



CANADIAN NETWORK for
the PREVENTION of ELDER ABUSE
RÉSEAU CANADIEN pour la PRÉVENTION
du MAUVAIS TRAITEMENT des AÎNÉS



Elder Abuse
Prevention
Ontario

● **WEBINAR**

Think before you click! *Staying Safe Online*

 24th October  1 PM - 2 PM

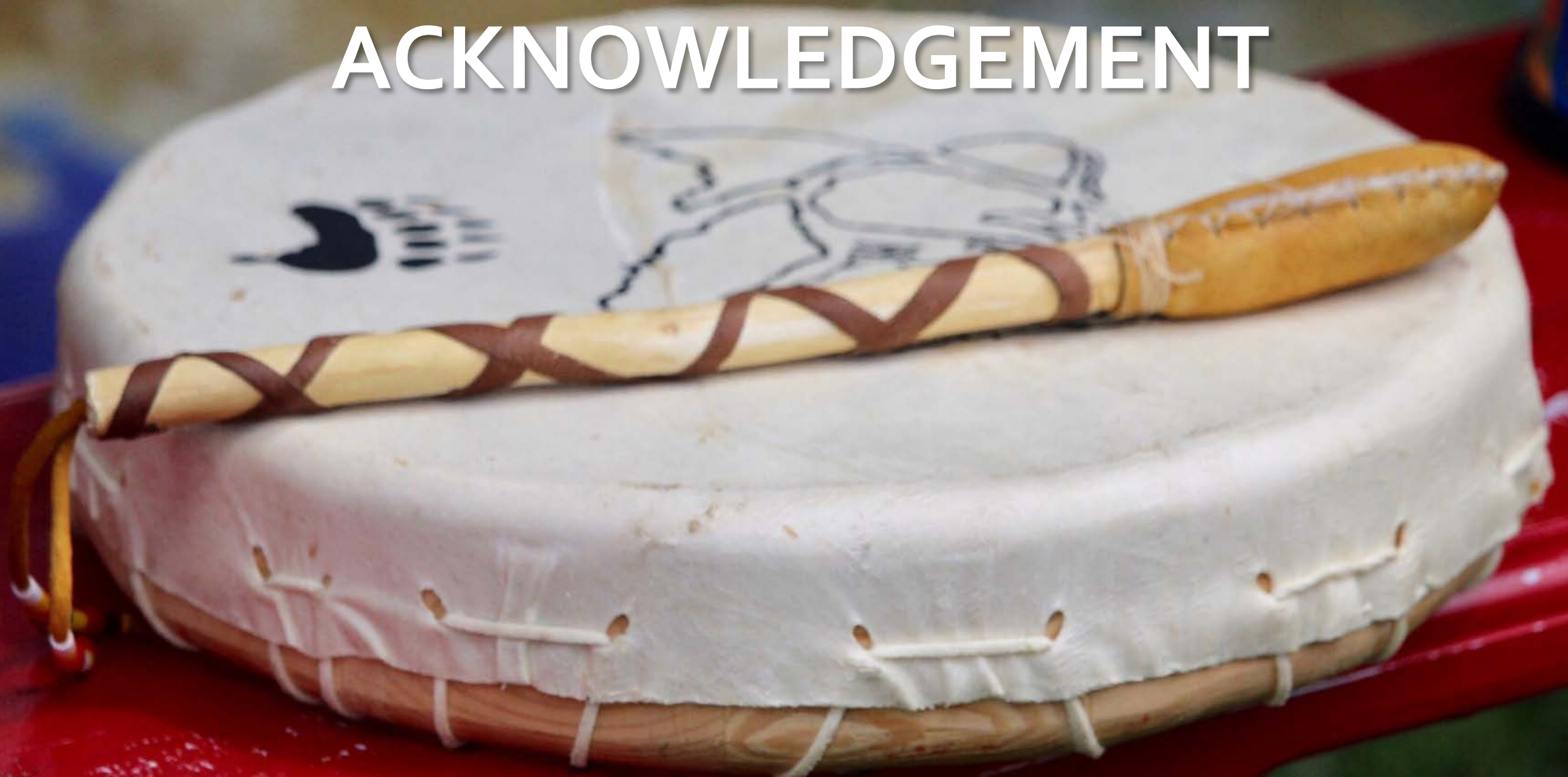
Speaker:

Stephanie Senecal

OPP Civilian Member &
Senior Support Coordinator,
Canadian Anti-Fraud Centre



LAND ACKNOWLEDGEMENT



WEBINAR LOGISTICS

Communication

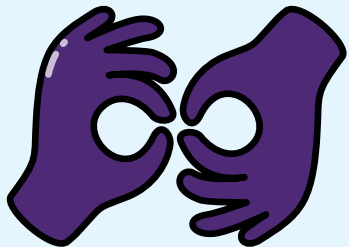


Microphones: All attendees will be muted during the webinar.

CHAT Box - Welcome to post comments during the session.

Q & A - Type your questions in Question/Answer Box and addressed after the presentation.

ASL



- **Image and name** (ASL Interpreter) on screen
- **Speaker /Gallery view:** Grid at top of right corner of screen - choose the layout you prefer on your screen
- **Closed Captioning:** Enable or Disable

WEBINAR LOGISTICS

Evaluation



Your feedback on knowledge gain from the session and suggestions for future topics is appreciated.

- Follow-up email with survey link

Recording



A recorded version of this webinar will be available on our EAPO and CNPEA websites.

Links and documents shared during the webinar will also be posted.

Respecting Privacy and Confidentiality



We appreciate there may be personal circumstances or issues which participants may wish to address. However, in keeping with our commitment to maintaining your privacy and confidentiality, today we will be answering general questions posed through the Q&A.

If someone wishes to discuss specific circumstances, we invite you to contact EAPO following this webinar to arrange for a confidential conversation so that we may further assist you.



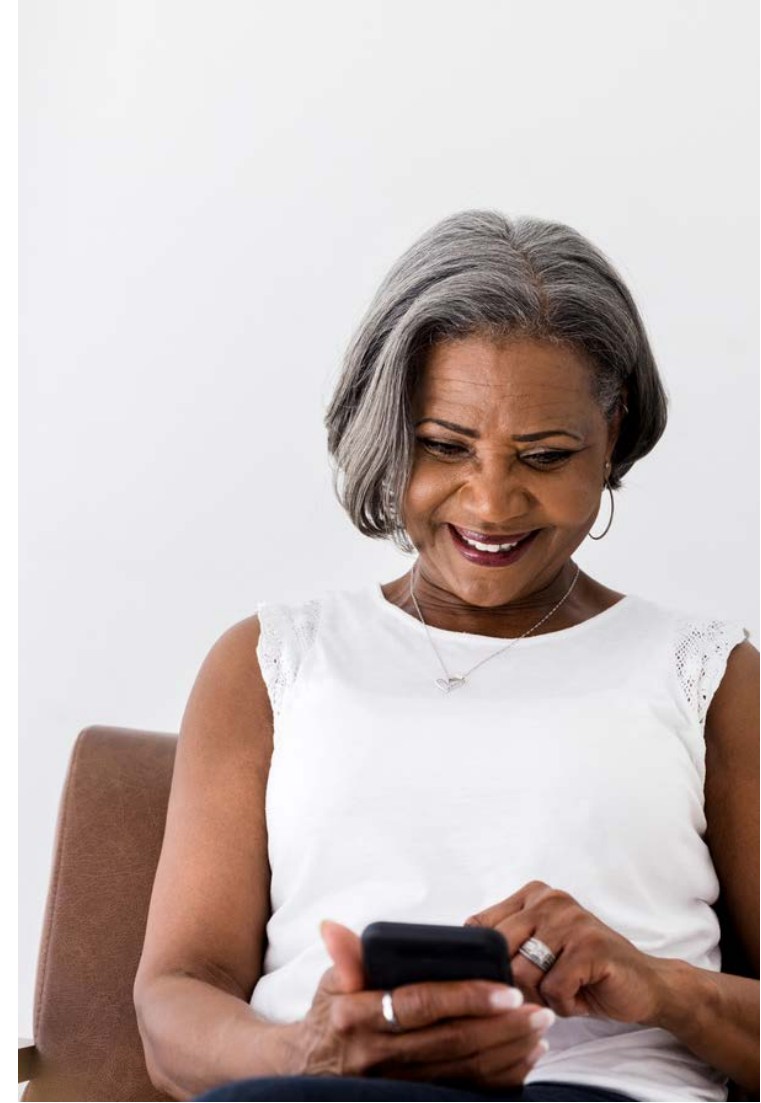
**Elder Abuse
Prevention
Ontario**

Vision

EAPO envisions an Ontario where ALL seniors are free from ageism and abuse, where human rights are advanced, protected and respected.

EAPO is mandated to support the implementation of Ontario's Strategy to Combat Elder Abuse.

Funded by the ON Government, under the Ministry for Seniors and Accessibility (MSAA)



STOP ABUSE –

SIMPLY PUT, WE ALL HAVE A ROLE TO PLAY

RESTORE RESPECT



Canadian Network For the Prevention of Elder Abuse

MISSION

The CNPEA works to improve awareness, supports, and capacity to develop a national coordinated approach to elder abuse and neglect. We promote the rights of seniors through knowledge mobilization, collaboration, policy reform and education.

VISION

All seniors in Canada have access to the services and supports necessary to lead a quality life in their communities and live without fear of violence or neglect.

@cnpea

www.cnpea.ca

Presenter



Stephanie Senecal

Senior Support Unit Coordinator,
Canadian Anti-Fraud Centre –
Royal Canadian Mounted Police and
Ontario Provincial Police

Stephanie is an OPP civilian member and the Senior Support Coordinator at the Canadian Anti-Fraud Centre.

She manages a team of senior volunteers who do call backs to senior victims of fraud, who input fraud data and who also do fraud prevention presentations to the public. Stephanie also presents on a regular basis and assists law enforcement with their senior victims of fraud.”



Frauds and Cybercrimes

By: Stephanie Senecal



Royal Canadian
Mounted Police

Gendarmerie royale
du Canada



Competition Bureau
Canada

Bureau de la concurrence
Canada



Ontario Provincial Police

Canada

What is the Canadian Anti-Fraud Centre? (CAFC)



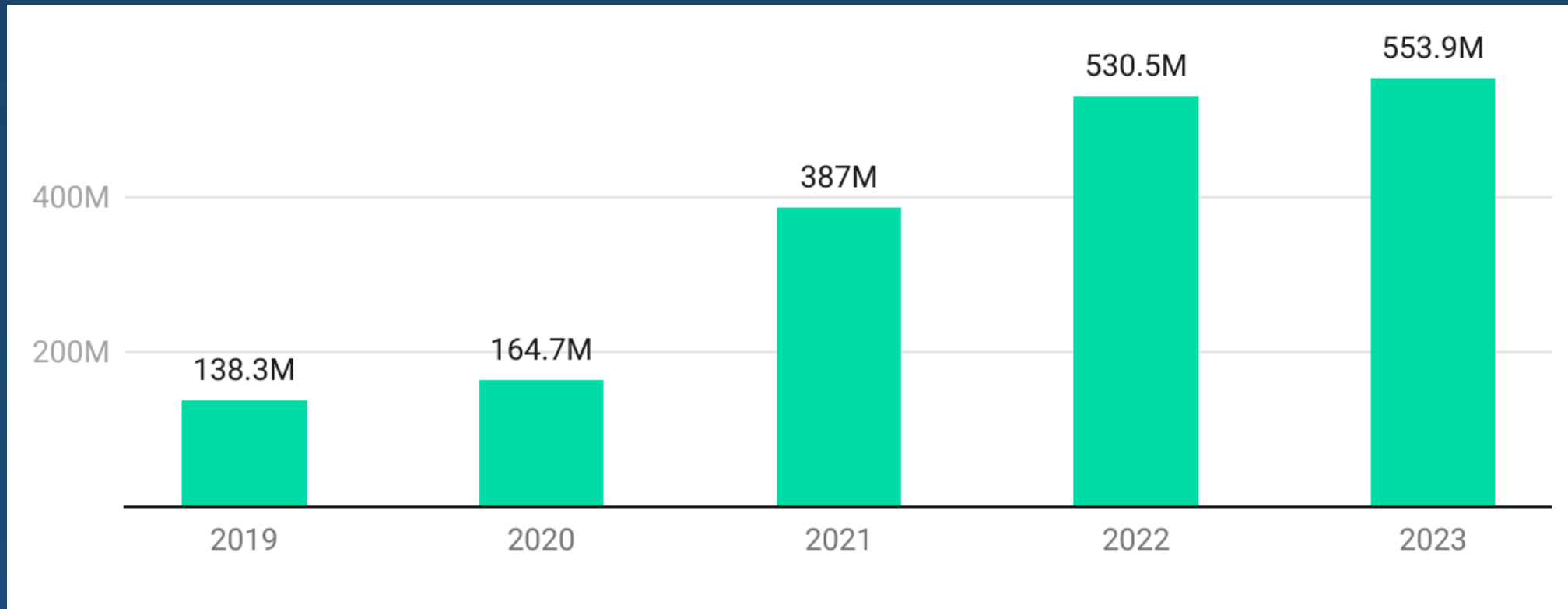
Competition Bureau
Canada

Bureau de la concurrence
Canada



Total Dollar Loss Over Time

This chart documents the total dollar losses suffered by fraud victims over the past 5 years



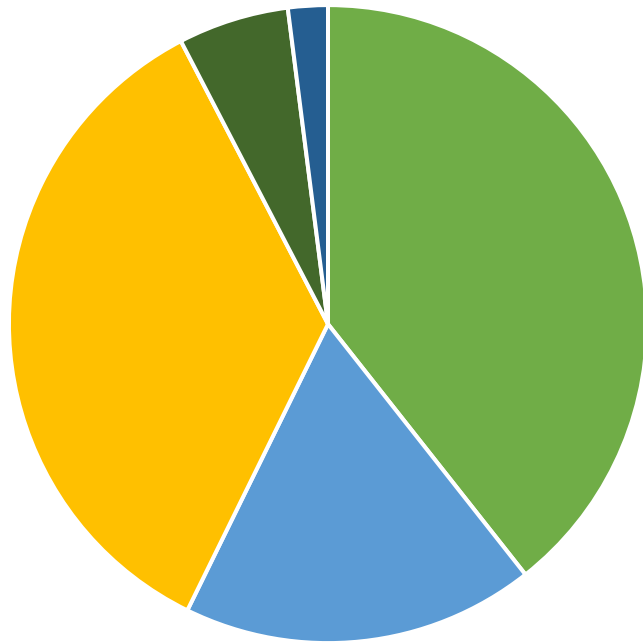


Fraud is Under Reported!

It is estimated that only 5 -
10 % of fraud is reported to
the CAFC.



Top Cyber Solicitation Methods

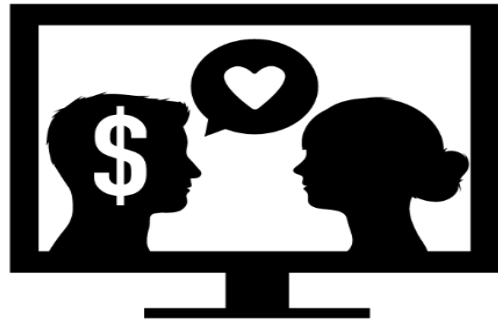


Internet-social network	8,055	6,637	174,665,572.38
Email	6,829	2,577	79,380,022.42
Internet	6,573	5,511	155,708,238.08
Text message	5,476	1,808	24,906,674.31
Not Available	3,680	3,129	8,939,712.96

■ Internet-social network ■ Email ■ Internet ■ Text message ■ Not available



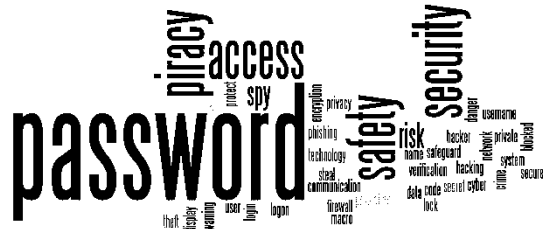
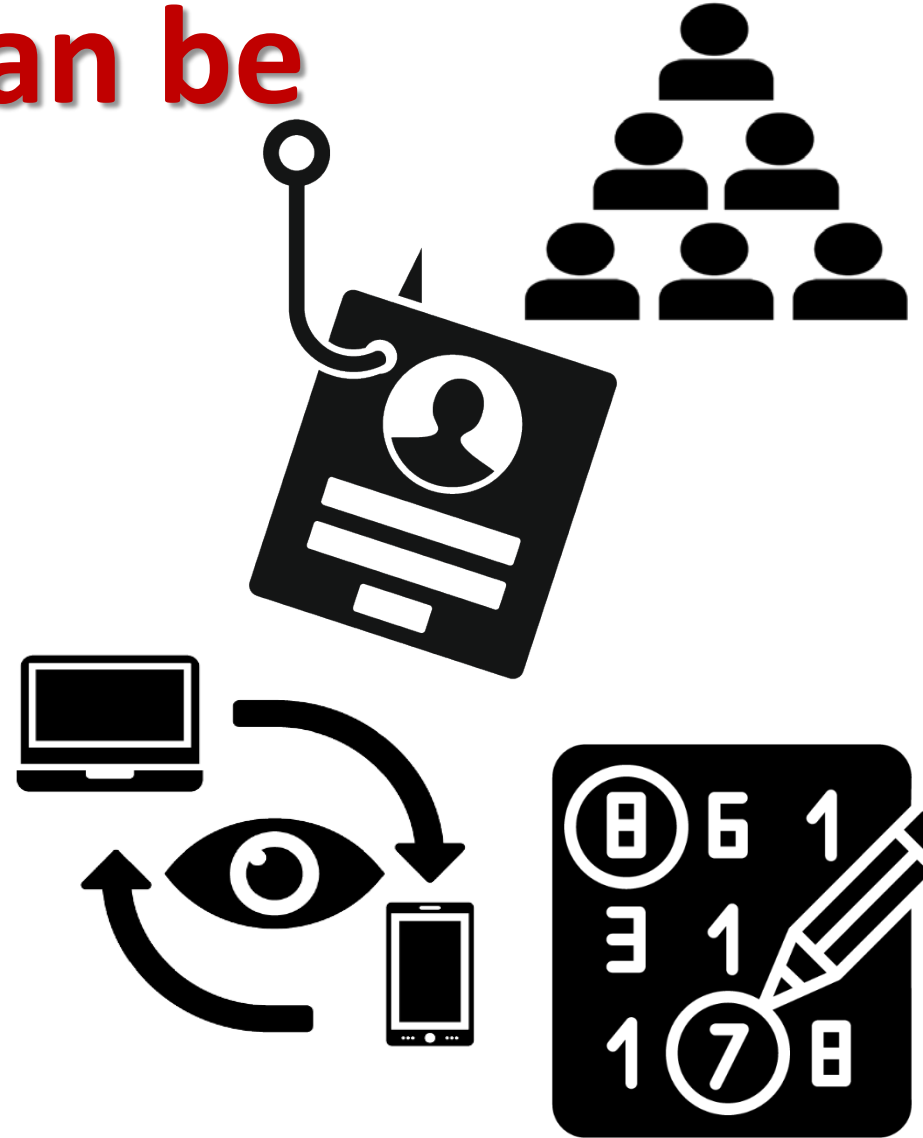
Cyber Frauds can be initiated



Online
E-mail

Text message

Social Networks

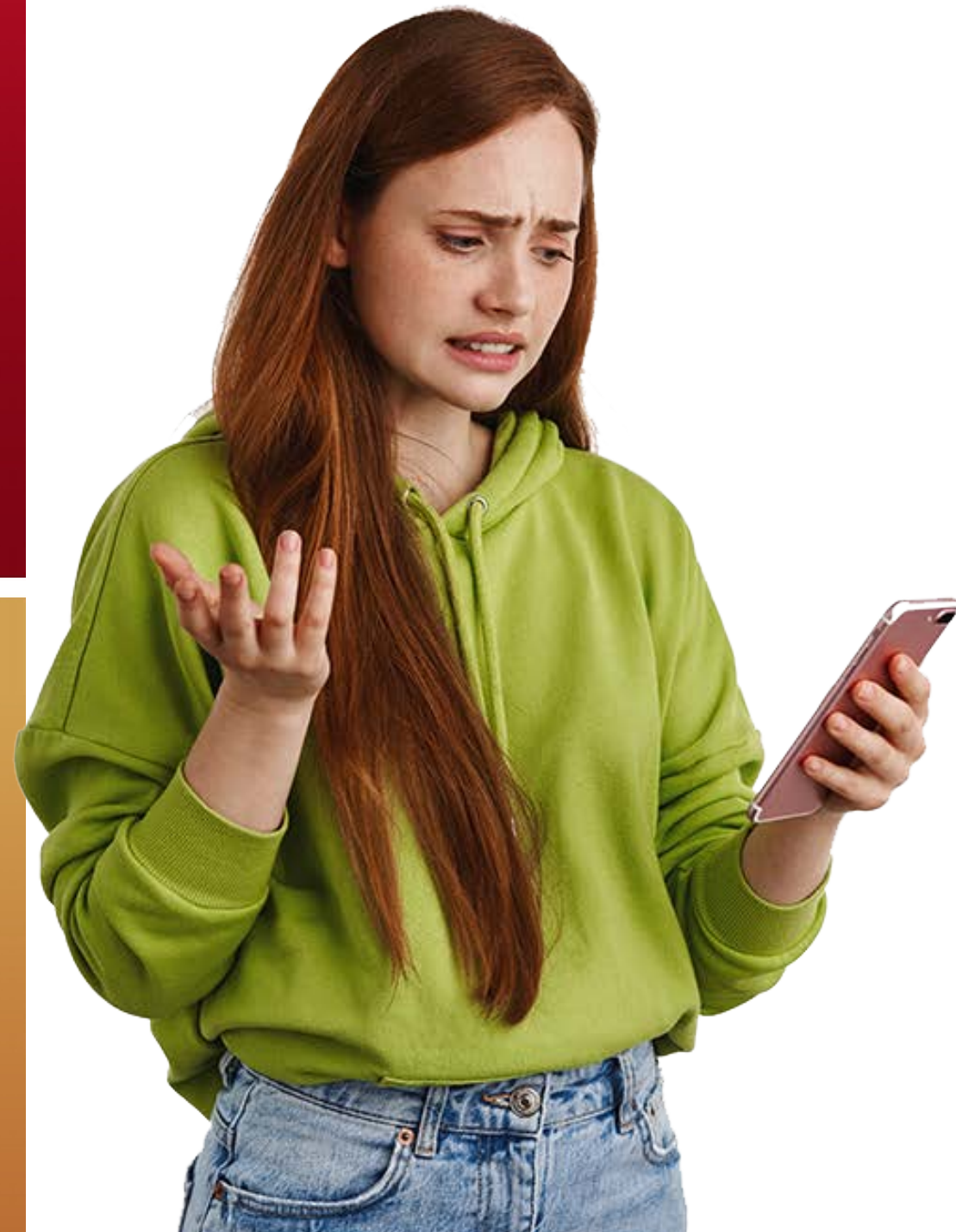


Fraud Initiated Online

- Search Engine Optimization
- Pop - Ups
- Online Classified
- Fake Information
- Stolen Credit Cards
- Fake Websites

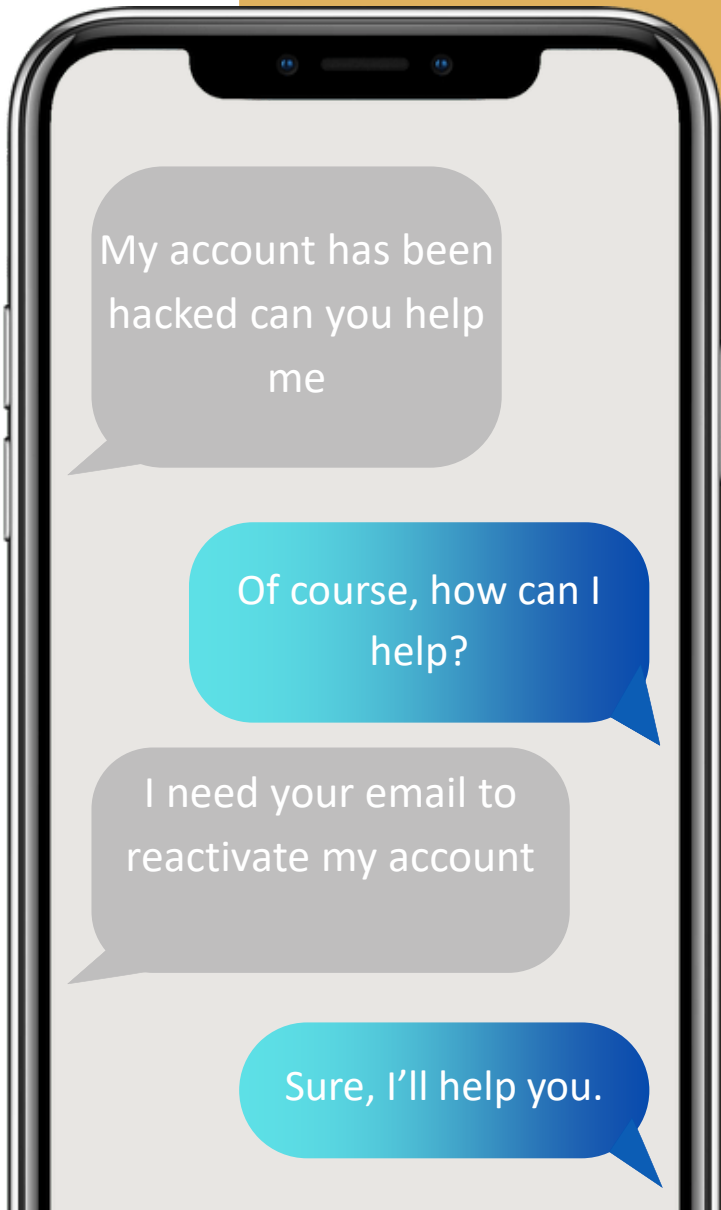
Fraud Initiated Email or Text Message

- Spoofing
- Automation
- Email Compromise



Fraud Initiated on Social Networks

- Fake Accounts
- Social Media Bots
- Compromised Accounts
- Advertisements



Examples of Phishing

YOUR BANK'S NAME: Unusual activities detected

Dear valued customer,

We've detected unusual transactions on your client card

4 FIRST DIGITS OF YOUR CLIENT CARD To ensure the security of your account, we kindly request that you verify your account by logging in immediately at <https://>

FAKEWEBSITEFORYOURFINANCIALINSTITUTION.COM

Thank you for choosing **BANK NAME**, and for your prompt attention to this matter.

Sincerely,

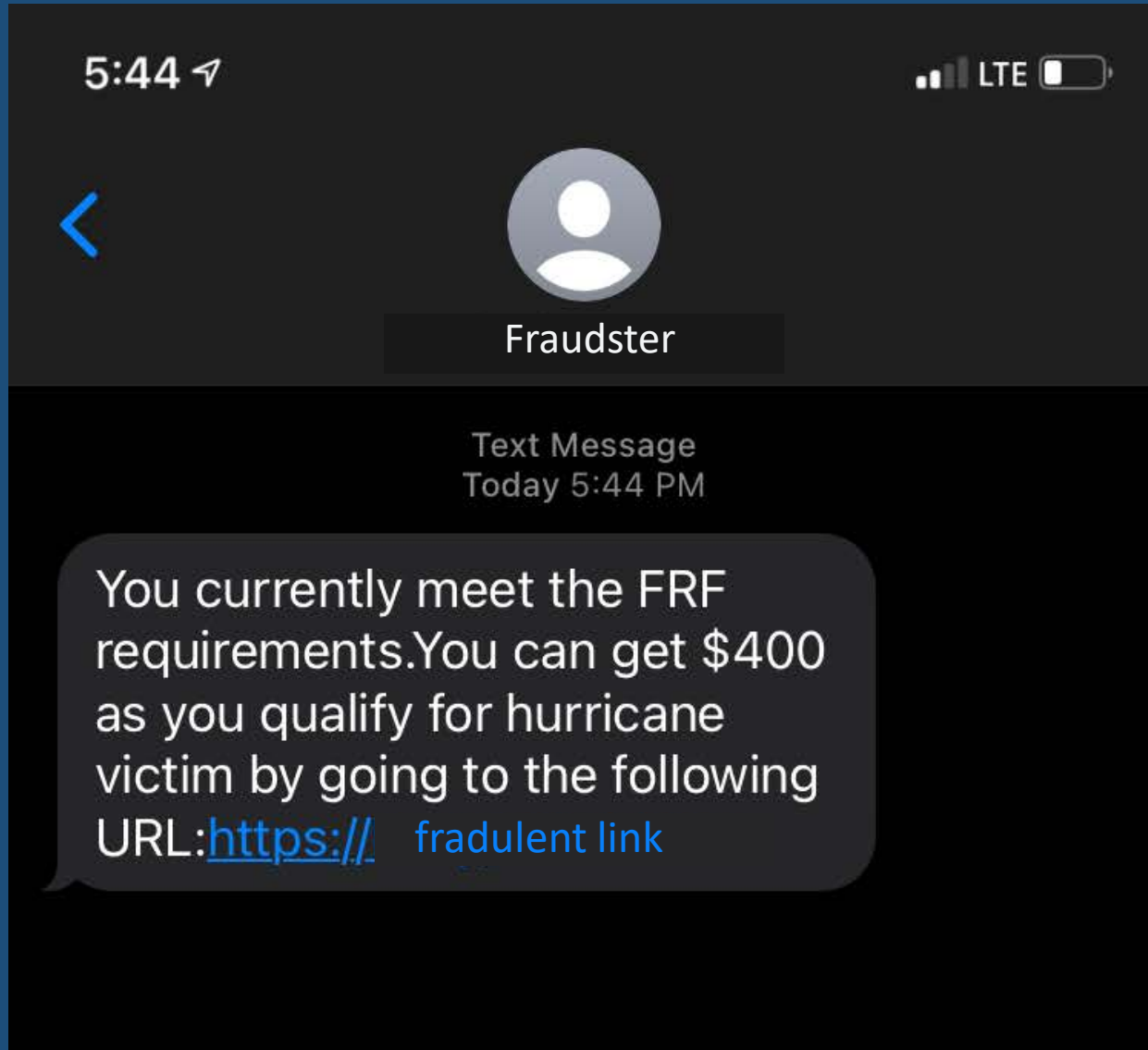
YOUR BANK'S NAME HERE

Examples of Phishing

(CRA) Notice: We determined your annual entitlement based on the tax form submitted. Please visit below to complete your pending (GST/HST) entitlement of \$447.95. See:

Data rates may apply

Examples of Phishing



QR Code Quishing

QR Codes can be found on websites, in e-mails, on printed flyers, on physical objects, on social media and more .

Make sure to verify the QR code's URL before following the link.

Make sure it is not a sticker over top of another QR code.

Redirects victims to malicious websites or downloads harmful content

Do not download anything from a QR Code.

Steals sensitive information such as passwords financial data or personal data

Can lead to Identity Fraud where suspect applies for credit cards, loans or creates accounts



Artificial Intelligence and Fraud:

Fraudsters are increasingly using artificial intelligence (AI) and related technologies to perpetrate various forms of fraud.

Deepfake Technology:

While not strictly AI, deepfake technology, which uses machine learning algorithms to create realistic fake videos or audio recordings, can be used for various fraudulent purposes, such as impersonating celebrities.



Secure your devices

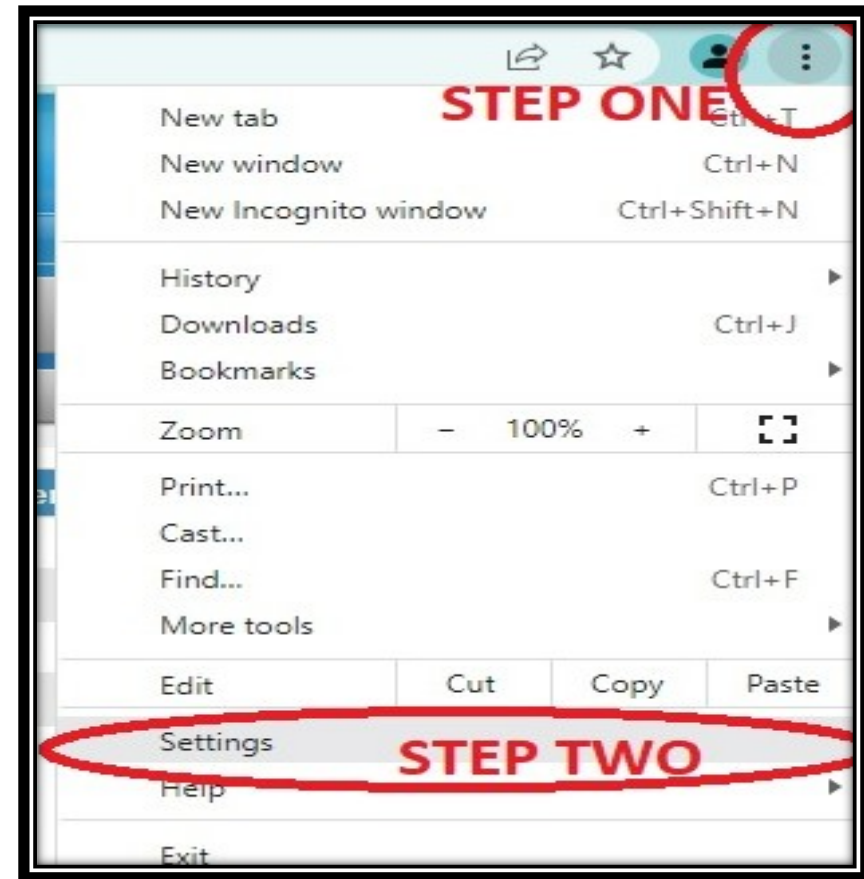
- Install an anti-virus and anti-spyware:
 - Make sure you purchase it from a trusted source
 - Do weekly scans
 - Update when prompted
- Restrict access by:
 - Shutting down your device
 - Locking your device
 - Disabling your webcam and storage device when not in use
- Clear your cache and browsing history, doing so will remove:
 - Log in IDs
 - Passwords
 - Banking information
 - Other sensitive data





How to clear your cache and browsing history

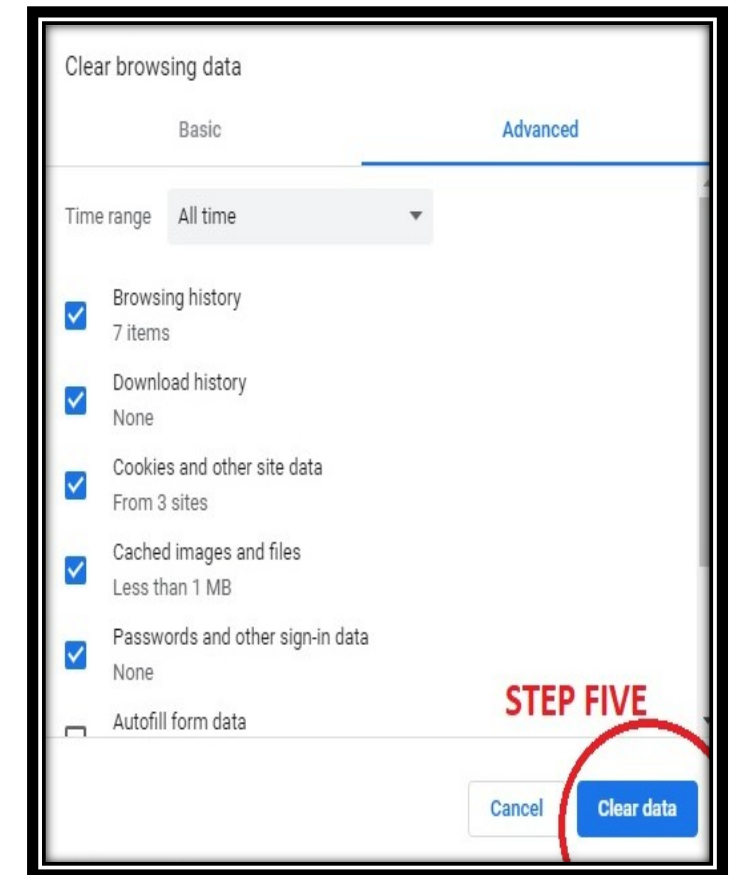
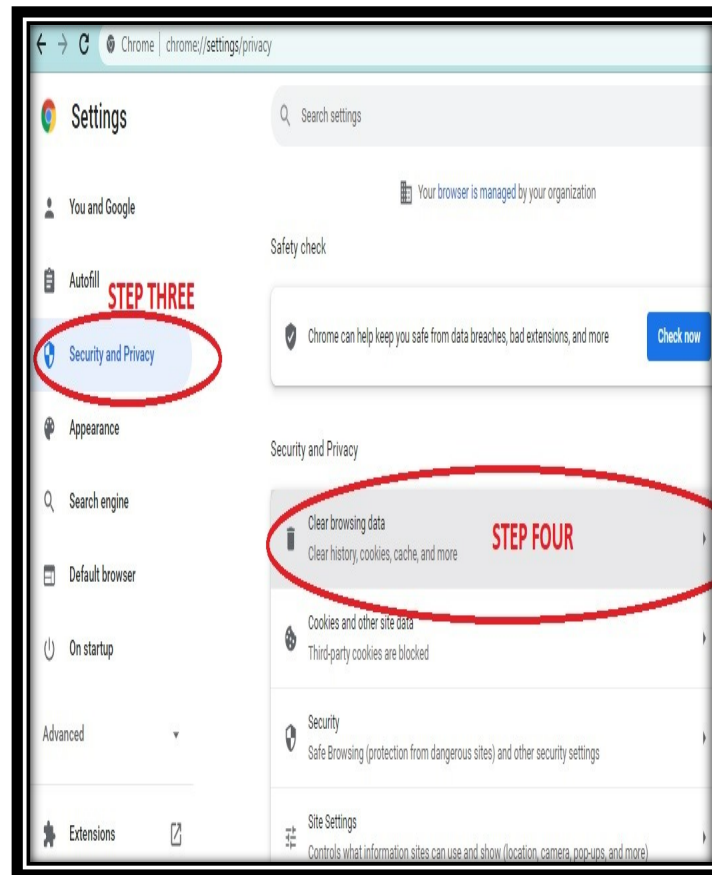
- Open browser
- Click 3 dots on the top right
- Go to settings





How to clear your cache and browsing history

- Go to privacy and security
- Click on clear browsing data
- Click on clear data





Keep your Wi-Fi secure

- Do not use default login information
- Change your network name and password
- Limit your coverage area



Never use public Wi-Fi to

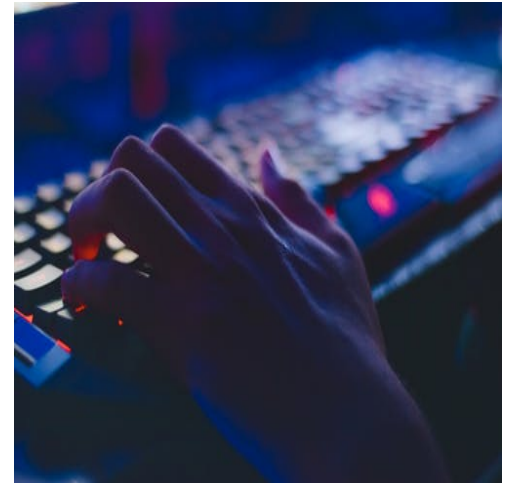
- Log into sensitive accounts
- Log into your bank accounts
- Make an online purchases
- Send confidential information





Passwords

- Use a password to log into all of your devices (phone, laptop, computer etc.)
- Never store your passwords on your devices or near your devices
- Never use the same password twice
- Utilize multi-factor authentication when available
- Change passwords twice a year
- Never share passwords
- Use strong passwords





What is a strong password?

- Create a passphrase
 - a combination of 4 or more random words with a minimum of 15 characters


OR

- Create a password that contains
 - 12 characters
 - Combination of upper and lowercase letters
 - Have a minimum of 1 number
 - Have a minimum of 1 special character (!@\$&*)





How to spot a fraudulent website

- Make sure there is a little lock  at the beginning of the website (domain) name. If you see an exclamation mark or a red line or a warning triangle over the lock do not proceed.
- Https websites are more secure than http.
- Check for spelling, grammar and formatting errors.
- Verify the domain name is spelled correctly. Fraudsters will mimic domain names. They might use an **rn** instead of an **m** or might swap letters (**Amazon vs Amaozn**).
- If a website does not have return or privacy policies, avoid them.



DO NOT

- Click on links within text messages or e-mails
- Call a telephone number that was provided to you, use the number you are familiar with
- Provide personal or financial information unless you are 100% sure it's a trusted source
- Make online purchases using e-transfers, wire transfers, cryptocurrency or money service business
- Give access to your device to anyone



DO NOT

- Trust advertisements on social media or on the internet
- Have faith in your caller ID or the e-mail address you see as it could be spoofed
- Trust any type of pop-ups, especially tech support
- Click on suspicious links as they can contain malware or viruses
- Believe anything that sounds too good to be true
- Post personal information or your marital status on Social Media



Unsure?

Ask for someone's input.
Do some research.
Cross reference.
Still unsure.....Do not proceed.





What To Do If You're A Victim

If you're a victim of identity theft and/or fraud, you should immediately complete the following steps:

Step 1: Gather the information pertaining to the fraud.

Step 2: Contact the two major credit bureaus; Equifax & Trans Union.

Step 3: Report the incident to your local law enforcement.

Step 4: Report the incident to the CAFC.

Step 5: Review your financial statements and notify them of any suspicious activity.

Step 6: Notify your financial institutions and credit card companies and change passwords to your online accounts.

Step 7: If you suspect that your mail has been redirected, notify Canada Post.

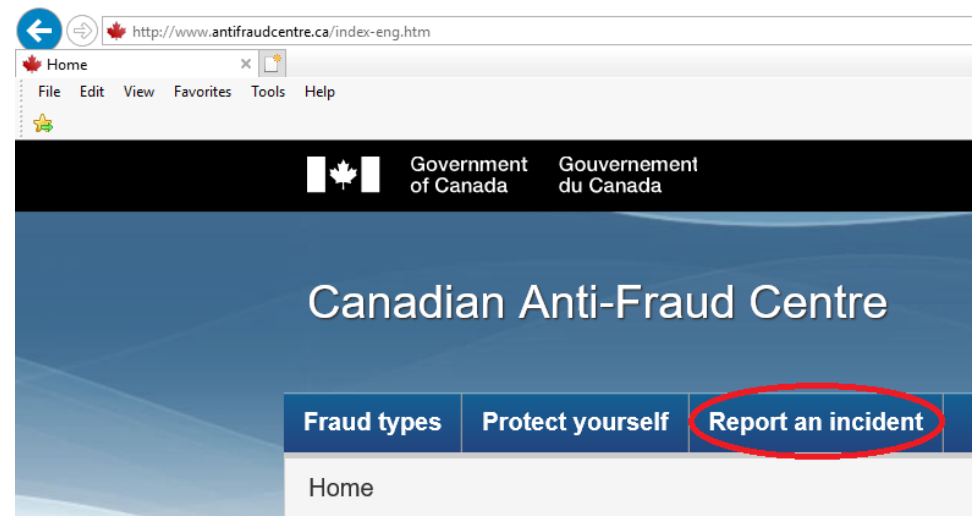
Step 8: Notify federal identity document issuing agencies.

Step 9: Notify provincial identity document issuing agencies.



How to Report Fraud

- Toll Free: 1-888-495-8501
- Online: Fraud Reporting System (FRS)
(www.antifraudcentre.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





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





Legal Supports



Advocacy Centre for the Elderly (ACE)

A community based legal clinic for low-income senior citizens.

1-855-598-2656

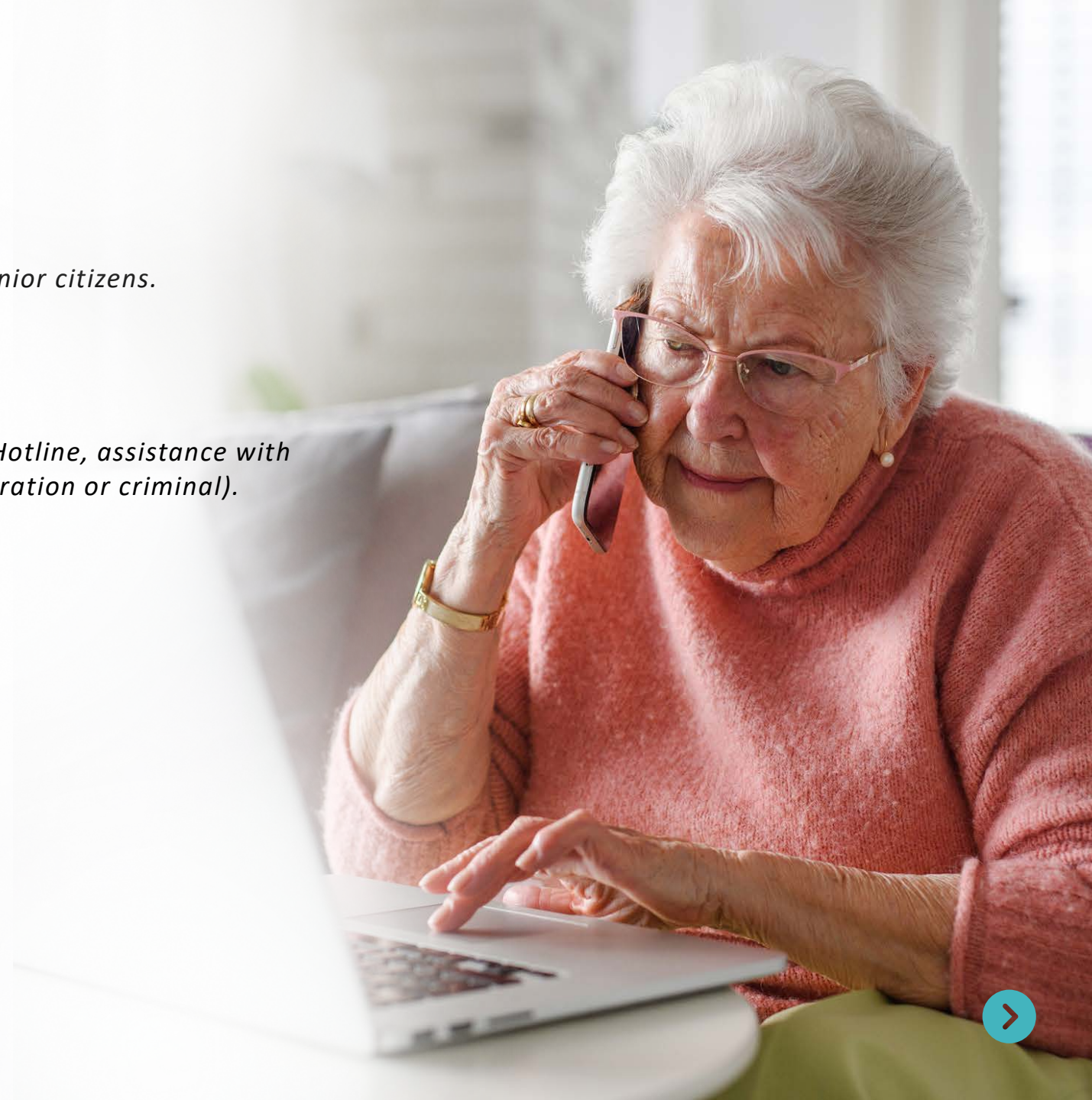
www.advocacycentreelderly.org



ProBono Ontario - *30 mins Free Legal Advice Hotline, assistance with civil law matters in Ontario (no family law, immigration or criminal).*

1-855-255-7256

www.probonoontario.org/hotline/



EAPOO Resources

Cyber Security Tips for Seniors

Cyber security is the set of practices that you have in place to protect your devices and personal and financial information. Cyber criminals target individuals to gain information that they can exploit to steal money from you.

- Create unique, strong passphrases and passwords**
 - Use a passphrase, a series of at least four words and 10 characters in length.
 - Or use complex passwords with:
 - at least 12 characters
 - upper and lower case letters, numbers and symbols
 - Use a different password for every account.
- Limit sharing of sensitive personal information online**

Be careful what personal data you share online. Don't provide your birthdate, sex or any personal or financial information.
- Enable multi-factor authentication (MFA)**

MFA uses two or more different ways of verifying that you are who you say you are to add an extra layer of protection for your accounts and devices.
- Install software updates and patches**

Install software updates as soon as they are available for all of your connected devices.
- Protect your devices**

Install antivirus and anti-malware software on all your connected devices and keep this software up to date.
- Phishing: Don't take the bait**

Phishing is one of the most common factors that cyber criminals use to steal your information. Phishing messages go often sent as emails, text messages (known as smishing) or phone calls.

Beware: Phishing messages often pressure or threaten you to respond quickly.

Links: Don't open any link or attachment you're unsure of.

Delete any messages that seem too good to be true, too convincing or that you didn't enter.

For more information:
Elder Abuse Prevention Centre
416-925-7272 | info@elderabuse.ca
www.elderabuse.ca

RESOURCES:
Canadian Anti-Fraud Centre
1-877-978-2839 or www.cafc-ccafrc.ca
Government of Canada
www150.com

Online Dating & Romance Scams

Tips for Seniors

1 Romance scammers use dating and social networking sites to contact their victims. They create accounts using stolen photos and fake stories that often suggest they work in the military, overseas or in business. They profess their love to gain victims' trust and eventually their money.

What are the signs?

Beware of:

- 01 Profiles that seem too perfect.
- 02 Someone you haven't met in person professes their love to you.
- 03 People who claim to be wealthy, but need to borrow money.
- 04 Any attempts to meet in person get cancelled.
- 05 A person who discourages you from talking about them to friends & family.

What to do:

- 01 Slow down. Don't send money or interact with someone you just met online and have never seen before in person.
- 02 Talk to a trusted friend or family member for their opinion. A friend or family member can give you valuable, objective feedback.
- 03 Ask them for a recent photo or do a video call. If the person is real, they should be open to sharing their real photo with you or by video call.
- 04 Don't share any compromising material that can be used to blackmail you.
- 05 Be very careful about how much personal information you share on social nets and dating sites.

STATISTICS

Over **\$50.3 million** Lost to romance scams in 2020

Reports: **1,135** Victims: **945**

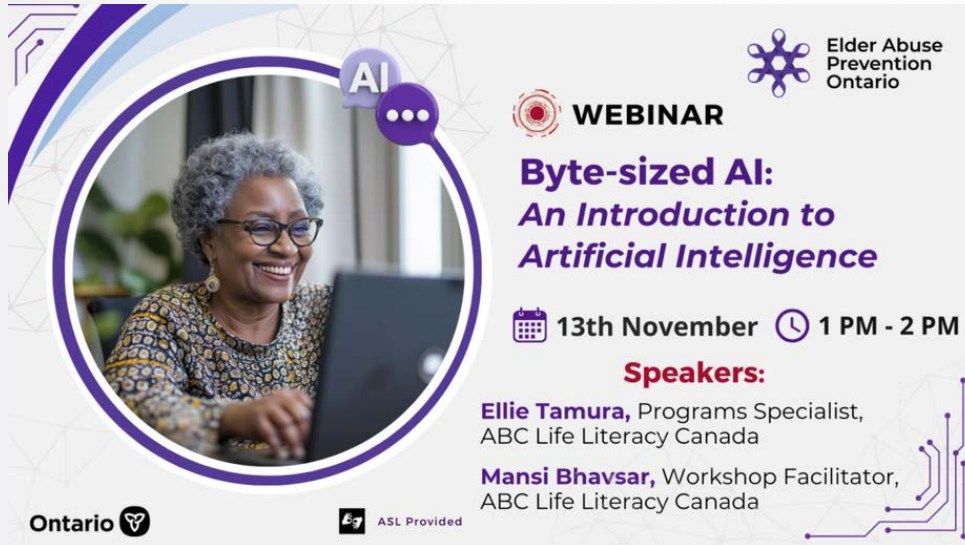
Source: Statistics Canada, Canadian Anti-Fraud Centre (CAFC) - 2021-03-04-07

For more information:
Elder Abuse Prevention Centre
416-925-7272 | info@elderabuse.ca
www.elderabuse.ca

Resources:
Government of Ontario
www.ontario.ca
Government of Canada
www150.com



EAPO Webinars





AI


WEBINAR

**Byte-sized AI:
An Introduction to
Artificial Intelligence**

13th November 1 PM - 2 PM

Speakers:
Ellie Tamura, Programs Specialist,
ABC Life Literacy Canada
Mansi Bhavsar, Workshop Facilitator,
ABC Life Literacy Canada

Ontario  ASL Provided 

Elder Abuse Prevention Ontario 



WEBINAR

**Banking Basics -
Advancing Financial Literacy
for Older Adults**

27th November 1 PM - 2 PM

Speaker:
ABC Life Literacy Canada

Ontario  ASL Provided 

Elder Abuse Prevention Ontario 

<https://eapon.ca/eapo-webinars/>





CNPEA  RCPMTA

CANADIAN NETWORK for
the PREVENTION of ELDER ABUSE
RÉSEAU CANADIEN pour la PRÉVENTION
du MAUVAIS TRAITEMENT des AÎNÉS



Elder Abuse
Prevention
Ontario



WEBINAR

How to Be #UnHackable: *Learn to Think Like a Scammer to Improve Your Cybersafety Skills*



19th November



1 PM - 2 PM

Speakers:

Claudiu Popa, Founder

KnowledgeFlow Cybersafety Foundation

Debra Popa, Executive Director

KnowledgeFlow Cybersafety Foundation



Ontario 



ASL Provided



Elder Abuse
Prevention
Ontario

**Join us...to help make a
safer Ontario for all
older adults.**

**Contact
EAPO:**

1-416-916-6728

1-833-916-6728



<http://eapon.ca>



@EAPreventionON



Contact Us



Comments? Questions?
Keep in Touch

Bénédicte Schoepflin

Executive Director,
Canadian Network for the Prevention of
Elder Abuse

benedictes.cnpea@gmail.com

www.cnpea.ca

@cnpea

Raeann Rideout

Director, Strategic Partnerships
Elder Abuse Prevention Ontario

rrideout@eapon.ca

www.eapon.ca

@EApreventionON





THANK
YOU