Ontario Provincial Police

Cyber-Enabled Fraud

Crime Prevention and Community Support Bureau

Reported dollar loss to CAFC (2024)

In 2024, Canadian Anti-Fraud Centre (CAFC) processed **49,432** fraud reports, representing **34,621** victims, totaling:

- **Over $637 MILLION** in overall **reported** losses.

Global cost of fraud is more than **$5 TRILLION,** according to the Association of Certified Fraud Examiners Report to the Nations study (2024)

Top 10 CAFC frauds 2024 by dollar loss

Pitch Offering (60 + / Seniors)	Reports	Victims	Dollar Loss
Identity Fraud	1,654	1,654	N/A.
Service	1,864	1,458	$9.6 Million
Investments (Crypto)	1,259	1,204	$110.9 Million
Personal Info (ID Theft)	1,031	770	N/A
Bank Investigator	1,165	638	$5.7 Million
Merchandise (Online)	419	350	$1.2 Million
Emergency-Grandparent	817	346	$1.9 Million
Romance	355	315	$22.8 Million
Phishing (SMS Text)	910	252	N/A
Extortion	936	156	$4.7 Million

Fraud is under reported

It is estimated that less than 5-10% of fraud is reported to the CAFC or law enforcement.

Victims of fraud may suffer financial and emotional abuse and even medical problems relating to their victimization. They are not alone – millions of people are victims of fraud every year.

Why should I report the fraud?

- The information could link a number of frauds together, within Canada and worldwide.
- The information could progress or assist in solving an investigation.
- Public reporting assists with determining crime trends fraud prevention/awareness and assist with disruption efforts.
- It assists law enforcement, private and public sector, academia, etc. to learn about the crimes.

What to do if you're a victim

- Stay calm and gather all information about the fraud, including:
  - Documents/receipts/copies of emails and/or text messages
  - Report the incident to the financial institution that transferred the money
  - Place flags on all your accounts
  - Change all your passwords
  - Report the fraud to both credit bureaus (Equifax and TransUnion)

What to do if you're a victim

- Report the incident to your local police of jurisdiction and obtain an incident number for future reference.
- Report the incident directly to the administrators of the website. You can do so through a link such as "Report Abuse" or "Report an Ad".
- Report fraud that took place online through the social media platform or app, such as Facebook or Kijiji.
- Protect yourself from future fraud. Those behind scams often target victims of fraud a second or third time with the promise of recovering money. Always do your due diligence and never send recovery money.

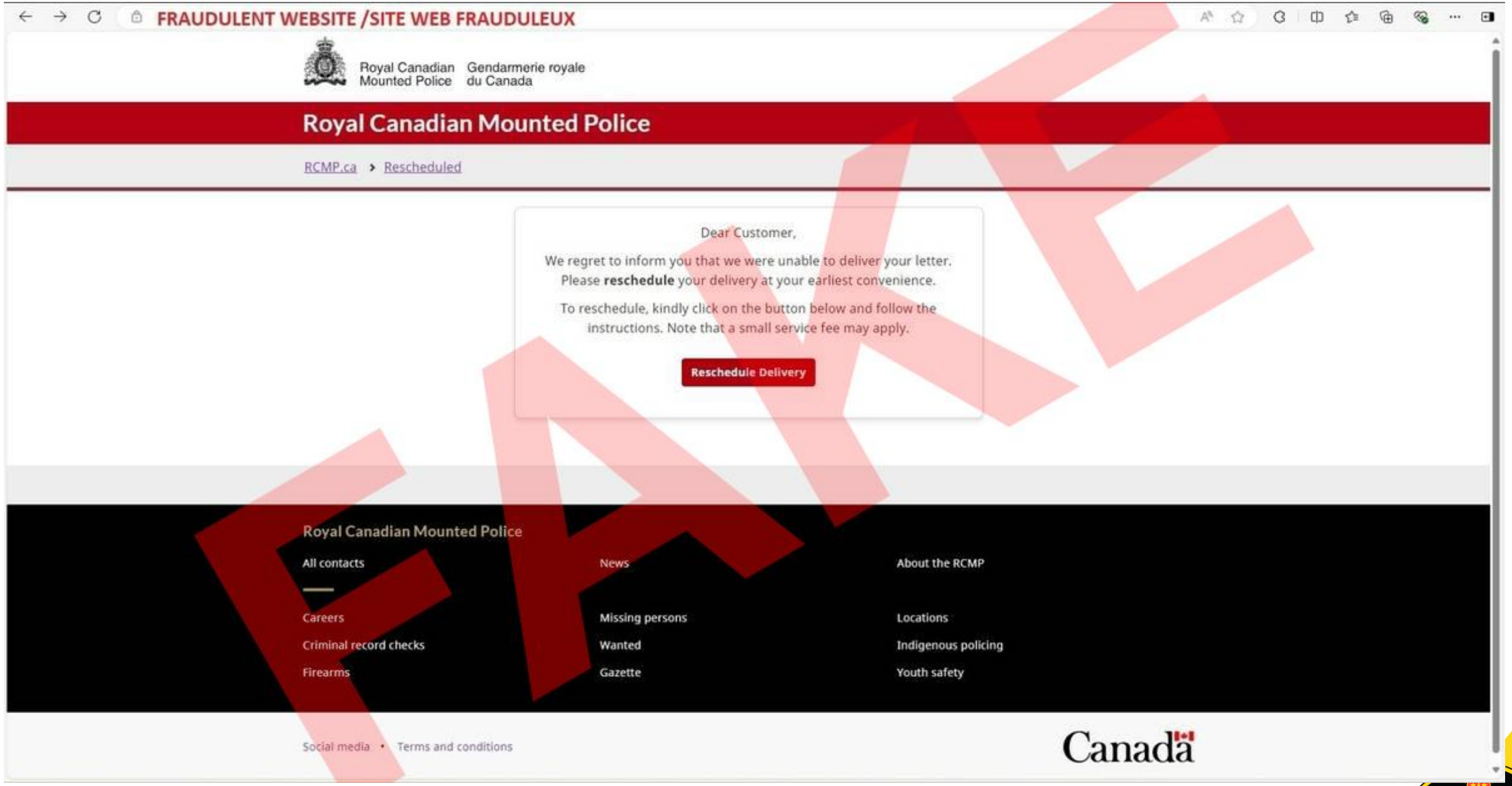
Those behind the scam

- The frauds are often very complex and elaborate.
- Those behind scams are very convincing.
- They will take all possible measures to keep their true identity anonymous.
- People engaged in fraudulent activities take advantage of technology and the anonymity it offers them, as well as the ability to easily and inexpensively reach thousands of people.

IT IS ABOUT MONEY

How modern scams use technology

- They will create spoofed (fake) websites.
- They use spoofed telephone numbers using Voice over Internet Protocol (VoIP) to mimic legitimate numbers.
- They'll have victims download remote-entry software providing access to devices and computers.
- They'll send out phishing texts with hyperlinks imitating legitimate businesses or governments offering refunds, rebates or requiring payments.


FRAUDULENT WEBSITE /SITE WEB FRAUDULEUX
Royal Canadian Mounted Police
Gendarmerie royale du Canada
Royal Canadian Mounted Police
RCMP.ca › Rescheduled
Dear Customer,
We regret to inform you that we were unable to deliver your letter. Please reschedule your delivery at your earliest convenience.
To reschedule, kindly click on the button below and follow the instructions. Note that a small service fee may apply.
Reschedule Delivery
Royal Canadian Mounted Police
All contacts
News
About the RCMP
Careers
Missing persons
Locations
Criminal record checks
Wanted
Indigenous policing
Firearms
Gazette
Youth safety
Social media • Terms and conditions
Canada
FAKE

Forms of contact

- **Telephone calls**
  - Automated dialing, Robocalls, spoofing, delayed disconnect
- **Email or Text**
  - Spoofing, automation, email compromise
- **Online**
  - Search engine optimization, pop-ups, classifieds, fake websites
- **Social Media**
  - Fake accounts, social media bots, compromised accounts, advertising
- **Mail or in person**
  - Employees/high pressure sales

Internet safety

- One of the first rules we learn as children is not to talk to strangers; the same rule should be used on the internet.
- Visit https://www.getcybersafe.gc.ca/en
- It is not recommended to talk to strangers on the internet or give out information that could put yourself in danger, such as posting your location in your Facebook status.

What frauds to be aware of…

Crypto Investment Scams

- Investment scams occur when individuals decide to invest in cryptocurrency after seeing a deceptive advertisement on social media, such as Instagram, YouTube, or Facebook.
- Victims download the trading platform and transfer cryptocurrency into their trading account.
- In most cases, victims are not able to withdraw their funds. Many of these of the trading platforms are fraudulent or controlled by bad faith actors.
- In addition to crypto trading scams, the OPP also receives reports on suspected fraudulent Initial Coin Offerings.

Ledger

A. Ledger Blue
97 x 68 x 10mm

B. Ledger Nano S
57 x 17.4 x 9.1mm

C. Ledger Nano X
72 x 18.6 x 11.75mm

How to protect yourself!

Caution:

- Be careful when sending cryptocurrency; once the transaction is completed, it is unlikely to be reversed.
- Be wary of individuals you've met on dating sites or social media who attempt to educate and convince you to invest into crypto currency.

How to protect yourself!

Research:

- Do your research to ensure they are using reputable and compliant services.
- Prior to investing, ask for information on the investment.
- Research the team behind the offering and analyze the feasibility of the project.
- Verify if the investment companies are registered with your Provincial Securities Regulator or the National Registration Search Tool (www.aretheyregistered.ca)

How to protect yourself!

Reason:

- The choice to open a wallet or invest should be yours, not someone else's.
- Beware of people asking you to open and fund new crypto accounts. They will direct you to send it to wallets they control… **don't!**
- Question why someone is reaching out to you about an investment offer:
  - Is this a conversation I would usually have with this person?
  - Does it make sense to invest in an opportunity based on a pop-up ad?
  - Should I feel pressure or urgency when deciding to invest?

Grandparent - Emergency Scams

- Claim to be law enforcement officials, lawyers and impersonate a **grandchild** or family member who has been in a collision or arrested.
- **Use urgency and threats** to convince you to take out money to pay for bail or release from jail.
- Claim that there is a court ordered **"gag order"** preventing you from speaking about the situation to anyone.
- If you agree to pay the requested amount (cash or cryptocurrency), those behind the scam **will arrange to pick up the funds** in person or will ask you to send cash in the mail.

Bank Investigator Scams

- Individuals engaged in fraudulent activities will convince victims that, in order to protect their account until a new debit card is issued, the victim must send an Interac e-transfer transaction to their own cellphone number.
- The suspect will instruct the victim on the steps required to add themselves as a payee and to increase their daily Interac e-transfer limit to $10,000 (note that the maximum amount that a sender may send through the Interac e-transfer network may vary depending on the sender's financial institution.
- Interac will automatically refuse to complete any payment by a sender above the limit established by the financial institution.

Bank Investigator Scams

- The suspect provides the e-transfer question and answer that the victim must use for the transfer.
- Once the victim sends the Interac e-transfer transaction to their own cellphone number, suspects will ask the victim for a “code,” which is the last portion of the Interac e-transfer URL/link received.
- If the victim provides the URL, suspects will have the ability to deposit the funds into their own account.

Bank Investigator Scams – Variation

- Victims receive an automated phone call claiming to be their financial institution, law enforcement or, in some cases, Amazon advising that there have been fraudulent transactions in their account.
- The suspect will then request access to the victims' computer to continue the "investigation". Victims are then shown a fraudulent transaction on their online bank account.
- The suspects state that they want the victims' help in an ongoing "investigation" against the criminals who stole their money and request that the victims send funds as part of the "investigation."

How to protect yourself!

- Those engaged in fraudulent activities often use call-spoofing to mislead victims. Do not assume that phone numbers appearing on your call display are accurate.
- If you get an incoming call claiming to be from your financial institution, advise the caller that you will call them back. End the call and dial the number on the back of your bank debit card from a different phone if possible or wait 10 minutes before making the outgoing call.
- Never provide details of links or URLs received via text message or email to individuals engaged in fraudulent activities.

How to protect yourself!

- Don’t share codes received via text message or email with anyone. In most cases, these are multi-factor authentication codes that will give those behind the scam access to your account.
- Those behind the scam will often provide the first 4 to 6 numbers of your debit or credit card. Remember that these numbers are used to identify the card issuer and are known as the Bank Identifier Number (BIN). Most debit and credit card numbers issued by specific financial institutions begin with the same 4 to 6 numbers.

How to protect yourself!

- If your personal information has been compromised in the past through a breach or a phishing message, remember that the information can be used as a tool to make the communication appear legitimate.
- Never provide remote access to your computer.
- Financial institutions or online merchants will never request transferring funds to an external account for security reasons.
- Financial institutions or police will never request you to turn over your bank card nor attend your residence to pick up your bank card.

Service Frauds – Door-to-Door

- Home services and equipment sales.
- Victims are being contacted through ads on social media, telemarketing calls or through door-to-door salespersons.
- Be wary of ads on social media offering grants, equipment or services at a price below market value.
- Remember to research the company before providing your contact information and especially before signing a contract!
- Visit https://news.ontario.ca/en/release/48303/ontario-ban-on-door-to-door-sales-in-effect-as-of-march-1st

Service Frauds – Tech Support

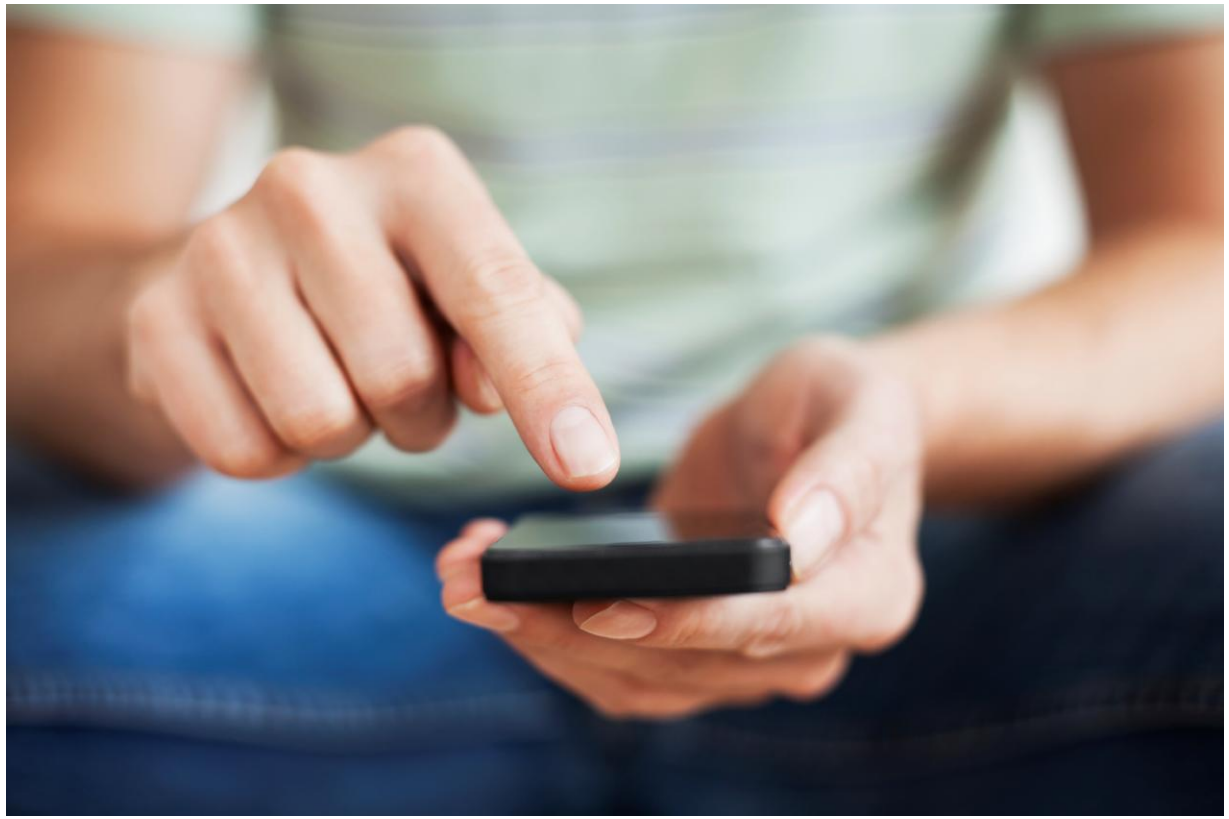
- A person claims a virus has infected your computer.
- Alarming website pop-ups that demand you call a number urgently.
- Unsolicited telephone calls (they may claim to be a Microsoft or other well-known computer company employee).

Service Frauds – Tech Support

- That your computer is sending out viruses or has been hacked and must be serviced. They request remote access to your computer and may run programs or alter settings.
- Asks you to pay a fee for fixing your computer via credit card or money transfer.
- In some cases, **those behind the scam will ask you to log into your bank account to transfer funds**.

You can stop phone fraud

Just hang up!



Identity fraud

Cyber criminals use personal information to apply for government benefits, credit cards, bank accounts, cell phone accounts or even take over social media and email accounts.

It is important that you take steps to secure your personal and financial information and know what to do when identity fraud occurs.

How to protect yourself!

- Unsolicited emails, text message, phone calls asking for personal or financial information.
- Be careful about giving out your personal information (Bank account/SIN, date of birth).
- Do not reply to or click on links in any email that looks suspicious.

How to protect yourself!

- Never open an attachment from spam or sender not known to you.
- Never use automatic login features that save your username and password. Take the time to re-enter your password each time.
- Consider carefully what you're putting out there through email and social networking sites.
- Choose strong passwords.

Phishing

- Phishing is one of the easiest ways for those engaging in fraudulent activities to steal log in credentials, personal information or even infiltrate business networks.

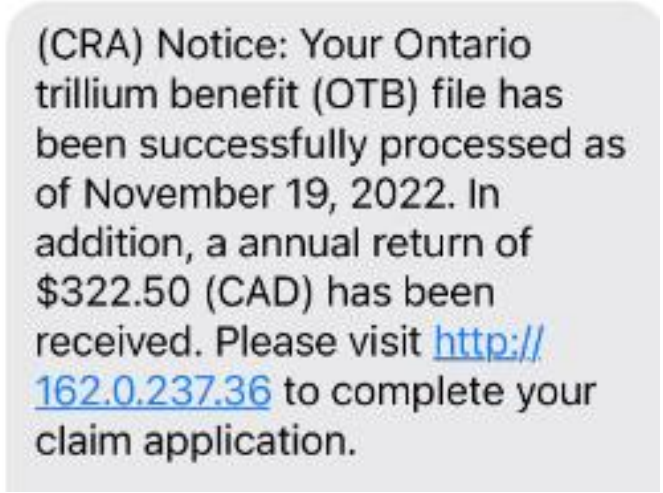
- Individuals engaged in fraudulent activities will use mass email or text campaigns to send messages that appear to be from recognized institutions, companies or government agencies.

- These emails may claim that you need to update your account or that money is ready to be deposited or receive a rebate.

Phishing

These tactics could be:

- Email and website name spoofing
- Sense of urgency
- Offers of refunds or money
- Seemingly "harmless" requests to click links, download attachments or fill out forms online
- Instructions to scan a QR code

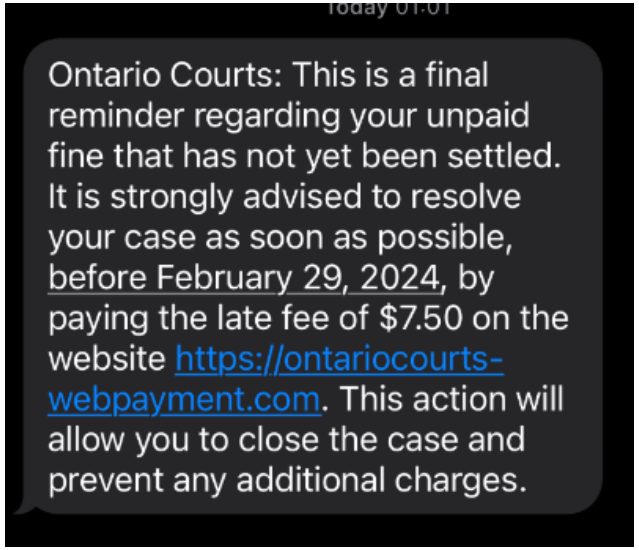


Phishing

Do you know how to spot phishing messages?

Phishing

- Forward the spam message to 7726 (SPAM on most keypads).
- This will alert your cellular provider to open an investigation on the contents of the message.
- Forwarding methods will vary depending on your phone.



Romance / Crypto Romance scams

- Victims are contacted on dating websites or social media (e.g. Facebook) and then asked to switch to a different method of communication (e.g. Signal, WhatsApp).
- It is common for suspects to use pictures found on social media of real people (e.g. businesspeople, members of the military, family photos), pet photos and hobbies.
- Those behind scams quickly profess their love to gain their victims' trust, affection, and money. This type of fraud relies heavily on victim emotions and may last for months, years, or until the victim has nothing left to give.
- Those behind the scam will never end up repaying the victim and continue to make empty promises while asking for more money.

Romance / Crypto Romance scams

- Another prevalent variation is the “CryptoRom”

- In these cases, those behind the scam convince the victim to invest into fraudulent cryptocurrency platforms with the promise of large monetary returns.
- In fact, the individuals engaged in fraudulent activities may even let the victim cash out some of their investment returns only to get them to invest a larger amount.

How to protect yourself!

- Don’t give out your personal information (i.e. name, address, DOB, SIN, banking credentials).
- Don’t accept friend requests from people you do not know.
- Don’t invest your money in platforms provided by people you don’t know.
- Be careful who you share images with. Suspects will often use explicit pictures to extort victims into sending more money.
- Protect your online accounts.
- Never send money to someone you haven’t met.
- Don’t respond to text messages from phone numbers you do not recognize.
- Beware of people asking you to open and fund new crypto accounts. They will direct you to send it to wallets they control… **don’t!**

Online Merchandise Scams

- Beware when shopping online with peer-to-peer transactions like Facebook Marketplace or Kijiji.
- Never pre-pay for an item or provide a deposit in advance.
- Check seller's rating and feedback from other shoppers.
- Consider meeting in a safe location (e.g. Police Station parking lot)
- If it doesn't feel right, it probably isn't – don't be pressured into a sale/purchase.
- Do your due diligence and protect yourself.

How to protect yourself – Red Flags

- Don't be afraid to say no.
- Don’t react impulsively – scrutinize urgent requests.
- Don't be intimidated by high-pressure sales tactics.
- Ask questions and talk to family members or friends.
- Request the information in writing.
- If in doubt, simply hang up.
- Watch out for urgent pleas that play on your emotions.
- Always verify that the organization you're dealing with is legitimate.
- Don't give out personal information.
- Beware of unsolicited calls or emails (e.g. phishing) that ask you to confirm or update your personal or financial information.

Be Cyber Secure

- Protect your computer by ensuring your operating system and security software are up-to-date.
- Secure your online accounts, use strong passwords and, where possible, enable two-factor authentication. Secure your devices and internet connections.
- Some websites, such as music, game, movie, and adult sites, may try to install viruses or malware without your knowledge.
- Watch out for pop-ups or emails with spelling and formatting errors.
- Beware of attachments and links as they may contain malware or spyware.
- Never give anyone remote access to your computer.
- Disable your webcam or storage devices when not in use.
- If you are having problems with your computer, bring it to a local technician.

Protect your online accounts

By taking the following steps, you can better protect your online accounts from fraud and data breaches:

- Change passwords regularly and create a strong password by:
  - ✓ Using a minimum of 8 characters including upper and lower case letters, and at least 1 number and a symbol
  - ✓ Creating unique passwords for every online account including social networks, emails, financial and other accounts
  - ✓ Using a combination of passphrases that are easy for you to remember but hard for others to guess, such as using a phrase and not just a word
- Enable multi-factor authentication.
- Only log into your accounts from trusted sources.
- Don't reveal personal information over social media.

Where can I go for help?

- The first step is to report the fraud to your **local police service**. If your local police service is the OPP, use the detachment locator to find your nearest detachment.
- You have different options to report a fraud to your local police, depending on where you live.
- Report in-person by attending your local police service.
- Report over the phone by calling your local police service.
- You are also encouraged to report the incident to the Canadian Anti-Fraud Centre (CAFC). You can contact the CAFC toll free by calling 1-888-495-8501 or through the Fraud Reporting System.

Where can I go for help?

- **Ontario Provincial Police**

1-888-310-1122

- **Canadian Anti-Fraud Centre**

1-888-495-8501

antifraudcentre-centreantifraude.ca

Where can I go for help?

Consumer Protection Ontario
www.ontario.ca
1-844-286-8404

Better Business Bureau
www.bbb.org/
1-613-237-4856

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

TransUnion
www.transunion.ca
1-866-525-0262

What else can we do to help?

- The OPP works closely with community partners on a regular basis and support numerous community anti-fraud projects.
- We provide public education and online resources in every community.
- Visit www.opp.ca for resources – Ontario Provincial Police - Fraud

To receive CAFC bulletins, trends, media releases…
simply send an email to get added on the list!

partners@antifraudcentre.ca

The Canadian Anti-Fraud Centre (CAFC), Ontario Provincial Police and Royal Canadian Mounted Police are launching a fraud prevention campaign to raise awareness about the significant increase in emergency scams targeting Canadian seniors.

Follow us for more information

Questions?

Thank you and please take care!