CANADIAN ANTI-FRAUD CENTRE

Royal Canadian Mounted Police | Gendarmerie royale du Canada | Competition Bureau Canada | Bureau de la concurrence Canada | Ontario Provincial Police | Canada

SENIORS

2023 Fraud Prevention Handbook

Table of Contents

Introduction

Since 2020, the Canadian Anti-Fraud Centre (CAFC) has seen fraud victimization grow to shocking new heights. While we know that the COVID-19 pandemic exposed new vulnerabilities and increased the potential of fraud victimization, fraud losses continue to rise. Losses reported to the CAFC reached an all-time high of $383 million in 2021. In 2022, reports shattered that record at yet another all-time high of $530 million in victim losses.

While law enforcement and partners continue to work tirelessly to combat fraud, the general Canadian public has a huge role to play in protecting themselves and their communities; and we want to show them how.

Fraud Prevention Month is a campaign held each March to inform and educate the public on the importance of protecting yourself from fraud. This year's theme is "Tricks of the trade: What's in a fraudster's toolbox?". This theme is meant to expose the common tactics that fraudsters use to victimize targets.

The CAFC has compiled a toolkit specifically designed for senior Canadians (60+) to raise awareness about fraud and prevent victimization. We encourage all of our partners to use the resources in this toolkit on their websites, in print and on their social media platforms.

Comments, questions or feedback on fraud prevention are always welcome.

Thank you,

Your CAFC Fraud Prevention Team

Follow us on Twitter – @canantifraud
Like us on Facebook – Canadian Anti-Fraud Centre

Resources:

1) **RCMP Videos**

The Face of Fraud

English: https://www.youtube.com/watch?v=0rlWUcc57dM

French: https://www.youtube.com/watch?v=cXXP35rICQY

A Cry from the Heart from Victims

English: https://www.youtube.com/watch?v=blyhHl8rc7g

French: https://www.youtube.com/watch?v=cHZfvpH2YW8

Telemarketing Fraud: The Seamy Side

English: https://www.youtube.com/watch?v=t7bhQJkelEg

French: https://www.youtube.com/watch?v=XteG_fdasdw

2) **OPP Videos**

Fraud Prevention Month Playlist

https://www.youtube.com/playlist?list=PLbecW3cjtFJ4gxFvi9vuGlh8hJR13y1-c

Senior Internet Scams Playlist

English:

https://www.youtube.com/c/OntarioProvincialPolice/search?query=Senior%20fraud

French: https://www.youtube.com/user/OPPCorpCommFR/search?query=fraude

3) **Competition Bureau of Canada Videos**

Mass marketing fraud can take many forms. These videos help describe the way they work and how to avoid victimization.

English: https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04272.html

French: https://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/04272.html

4) **CAFC Fraud Prevention Video Playlists**

https://www.youtube.com/channel/UCnvTfqttCb4K6wyVC6rMJkw/playlists

5) **CAFC Logo**

6) About the CAFC

The CAFC is Canada's central repository for information about fraud. We help citizens and businesses:

- report fraud;
- learn about different types of fraud;
- recognize the warning signs of fraud;
- protect themselves from fraud.

The CAFC does not conduct investigations but provides valuable assistance to law enforcement agencies by identifying connections all over the world. Our goals include:

- disrupting crime;
- strengthening the partnership between the private and public sectors;
- maintaining Canada's economy.

The CAFC is jointly managed by the Royal Canadian Mounted Police, the Competition Bureau, and the Ontario Provincial Police.

7) Statistics

In 2022, the CAFC received 90,438 fraud reports involving over $530 million in reported losses. Moreover, 16,894 of the reports were from seniors, that reported losses totalling more than $137.8 million.

Top 10 frauds affecting seniors based on number of reports in 2022:

Fraud Type	Reports	Victims	Dollar Loss
Identity Fraud	2510	2510	N/A
Phishing	2412	601	N/A
Extortion	2193	475	$7.7M
Service	2137	1669	$8.6M
Personal Info	1816	1175	N/A
Emergency	1672	750	$7.1M
Bank Investigator	1660	503	$4.1M
Investments	852	820	$78.6M
Prize	742	230	$3.2M
Merchandise	508	393	$0.8M

Top 10 frauds affecting seniors based on dollar loss in 2022:

Fraud Type	Reports	Victims	Dollar Loss
Investments	852	820	$78.6M
Romance	352	291	$19.5M
Service	2137	1669	$8.6M
Extortion	2193	475	$7.7M
Emergency	1672	750	$7.1M
Bank Investigator	1660	503	$4.2M
Prize	742	230	$3.2M
Foreign Money Offer	116	21	$2.4M
Grant	240	156	$1.6M
Recovery Pitch	85	62	$1.0M

➔ It is estimated that **5%-10%** of victims file a fraud report with the CAFC.

8) Reporting Fraud

Fraud is evolving. A fraud can often carry on over an extended period of time and is a crime that is difficult to recognize and report. To make reporting easier the CAFC suggests completing the following six steps:

Step 1: Gather all information pertaining to the fraud.
Step 2: Write out a chronological statement of events.
Step 3: Report the incident to your local law enforcement.
Step 4: Report the incident to the CAFC through the Fraud Reporting System (FRS) or toll free at 1-888-495-8501.
Step 5: Report the incident to the Financial Institution or Payment Provider used to send the money.
Step 6: If the fraud took place online, report the incident directly to the appropriate website.

9) Most Common Frauds and How to Protect Yourself

Below are the most common frauds affecting senior Canadians:

Identity Theft & Fraud
A victim of identity fraud has previously been the victim of identity theft.

Identity theft occurs when a victim's personal information is stolen or compromised. This can happen as a result of volunteering personal or financial information, a phishing fraud, a stolen wallet, a database breach, etc.

Identity fraud occurs when the fraudster uses the victim's information for fraudulent activity. Fraudsters may create fake identity documents, submit unauthorized credit applications and open financial accounts in your name, re-route your mail, purchase mobile phones, takeover your existing financial and social accounts, etc.

If you are 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 to obtain a copy of your credit report and review with reports.
  - **Equifax Canada**
  - **TransUnion Canada**
- **Step 3:** Report the incident to your local law enforcement.
- **Step 4:** Report the incident to the CAFC through the Fraud Reporting System (FRS) or toll free at 1-888-495-8501.
- **Step 5:** Review your financial statements and notify the affected agency if you notice any suspicious activity.
- **Step 6:** Notify your financial institutions and credit card companies, and change the passwords to your online accounts.
- **Step 7:** If you suspect that your mail has been redirected, notify Canada Post and any service providers.
- **Step 8:** Notify federal identity document issuing agencies:
  - **Service Canada**
  - **Passport Canada**
  - **Immigration, Refugees and Citizenship**
- **Step 9:** Notify provincial identity document issuing agencies.

Emergency - Grandparents Scam

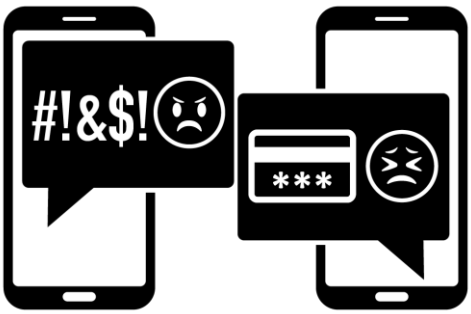
Suspects contact seniors or family members claiming that their grandchild or family member was in an accident, charged with an offence such as a DUI and drug offences or, in some cases, is ill with Covid-19. Suspects will claim that they are law enforcement officials, lawyers and even impersonate the grandchild/family member. They will proceed to advise the victim that a payment for supposed bail or fine is required immediately in order for the family member to avoid going to jail. If the victim agrees to pay the requested amount, suspects will arrange to pick up the funds in person or will ask the victim to send cash in the mail.

Be cautious of:

- **Urgency:**
  - Be suspicious of telephone calls that require you to immediately act and request bail money for a family member in distress.
  - Fraudsters will use urgency to get you to send the money or information before you have time to verify with other people if the request is legitimate.
- **Spoofing:**
  - Be careful with caller ID numbers that look familiar. Scammers use technology to disguise the actual number they are calling from (spoof) and make it appear as a trusted phone number.
- **Emotions:**
  - Fraudsters will play into your emotions by making you concerned about your loved one in order to get you to send money.
- **Gag orders:**
  - Fraudsters may threaten a gag order to isolate you and make sure you don't contact your family or loved ones. Don't fall for it!
- **Leading questions:**
  - The fraudster may try to get you to share personal information with them by asking you to "confirm" your personal information. Don't answer questions such as, "Can you please confirm your SIN?", "Can you please confirm your birth date, address etc.?". This is how they'll steal your information.
  - Grandparent scammers will also get you to provide them with information to make the story more believable, such as saying:
    - "Hey, it's your grandson."
    - "Jeremy, is that you?"
    - "Yes, it's Jeremy! I need help right away. Please send gift cards to pay my bail."

- **Time:**
  - No matter what a call says, you have time to do some research and contact others. Take a minute to think things through and talk with others.
- **Contact list:**
  - If you receive a suspicious phone call claiming to be from a loved one in an emergency situation, hang up the phone and contact them directly with the contact information you already had for them.
  - If the caller claims to be a law enforcement official, hang up and call your police directly.
- **Instincts:**
  - Listen to that inner voice that is screaming at you, "This doesn't sound right".
- **Privacy:**
  Be careful what you post online. Scammers can use details shared on social media platforms and dating sites for targeting purposes. Suspects can easily gather names and details about your loved ones.

Extortion

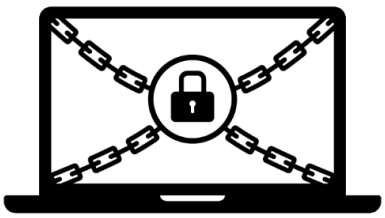


Extortion happens when someone unlawfully obtains money, property or services from a person, entity or institution through coercion.

SIN Scam Extortion: Targets get recorded messages about their Social Insurance Number (SIN) being linked to fraudulent or criminal activity. The recorded message claims to be from a federal government agency and states that your SIN has been blocked, compromised or suspended. There may be threats of an arrest warrant or imprisonment, if the target does not cooperate with the fraudster's demands. They may request personal information (SIN, date of birth, address etc.) or request that consumers empty their bank accounts and deposit the funds elsewhere. The fraudsters claim to want to clear the money from illegal activity and that it will be returned once their investigation is complete.

Hydro Extortion: A business or individual gets a call claiming to be from their hydro provider. The fraudster demands an immediate payment, typically via Bitcoin, or threatens that your power will be disconnected.

Ransomware: A type of malware designed to infect or block access to a system or data. A device can be infected by a malware in a number of ways, but it often starts with a victim clicking on a malicious link or attachment. At present, the most common form of ransomware will encrypt data. Once the system or data is infected, victims will receive the demand for ransom. There may also be threats of distributing the data publicly if the ransom is not paid.



Be cautious of:

- **Spoofing:**
  - Fraudsters use call-spoofing to mislead consumers. This technology is easily available. Never assume that the phone numbers appearing on your call display are accurate.
  - No government agency will contact you and tell you that your SIN is blocked or suspended, nor will they send threats of legal action.
  - No government or law enforcement agency will request payment by Bitcoin, a money service business, or gift cards (i.e. iTunes, Google Play, Steam).
- **Urgency:**
  - No government or law enforcement agency will use pressure and urgency to demand an immediate payment or to submit all of your money for investigation.
  - Fraudsters use this tool in hopes that you'll act before thinking things through.
- **Leading questions:**
  - The fraudster may try to get you to share personal information with them by asking you to "confirm" your personal information. Don't answer questions such as, "Can you please confirm your SIN?", "Can you please confirm your birth date, address etc.?". This is how they'll steal your information.
- **Time:**
  - Don't be pressured into sending information or money.
  - Time is on your side.
- **Security measures:**
  - Never provide personal information over the phone to an unknown caller.
  - Do not open unsolicited emails and text messages.
  - Do not click on suspicious links or attachments.
  - Regularly back-up important files.
  - Keep your operating system and software updated.
- **Resources:**
  - You're not alone!

- Contact local police immediately if you're experiencing a ransomware attack or threatened. Paying a ransom request does not guarantee that your files and devices will be restored. Fraudsters may continue to request additional funds.
- Have your systems reviewed by local technicians.
- Be familiar with your service provider's terms of service.
- Contact your service provider directly and verify that your account is in good standing.
- Report any database breach as per Canada's federal private sector privacy law, to the Personal Information Protection and Electronic Documents Act (PIPEDA).
- Learn how to recognize government frauds: https://www.canada.ca/en/revenue-agency/corporate/security/protect-yourself-against-fraud.html

Romance

Fraudsters use every type of dating or social networking site available to contact their victims. Their accounts are created using photos stolen from real people. Their background stories often mimic the victim's and they're often in the military, work overseas, or are successful business people. They 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. The fraudsters will never end up repaying the victim and continue to make empty promises while asking for more money.

Be aware of:

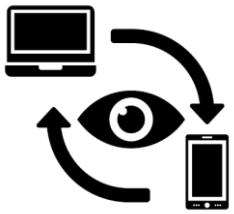
- **Excuses:**
  - When trying to setup an in-person meeting, be suspicious if they always cancel. Note: If you do proceed, meet in a public place and inform someone of the details.
- **Manipulation:**
  - Fraudsters will quickly profess their love for you and will say anything to gain your trust and returned affection. This is done to make it easier to convince you to send them money.
  - Fraudsters may claim to be wealthy and show pictures or other demonstrations to "prove" this wealth, but will still need to borrow money from you. Don't fall for their act.

Use Caution:

- Protect your heart and your wallet.
- Just like online shopping, if it seems too good to be true, it probably is.
- Use caution when meeting someone with an incredible story, extraordinarily complimentary and who has an 'ask' for you.
- Never send intimate pictures or videos of yourself; these can be used for blackmail or "sextortion".
- Never send or accept money under any circumstances. You may, unknowingly, be participating in money laundering and brought into a criminal scheme.

Service

These frauds often involve offers for telecommunications, internet, finance, medical, and energy services. In addition, extended warranties, insurance and sales services may also fall under this category.



Tech Support: Consumers receive an email, pop-up or a call claiming to be from a well-known tech company (e.g. Microsoft or Windows). The computer is said to be infected with malware or viruses, or that someone is attempting to hack it. The fraudster will offer to resolve the issue by gaining remote access to the computer. This allows them the opportunity to steal your personal information.

Lower Interest Rate: Fraudsters call consumers to offer a reduced interest rate on their credit card. The goal of the fraud is to collect the consumer's personal and credit card information.

Home Repairs and Products: Home owners are offered services at lower prices. These services can include air duct cleaning, furnace repairs, water treatment systems, or home renovations. If the services are completed at all, they are of low quality, offer impractical warranties or can cause further damage.

Be cautious of:

- **Remote access:**
  - By requesting remote access to your computer or device, the fraudsters can watch you type in your usernames and passwords or send themselves money.
- **"Great deals!"**
  - Fraudsters will offer low interest rates or services that are discounted or much better than competitor's rates.
  - They may claim they're new and don't have any reviews online yet so you can't search them up.
  - If it's too good to be true, it probably is.
  - If the services are completed at all, they are of low quality and can cause further damage.

- **Search engine optimization:**
  - Fraudsters frequently use search engine optimization for service scams. Make sure you are dealing with the official company by verifying the address, phone number and website address.
- **Local technicians:**
  - Never allow an individual to remotely access your computer. If you are experiencing problems with your operating system, bring it to a local technician.
  - Research all companies and contractors offering services before hiring them.
- **Credit card company:**
  - Verify any incoming calls claiming to be from your credit card company by calling the number on the back of your card. Be sure to end the original call and wait a few minutes before dialing or calling from a different phone.
- **Caution:**
  - Never provide any personal or financial information over the telephone, unless you initiated the call.
  - Only a credit card company can adjust the interest rate on their own product.
  - If you receive a call from your service provider, advise them that you will call them back and end the call.
  - Be suspicious about unsolicited phone calls, emails or pop-ups stating your computer/device is infected with a virus, a threat has been detected or a subscription will be automatically renewed.
- **Research:**
  - Look up the legitimate phone number for the company and communicate with them directly by always making the outgoing call.
  - For information on immigration scams, visit: http://www.cic.gc.ca/english/helpcentre/answer.asp?qnum=1206&top=31

Bank Investigator

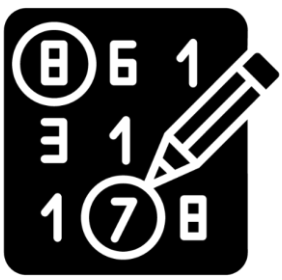
Fraudsters call consumers claiming to be a financial institution a major credit card provider or an online merchant such as Amazon. To prove the legitimacy of the call, the fraudsters often ask the consumer to end the call and immediately call the number on the back of their card. The fraudsters then inform the consumer that they are investigating unauthorized activity on their account. The fraudsters ask the consumer to help them catch the criminal. By providing remote access to their device, the fraudsters will claim to put money into the victim's account so that they can send *bait money*. Unfortunately, the funds seen going into the victim's account are coming from their other accounts and the money being sent is going directly to the fraudsters.

Be cautious of:

- **Early birds**
  - Fraudsters often call early in the morning, hoping to catch their targets by surprise or while they're still sleepy.
- **Phone line holds**
  - Fraudsters can make sure the phone line doesn't disconnect when you hang up (only on landlines). If you end a call on a landline phone and immediately dial another call, the original call may not be completely disconnected. Wait a few minutes or use another phone to complete another call.
  - Never provide personal or financial information over the phone unless you called your financial institution.
  - Financial institutions will never ask for help from the public for internal investigations. They will also never ask you to transfer money to an external account for security reasons. When in doubt, visit your bank branch in-person to verify the requests.
- **Friends and family**
  - If you get a strange call or message, reach out to those around you or a trusted authority and talk it out with them.
- **Control**
  - No one can or should pressure you into sending money/information or giving remote access to a device.

Prize

Consumers are informed that they are the winner of a large lottery or sweepstake even though they have never purchased a ticket or entered to win. Prior to receiving any winnings, the victim will be asked to pay a number of upfront fees. No winnings are ever received.



A variation of this fraud includes the consumer receiving a message from one of their friends on social media. The friend shares that they won a prize and asks the consumer if they have already collected their prize as they noticed their name was also on the winner's list. The consumer's friend encourages them to contact the person responsible for delivering the prizes. Unfortunately, unbeknownst to the victim, their friend's social account has been compromised and they have been communicating with the fraudster the entire time.

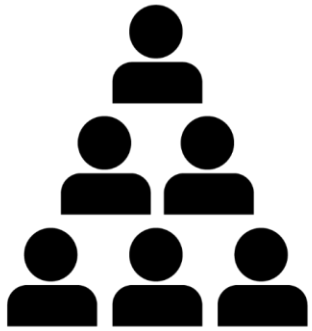
Be cautious of:

- **Excitement:**
  - The fraudsters will create excitement and offer a tempting prize, hoping you won't ask questions and will fill out any forms they ask you to or send "advanced" payment fees before collecting.
    - **Note:** In Canada, if you win a lottery, you are not required to pay any fees or taxes in advance.
- **Caution:**
  - Never give out personal or financial information to strangers.
  - Never send or accept money under any circumstances. You may, unknowingly, be participating in money laundering which is a criminal offence.
- **Research:**
  - Research the supposed prize or lottery you were told you've won.
  - Know that the only way to participate in any foreign lottery is to go to the country of origin and purchase a ticket. A ticket cannot be purchased on your behalf.

Investment Scams

Investment scams were the highest reported scams based on dollar loss in 2021 and 2022. Investment Scams are defined as any false, deceptive, misleading or fraudulent investment opportunity, often offering higher than normal or true monetary returns. Victims often lose most or all of their money. Investors run the added risk of having their identity stolen, accumulating losses for unauthorized withdrawals on their credit cards and incurring high interest payments on investments that do not exist.

Initial Coin Offerings: The virtual currency market is constantly changing. New virtual currencies are developed monthly. Like an Initial Public Offering (IPO), an Initial Coin Offering (ICO) is an attempt to raise funds to help a company launch a new virtual currency. In an ICO fraud, the fraudsters solicit investment opportunities with fake ICOs. They provide official looking documentation, use buzz words and may even offer a real "token". In the end, everything is fake, and you lose your investment.



Pyramids: Similar to a Ponzi scheme, a pyramid scam focuses primarily on generating profits by recruiting other investors. A common pyramid scam today takes the form of a "gifting circle". Participants gift a sum of money to join and ultimately must recruit others to make their money back. These schemes may offer products, but they usually have very little value.

Crypto Investment Scams: The majority of the investment scam reports involve Canadians investing in crypto currency after seeing a deceptive advertisement. It typically involves victims downloading a trading platform and transferring crypto currency into their trading account. In most cases, victims are not able to withdraw their funds. It is very likely that many of the trading platforms are fraudulent or controlled by fraudsters

Variations of Crypto Investment Scams

- The victim is approached on a dating or social media website. In some cases, the scam starts as a romance scam and quickly turns into an "investment opportunity". Because suspects have gained the victim's trust, it can lead to a high dollar loss for the victim.
- In some reports, suspects have compromised victim's friend's social media accounts. Because the victim believes they are communicating with a friend or a trusted person, they are easily convinced to take advantage of the "investment opportunity".
- The suspect calls a victim directly and convinces them to invest in crypto currency. In many cases, the suspect asks for remote access to the victim's computer. The suspect shows the victim a fraudulent crypto investing website and convinces the victim to invest based on the potential exponential growth of the investment. In many cases, the victim will invest over a long period of time and, in the end, will realize that the funds can not be withdrawn.
- An email is received by the victim offering a crypto investment opportunity.
- The victim comes across an advertisement on social media. After the victim clicks on the ad and provides their contact information, suspects contact the victim by telephone and convince them to invest.
-
- **Be cautious of:**
    - **Variety of solicitation methods:**
        - Investment fraudsters use various methods of solicitation including:
            - Search engine optimization
            - Compromised social media accounts
            - Ads on the internet and social media
            - Email or text message
            - Direct phone calls from fraudulent crypto investment companies

- Usually the solicitation will use urgency to get you to send money faster and have less time to think about the legitimacy of the investment.

- **An appealing sales pitch:**
  - Fraudsters will offer investment opportunities with higher than normal or true monetary returns.
  - Someone you meet on a dating or social media platform encourages you to invest into crypto currency, vouching that the company is "safe" or saying they're investing with them too.
  - Fraudsters will say whatever they have to, to get your money
- **Impersonation and spoofing:**
  - A "friend" tells you about a crypto currency investment opportunity via social media or email. This "friend" is actually a fraudster who has either hacked or spoofed one of your contact's accounts in order to scam you
- **Crypto currencies:**
  - Once a crypto currency transaction is complete, it is hard to reverse.
  - Proceeds of crime and anti-money laundering regimes around the world create regulatory frameworks that treat businesses dealing in crypto currencies as money service businesses.
  - Beware of fraudsters asking you to open and fund new crypto accounts. They will direct you to send it to wallets they control. Don't!
- **Caution:**
  - Be careful when sending cryptocurrency; once the transaction is completed, it is unlikely to be reversed.
  - Be wary of individuals met on dating sites or social media who attempt to educate and convince you to invest into crypto currency.
- **Research:**
  - As proceeds of crime and anti-money laundering regimes around the world create regulatory frameworks that treat businesses dealing in crypto currencies as money service businesses, Canadians need do their 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
- **Communication:**
  - If you receive a suspicious message from a trusted friend, reach out to them through a different means of communication to confirm that it is them.
  - Verify if the investment companies are registered with your Provincial Securities Agency or the National Registration Search Tool (www.aretheyregistered.ca).

- **Reason:**
    - The choice to open a wallet or invest should be yours, not someone else's.
    - 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 without going in and speaking to my bank or financial advisor?

Checklist: Be Cyber Secure and Fraud Aware

With fraud and cybercrime reporting going up again this year, the CAFC created the following checklists so that Canadians can be fraud aware and cyber secure in 2023.

Be Fraud Aware

- ✓ 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, 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.

EMERGENCY-GRANDPARENT SCAM

Fraudsters are targeting seniors by calling and pretending to be a family member in distress, the police or a justice official claiming that a loved one or grandchild is in trouble, and needs money immediately. **Victims are told there's a gag order, and can't speak to anyone.**

PROTECT YOURSELF

Fraudsters...

Call demanding immediate payment for bail, or fines to avoid going to jail

Remember! The courts won't ask for cash to bail out someone in custody, and will require people to be present in court.

Claim to be a lawyer, police or family member in an emergency situation demanding funds

Be suspicious of calls that require immediate action. **Hang up!** Call your local police and contact the family member directly.

Request cash and send couriers for pick up, or demand the victim send cash by courier services or via cryptocurrency

Never send cash, cryptocurrencies or any other funds to unknown persons, unverified addresses or bank accounts.

If you believe you have been scammed, contact your local police and the **Canadian Anti-Fraud Centre**:

1 (888) 495-8501 / antifraudcentre.ca

Fraud. Recognize. Reject. Report.