THE LINK! If you have received a similar email (as seen below), report it to the CAFC: https://antifraudcentre-centreantifraude.ca/report... #kNOwfraud #showmetheFRAUD #BeScamSmart

---

From:
Sent: July 18, 2022 10:52 AM
To: Documents
Subject:

-----Original Message-----
From: Canadian Anti-Fraud Centre <no-reply@antifraudcentre.ca>
Sent: July 15, 2022 4:34 PM
To:
Subject: CAFC Fraud Complaint Intimation

Canadian Anti-Fraud Centre - Fraud Reporting System

Complaint ID for reference is: 2022-82750

A Fraud Complaint with your Personal Information has been provided to the CAFC. The details of your circumstances have been added to a national fraud database for information purposes and may be shared on a priority basis for the purposes of investigation and disruption of criminal activities.

Please find the details of the Complaint here https://mountainbuffalo-my.sharepoint.com/:u:/g/personal/admin_mountainbuffalo_onmicrosoft_com/Eef6kjrkSkhltGYHTUhIRBABdZgkoil-ubupt3XioXE_xQ?e=Cw1epQ

If you need to update your file you will need to call our toll free number at 888-495-8501 (North America Only) or 705-

Source: CAFC Facebook - July 20, 2022

CRA Scam

Receive email or text message or on social media site, informing you of a pending refund from Canada Revenue Agency. You are instructed to **click a link** to confirm your personal information to receive the refund.

Email appears to be a legitimate in looks - logo - *ask you to provide* information such as, a social insurance number, bank account number, or passport number.

Watch out—this too good to be true situation is exactly what a tax scam looks like.

Phishing

Protect Yourself

- Do not open or click the link in unsolicited emails or text messages.
- Look for spelling and formatting errors.
- Verify the hyperlink behind the link's text or button by hovering over the text.
- Do not click on any suspicious links as they can contain malware

Source [The Litltle Black Book Of Scams]

SPOOFING

Like Caller ID - fraudsters are also able to alter the sender's information in emails and text messages.

They use spoofing tactics to display the name, phone number or email they want you to see.

In emails, you should be able to *hover over* the sender's name, hit reply or look at the email's properties to reveal the sender's real email address.

Source [The Litltle Black Book Of Scams]

Spoofing

- Do not assume that phone numbers appearing on your call display are accurate
- End the call and contact the agency or company in question by making the outgoing call
- If you receive a call from the CAFC`s phone number, report it to the CAFC

IDENTITY THEFT

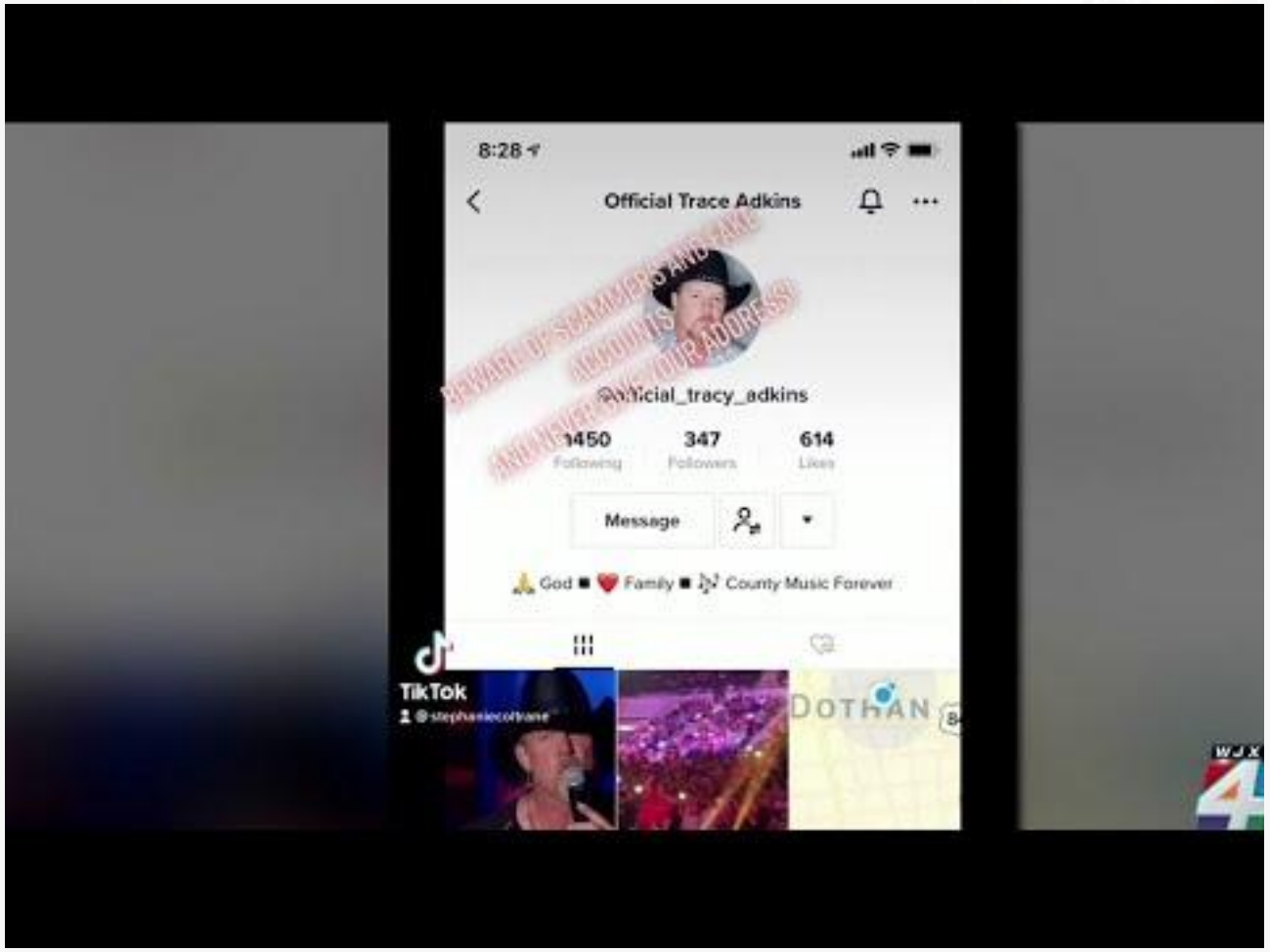
Identity theft occurs when someone uses your personally identifying information, like your name, social insurance number, credit card number, without your permission to access your money, apply for loans or mortgages, apply for government benefits and many other crimes.

- Occurs online, over the phone, or without engaging a victim in any way by stealing their information.

Source [The Litltle Black Book Of Scams]

SCAM ALERT Impersonating a famous person

Online Impersonation



https://www.tiktok.com/@plant_queens1/video/7123073000345275691

IDENTITY THEFT

Protect Yourself

- Never provide your personal information
- Avoid public computers or Wi-Fi hotspots
- Create strong and unique passwords -Password-protect your devices and home Wi-Fi network.
- Use a secure and reputable payment service when buying online
- Avoid giving out personal information on social media.
- Always shield your PIN when using your card.
- Shred and destroy documents with personal information.

In the wake of a fraud, victims can experience the following symptoms:

- Loss of appetite
- Insomnia
- Persistent feelings of anxiety
- Regret
- Embarrassment and shame
- Ongoing anger and resentment
- Depression and even suicidal thoughts

Providing Support:

- ★ Be empathetic, do not judge
- ★ Present options and ask the person what she wants to do
- ★ Offer your help and support
- ★ Do they want to share?

Be empathetic - ‘I’m really sorry this happened to you, let’s figure out how to get through this together.’

Older adults and their trusted family members should work out a plan for helping each other with finances.

What To Do If You're a Victim of a Fraud/Scam

- Gather the information pertaining to the fraud.
- Report the incident to your local law enforcement as soon as possible.
- Report the incident to the CAFC.

1-888-495-8501

Online: Fraud Reporting System

www.antifraudcentre.ca

What To Do If You're a Victim of a Fraud/Scam

First Steps

➔ **Collect your thoughts and stay calm.**

➔ **Stop all communication with the fraudster or scammer**

1. Correspondence with the scammer (i.e. Letters, emails, text messages, dates, times, names and contact information)
2. Financial statements
3. Credit card Receipts / money order receipts
4. Contracts / Shipping envelopes
5. Contact information the scammer used to contact you (i.e. Phone numbers, email addresses)
6. Websites and social media accounts used (chatroom or texts,print hard copies)

Source: www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04339.html

What To Do If You're a Victim of a Fraud/Scam

- Write out a **chronological statement** of events.
- Contact the two major **credit bureaus** (Equifax, TransUnion) ask for Credit Report
- Review your financial statements and n**otify Bank and credit card company**(s) of any suspicious activity .
- If fraud occurred **online report** to the website (i.e. dating website).
- If you suspect that your mail has been redirected, notify **Canada Post**.

What To Do If You're a Victim of a Fraud/Scam

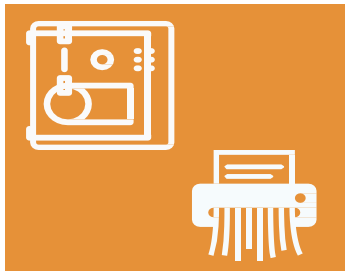
Scammer gets your username and password

- Create a new, strong password.
- Do not use use the same password for all devices.
- Change passwords to accounts (banking and online), including social media sites

Unauthorized transfer from your bank account

- Contact your financial institution and tell them about any unauthorized debits or withdrawals.
- Monitor your account to ensure there are no further unauthorized transactions.
- Place flags on all of your accounts
- Change your account numbers and/or your PINs, and get new debit and credit cards.

Quick Tips to Protect Your Personal Information in Cyberspace

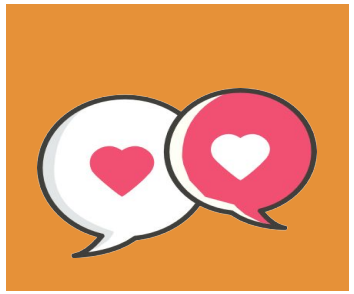


- Lock up personal documents
- Shred documents, bills, bank statements…

- Caution giving personal information over the internet.
- Don’t be afraid to delete emails.
- Spam blocking on phone.
- Do not send the scammer any money for any reason.

- Be aware of any unsolicited emails or correspondence where you are asked for, or to verify, private and personal information.
- Watch out for fake or deceptive ads, or spoofed emails.
- Don’t click on links in emails - be cautious what you download.
- Protect your computer - use reputable antivirus software

Quick Tips to Protect Your Personal Information in Cyberspace



- Be suspicious when someone online you have not met professes their love for you.
- If you use social media, limit the amount of personal information you post and only add people that you know.

- Be cautious when chatting online to an individual who claims to live close but works overseas.
- Never share your user name or password.
- Create unique passwords and change often.

- Control your own banking when possible.
- Routinely monitor financial accounts and billing statements online for any transactions you didn't make.
- Do not provide your pin or anyone access to you credit/debit cards.
- Always do your due diligence and never send recovery money

REACH OUT FOR SUPPORT / Report

Report it

The best thing you can do is to report the fraud, whatever the amount, to the appropriate authorities.

Warn your friends and family of any scams you come across!

Local Law Enforcement (i.e. RCMP, OPP)

Report the fraud or scam incident to your local law enforcement to ensure they are aware of the scams that are targeting the area.

If a victim of scam, make a report and request the file or occurrence numbers for future reference and/or ask for a copy of the police report.

Keep a log of all calls and document your actions.

Visit : www.rcmp.gc.ca Visit : www.opp.ca

Report it

Canadian Anti-Fraud Centre/ Le centre antifraude du Canada

CAFC provides valuable assistance to law enforcement agencies by identifying connections among seemingly unrelated cases.

Toll-Free 1-888-495-8501

Online through the Fraud Reporting System (FRS)

Visit : www.antifraudcentre-centreantifraude.ca/index-eng.htm

Spam Reporting Centre

Information provided is an essential part of the intelligence the Spam Reporting Centre gathers on spam and electronic threats.

Enforces the Canada's anti-spam legislation.

★ Use an online form to report spam or submit information about other electronic threats.

www.fightspam.gc.ca

Check Credit Report

Equifax and TransUnion

Request from each agency a copy of your credit report and then review it carefully to see if a scammer opened any accounts or incurred debt in your name. Also ask to put an alert on your credit report in case future scam attempts are made under your name.

Equifax : 1-800-465-7166 or www.equifax.ca

TransUnion : 1-800-663-9980 or www.transunion.ca

Sources: Consumer Protection Ontario
www.ontario.ca/page/report-scam-or-fraud#section-0

Report to Government Agencies

Competition Bureau

Handles reports of misleading or deceptive marketing practices.

Call : 1-800-348-5358
Visit : www.competitionbureau.gc.ca or Online form: online complaint form

Ministry of Government and Consumer Services

Inform so other people can be warned about the scam.

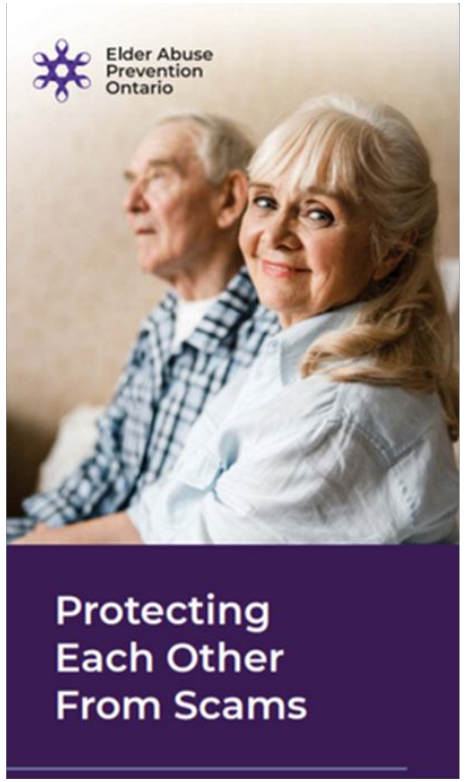
Call : 1-800-889-9768
Visit : www.ontario.ca/consumer

Canada Revenue Agency

You can call the CRA to confirm account and if any balance is actually owing.

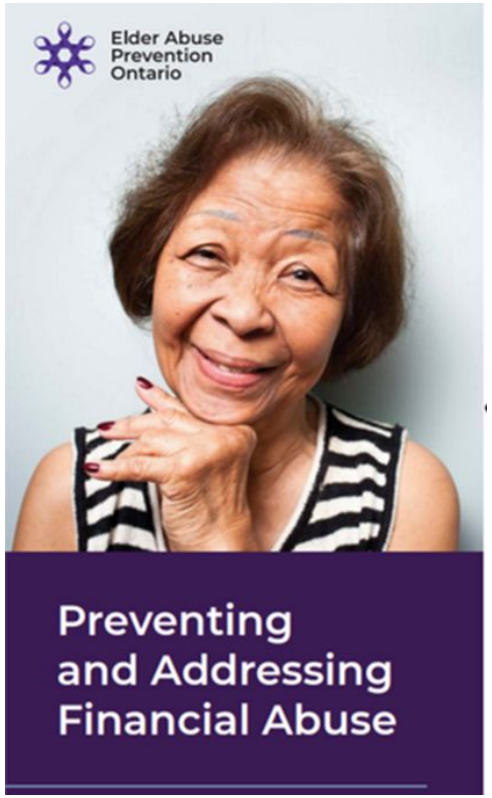
Call : 1-800-959-8281
Visit : www.canada.ca/en/revenue-agency

Tools and Resources



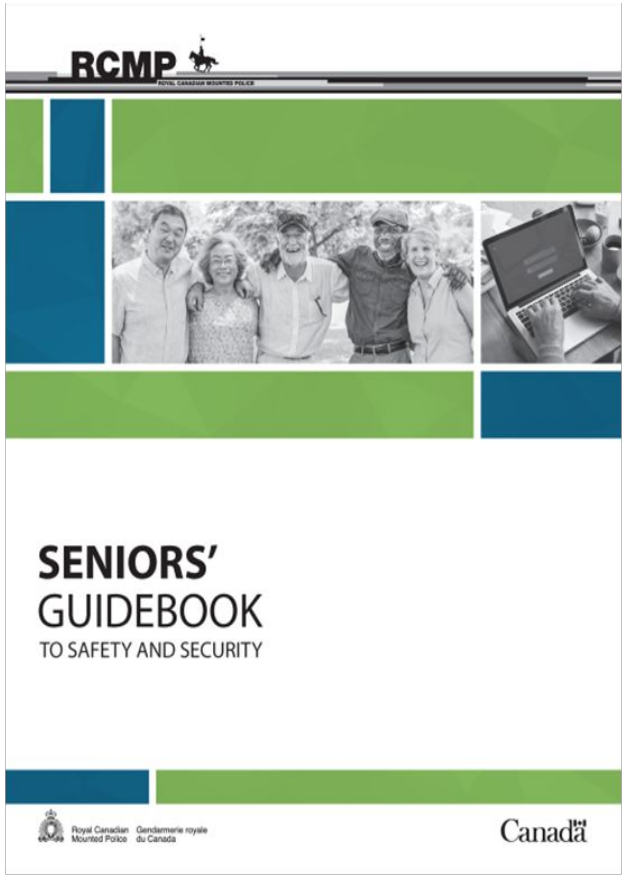
Protecting Each Other From Scams
Download in: English

Safe and Sound: A tool to Guard your Financial Security
Download : English | French | Farsi | Punjabi | Russian



Download Brochure in: English | French

Tools and Resources



[Seniors Guidebook to Safety and Security]

https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04333.html

Contact Us

Bénédicte Schoepflin
Executive Director,
Canadian Network for the Prevention of Elder Abuse

Tel: 604.715.1007

@cnpea

www.cnpea.ca

Raeann Rideout
Director, Strategic Partnerships
Elder Abuse Prevention Ontario

www.eapon.ca
Tel: 705.927.3114

@EApreventionON

www.eapon.ca

Speak up ...
Report
CyberCrimes!

Questions