CANADIAN ANTI-FRAUD CENTRE BULLETIN

2021 Fraud Prevention Toolkit – Seniors 2021-02-15

FRAUD: RECOGNIZE, REJECT, REPORT

SENIORS

2021 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

As fraud rates continue to increase in Canada, the world is going through a global pandemic. The COVID-19 has created an environment that is ripe for fraud and online criminal activity. The COVID-19 has resulted in never-before-seen numbers of people turning to the internet for their groceries, everyday shopping, banking and companionship. Coupled with the profound social, psychological and emotional impacts of COVID-19 on people, one could argue that the pool of potential victims has increased dramatically.

March is Fraud Prevention Month. This year's efforts will focus on the Digital Economy of Scams and Frauds.

The Canadian Anti-Fraud Centre (CAFC) has compiled a toolkit specifically designed for senior Canadians (60+) to further raise public awareness and prevent victimization. We encourage all our partner 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 daily on its Facebook and Twitter platforms (#FPM2021). Our weekly bulletin will be published every Monday and, every Wednesday, we will host a #FraudChat at 1 p.m. (Eastern Time) on Twitter. Everyone is invited to join the conversation.

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 https://www.youtube.com/watch?v=0rlWUcc57dM
French: https://www.youtube.com/watch?v=cXXP35rICQY
A Cry from the Heart from Victims
https://www.youtube.com/watch?v=blyhHl8rc7g
French: https://www.youtube.com/watch?v=cHZfvpH2YW8
Telemarketing Fraud: The Seamy Side
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
https://www.youtube.com/playlist?list=PLbecW3cjtFJ6jyMpBlsY1NQkrj0-59Kp2
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. Videos are available in both official languages.
https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04272.html
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 Monday aimed at Recognizing Fraud and highlighting our weekly themes tied to the Digital Economy of Scams and Fraud. Every Wednesday, we will host a Twitter #FraudChat at 1 p.m. (Eastern Time) providing advice on breaking the contact with fraudsters.

Bulletins
Week 1: Buying and Selling Online
Week 2: Online Financial Scams
Week 3: Securing Your Accounts and Your Identity
Week 4: Email Scams
Week 5: Online Scams

Fraud Chats
Week 1: Fraud initiated by telephone call
Week 2: Fraud initiated by email or text message
Week 3: Fraud initiated online
Week 4: Fraud initiated on social networks
Week 5: Fraud initiated by mail or in person

On a daily basis, the CAFC will highlight a fraud topic on our social media accounts.
Like us on Facebook – Canadian Anti-Fraud Centre
Follow us on Twitter – @canantifraud

On **March 2, 2021** - Join us on Facebook for a live 13-hour Canada-wide Fraud Prevention Month launch event.

March 2021

Mon., March 1 Facebook & Twitter Bulletin - Buying & Selling Online	**Tues., March 2** Facebook **13-HR LIVE LAUNCH**	**Wed., March 3** Facebook & Twitter Puppy Scams **1 p.m. Eastern** #Fraudchat	**Thurs., March 4** Facebook & Twitter Rental Scams	**Fri., March 5** Facebook & Twitter Merchandise and Counterfeit scams
Mon., March 8 Facebook & Twitter Bulletin -Financial Scams	**Tues., March 9** Facebook & Twitter Investment Scams	**Wed., March 10** Facebook & Twitter Loan Scams **1 p.m. Eastern** #Fraudchat	**Thurs., March 11** Facebook & Twitter Grant Scams	**Fri., March 12** Facebook & Twitter Job Scams
Mon., March 15 Facebook & Twitter Bulletin -Protecting Your Information	**Tues., March 16** Facebook & Twitter Id Theft and Fraud	**Wed., March 17** Facebook & Twitter Social Media Scams **1 p.m. Eastern** #Fraudchat	**Thurs., March 18** Facebook & Twitter Securing your Accounts	**Fri., March 19** Facebook & Twitter Ransomware
Mon., March 22 Facebook & Twitter Bulletin – Email and Text Message Scams	**Tues., March 23** Facebook & Twitter Phishing	**Wed., March 24** Facebook & Twitter Spear Phishing **1 p.m. Eastern** #Fraudchat	**Thurs., March 25** Facebook & Twitter Extortion Scams	**Fri., March 26** Facebook & Twitter Prize Scams
Mon., March 29 Facebook & Twitter Bulletin – Prevalent Online Scams	**Tues., March 30** Facebook & Twitter Romance Scams	**Wed., March 31** Facebook & Twitter Immigration scams **1 p.m. Eastern** #Fraudchat	**Thurs April 1** Facebook & Twitter Fraud is no joke	

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 2020, the CAFC received 101,483 fraud reports involving nearly $160 million in reported losses. Moreover, 11,447 of the reports were from senior Canadians, that reported losses totalling more than $31.8 million.

Top 10 frauds affecting seniors Canadians based on number of reports in 2020:

Fraud Type	Reports	Victims	Dollar Loss
Extortion	3,651	1,207	$1.1 M
Personal Info	1,350	804	N/A
Phishing	1,047	268	N/A
Service	692	419	$6.5 M
Bank Investigator	524	228	$2.5 M
Emergency	501	172	$0.6 M
Merchandise	425	328	$0.4 M
Prize	408	133	$2.5 M
Vendor Fraud	279	105	$0.2 M
Romance	251	169	$7.3 M

Top 10 frauds affecting seniors Canadians based on dollar loss in 2020:

Fraud Type	Reports	Victims	Dollar Loss
Romance	251	169	$7.3 M
Service	692	419	$6.5 M
Investment	96	86	$6.1 M
Prize	408	133	$2.5 M
Bank Investigator	524	228	$2.5 M
Spear Phishing	183	84	$1.1 M
Extortion	3,651	1,207	$1.1 M
Inheritance	86	8	$0.8 M
Emergency	501	172	$0.7 M
Loan	55	35	$0.5 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:

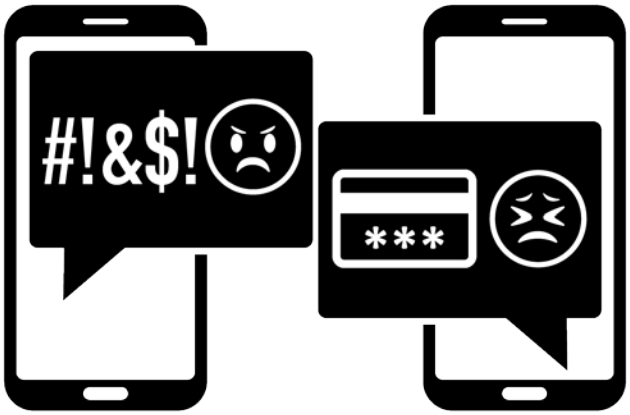
Step 1: Gather all information pertaining to the fraud.
Step 2: Write out a chronological statement of events.
Step 3: Report the incident to your local law enforcement.
Step 4: Report the incident to the CAFC through the Fraud Reporting System (FRS) or toll free at 1-888-495-8501.
Step 5: Report the 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:

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.

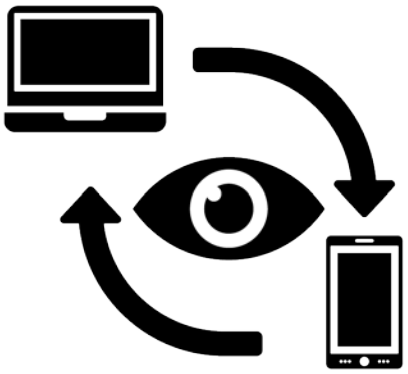
Warning Signs - How to Protect Yourself

- 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.

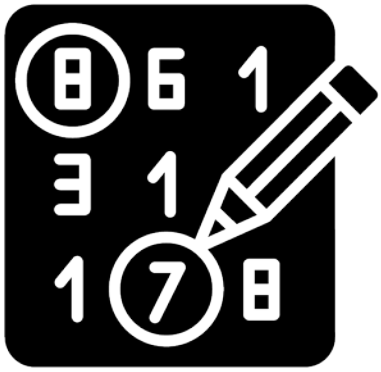
Bank Investigator

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 call 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.