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

2022 Fraud Prevention Toolkit

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

Table of Contents

Introduction

While we know that the COVID-19 pandemic exposed new vulnerabilities and increased the potential of fraud victimization, we did not expect to see fraud losses more than double from 2020 to 2021. Losses reported to the Canadian Anti-Fraud Centre reached an all- time high of 379 million in 2021, with Canadian losses accounting for 275 million of this. Fraud Prevention Month is a campaign held each March to inform and educate the public on the importance of protecting yourself from being a victim of fraud. This year's theme is impersonation, and focuses on scams where fraudsters will claim to be government official, critical infrastructure companies, and even law enforcement officials.

March is Fraud Prevention Month. This year's efforts will focus on Impersonation Scams.

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

Throughout the year, the CAFC will be using the #kNOwfraud and #ShowmetheFRAUD descriptors to link fraud prevention messaging. We will also continue to use the slogan "Fraud: Recognize, Reject, Report".

During Fraud Prevention Month, the CAFC will post on its Facebook and Twitter platforms, using #FPM2022. Bulletins will also be published weekly on social media.

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

This Toolkit Includes:

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

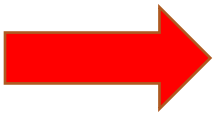
3) Competition Bureau of Canada Videos

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) Calendar of Events

Throughout the month of March, the CAFC will release a bulletin every week aimed at highlighting the top impersonation scams reported to CAFC in 2021.

Bulletins

Week 1: Investments
Week 2: Extortion Scams & Emergency Scams
Week 3: Phishing
Week 4: Spear Phishing

CAFC will highlight the weekly bulletin topic throughout each week.
Like us on Facebook – Canadian Anti-Fraud Centre
Follow us on Twitter – @canantifraud

March 2022 – An FPM video will be shared on social media highlighting ways to protect yourself from being a victim.

March 2022

	Tues March 1 Facebook & Twitter: #FPM2022 Introduction and Kick-Off	Wed March 2 Facebook & Twitter #FPM2022 Launch Video	Thurs March 3 Facebook & Twitter Bulletin- Investment Scams	Fri March 4 Facebook & Twitter Social Media Impersonation Investment Scams
Mon March 7 Facebook & Twitter Fake crypto investment websites	Tues March 8 Facebook & Twitter Share partner #FPM2022 posts	Wed March 9 Facebook & Twitter Request to transfer crypto investments to fraudulent platforms	Thurs March 10 Facebook & Twitter Share partner #FPM2022 posts	Fri March 11 Facebook & Twitter Pyramid, job and investment scams.
Mon March 14 Facebook & Twitter Bulletin: Extortion Scams	Tues March 15 Facebook & Twitter Threatening automated CBSA phone calls	Wed March 16 Facebook & Twitter Bulletin: Emergency/Grandparent Scam	Thurs March 17 Facebook & Twitter Share partner #FPM2022 posts	Fri March 18 Facebook & Twitter Threatening letters impersonating RCMP
Mon March 21 Facebook & Twitter Bulletin: Phishing	Tues March 22 Facebook & Twitter Share partner #FPM2022 posts	Wed March 23 Facebook & Twitter Phishing messages impersonating government agencies	Thurs March 24 Facebook & Twitter Share partner #FPM2022 posts	Fri March 25 Facebook & Twitter Phishing messages impersonating financial institutions
Mon March 28 Facebook & Twitter Bulletin: Spear Phishing	Tues March 29 Facebook & Twitter Spear Phishing stats and warning signs	Wed Mar 30 Facebook & Twitter Share partner #FPM2022 posts	Thurs March 31 Facebook & Twitter How to protect yourself from Spear Phishing scams	

7) 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.

8) Statistics

In 2021, the CAFC received 104,295 fraud reports involving over $379 million in reported losses. Moreover, 12,944 of the reports were from seniors, that reported losses totalling more than $83.5 million.

Top 10 frauds affecting seniors based on number of reports in 2021:

Fraud Type	Reports	Victims	Dollar Loss
Identity Fraud	4853	4853	N/A
Extortion	2483	391	$4.5 M
Service	1525	1051	$4.9 M
Personal Info	1519	878	N/A
Phishing	1389	356	N/A
Bank Investigator	858	339	$2.5 M
Prize	580	165	$2.5 M
Emergency	573	181	$1.9 M
Merchandise	492	401	$0.9 M
Investments	487	449	$38 M

Top 10 frauds affecting seniors based on dollar loss in 2021:

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

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

9) 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.

10) Most Common Frauds & How to Protect Yourself

Below are the most common frauds affecting senior Canadians:

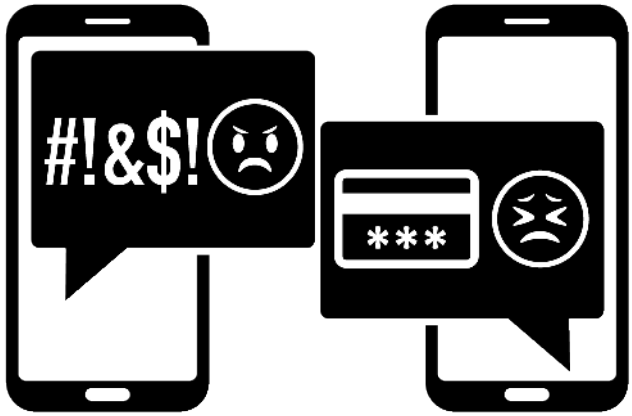
Emergency/Grandparents Scam
Suspects contact seniors or family members claiming that their grandchild or family member was in an accident, charged with an offence such as a DUI and drug offences or, in some cases, is ill with Covid-19. Suspects will claim that they are law enforcement officials, lawyers 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.

How to protect yourself

- If you receive a suspicious phone call claiming to be from a family member in an emergency situation, hang up the phone and contact them directly.
- If the caller claims to be a law enforcement official, hang up and call your police directly.
- Listen to that inner voice that is screaming at you, "This doesn't sound right".
- 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.
- Be suspicious of telephone calls that require you to immediately take action and request bail money for a family member in distress.
- 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.

Extortion

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



Hydro: The business receives a call claiming to be from their hydro provider. The fraudster demands an immediate payment, typically via Bitcoin, or their 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, most commonly, it 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.

Warning Signs – How to Protect Yourself

- Be familiar with your service provider's terms of service.
- Contact your service provider directly and verify that your account is in good standing.
- 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.
- 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?
- Report any database breach as per Canada's federal private sector privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA).

Romance

Fraudsters use every type of dating or social networking site available to contact their victims. Their accounts are created using photos stolen from legitimate people. Their background stories often mimic the victim's and they are 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 always run into trouble and are unable to refund their victims; however, they will continue to make empty promises and ask for more money.

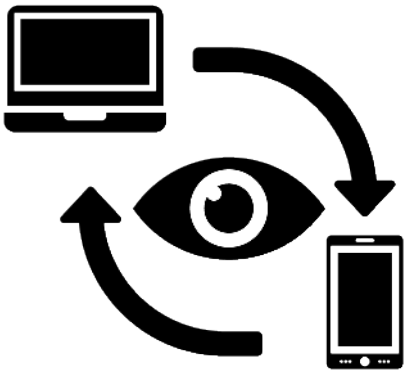
Warning Signs - How to Protect Yourself

- Beware of individuals quickly professing their love for you.
- Beware of individuals who claim to be wealthy, but need to borrow money.
- When trying to setup an in-person meeting, be suspicious if they always provide you with reasons to cancel. If you do proceed, meet in a public place and inform someone of the details.
- Never send intimate photos or video of yourself as they may be used to blackmail you.
- Never send or accept money under any circumstances. You may, unknowingly, be participating in money laundering which is a criminal offence.

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 a 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.



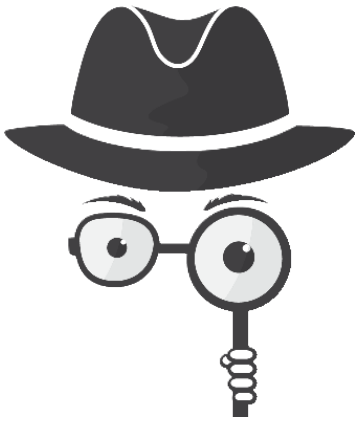
Lower Interest Rate: Fraudsters call consumers to offer a reduced interest rate on their credit card. The goal of the fraud is to collect the consumer's personal and credit card information.

Home Repairs & 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.

Warning Signs - How to Protect Yourself

- Never allow an individual to remotely access your computer. If you are experiencing problems with your operating system, bring it to a local technician.
- Verify any incoming calls with your credit card company by calling the number on the back of the card. Be sure to end the original call and wait a few minutes before dialing.
- 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.
- Research all companies and contractors offering services before hiring them.

Bank Investigator



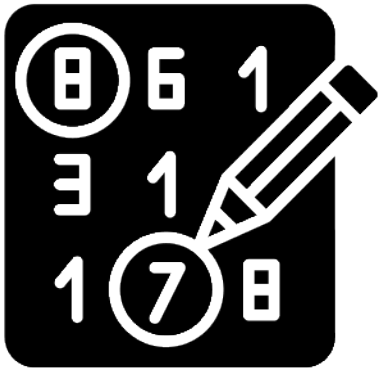
Fraudsters call consumers claiming to be a financial institution or a major credit card provider. To prove the legitimacy of the call, the fraudsters often ask the consumer to end the call and immediately call the number on the back of their card. The fraudsters then inform the consumer that they are 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.

Warning Signs - How to Protect Yourself

- Typically, these calls tend to happen early in the morning. Always make sure you are alert when dealing with finances.
- 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 assistance from the public for internal investigations. They will also never ask you to transfer money to an external account for security reasons.
- Never provide remote access to your device to unknown callers.

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.

Warning Signs - How to Protect Yourself

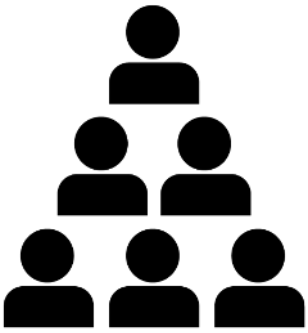
- Never give out personal or financial information to strangers.
- The only way to participate in any foreign lottery is to go to the country of origin and purchase a ticket. A ticket cannot be purchased on your behalf.

- In Canada, if you win a lottery, you are not required to pay any fees or taxes in advance.

Investment Scams

Investment scams were the highest reported scams based on dollar loss in 2021. Victims of investment scams reported a total loss of $169.9 Million to CAFC. 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 into 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.

Warning Signs – How to Protect Yourself

- Be careful when sending cryptocurrency. Once the transaction is completed, it is unlikely to be reversed.
- 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.
- 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).
- Prior to investing, ask for information on the investment. Research the team behind the offering and analyze the feasibility of the project.
- Be weary of individuals met on dating or social media who attempt to educate and convince you to invest into crypto currency.
- 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!

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 2022.

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.
- ✓ If you are having problems with your computer bring it to a local technician.