

Toolkit for March Fraud Prevention Month 2019 Senior Support

#KNOWFRAUD

Fraud: Recognize. Reject. Report.



Table of Contents

Introduction	 3
RCMP Videos	 4
OPP Fraud Prevention Videos	 4
Competition Bureau Fraud Prevention Videos	 4
CAFC Logo	 4
Calendar of Events - Facebook and Twitter	 5
Statistics	 6
Scams Targeting Seniors	 7
 Emergency 	 7
 Prize 	 7
 Service – Tech Support Scam 	 8
 Romance 	 9
 Telephone Extortion – CRA Scam 	 9
 Bank Investigator 	 10
Recovery Pitch	 11

Introduction

In preparation for March Fraud Prevention Month, the Canadian Anti-Fraud Centre (CAFC) has compiled this toolkit specifically for seniors to further raise public awareness and help prevent victimization. We encourage all partners to use the CAFC logo, contact points, and resource materials in this



toolkit on their websites, in print and on their social media platforms. The CAFC will post daily on Facebook and Twitter (#FPM2019, #MPF2019) and be participating in the fraud chats: Use the following hashtag – #fraudchat – to join.

The CAFC is Canada's central repository for data, intelligence and resource material as it relates to mass marketing fraud and identity fraud. The CAFC does not conduct investigations but provides valuable assistance to law enforcement agencies all over the world by identifying connections among seemingly unrelated cases. Victims who report to the CAFC are also encouraged to report directly to their local police. Your information may provide the piece that completes the puzzle.

Senior consumers can report directly to the CAFC by calling toll free 1-888-495-8501 or online through the CAFC Online Fraud Reporting System (FRS).

English - http://www.antifraudcentre-centreantifraude.ca/reportincident-signalerincident/index-eng.htm

French - http://www.antifraudcentre-centreantifraude.ca/reportincident-signalerincident/index-fra.htm

Comments, questions or feedback on Fraud Prevention Month are always welcomed.

Thank you,
The CAFC Fraud Prevention Team



Follow us on Twitter - <u>@canantifraud</u>
Like us on Facebook - <u>Canadian Anti-Fraud Centre</u>

This Toolkit Includes:

1) RCMP Videos

- Face of Fraud Commercial (YouTube) https://www.youtube.com/watch?v=0rlWUcc57dM
- A Cry from the Heart from Victims, Romance Scam (YouTube) https://www.youtube.com/watch?v=blyhHl8rc7g French video with English subtitles
- Telemarketing Fraud: The Seamy Side (YouTube) https://www.youtube.com/watch?v=t7bhQJkelEg

2) OPP Fraud Prevention Videos

CAFC staff and volunteers highlight a number of well-known scams in these short videos. Videos are available in both official languages.

- English (YouTube)
 https://www.youtube.com/user/OPPCorpComm/search?query=scam
- French (YouTube)
 https://www.youtube.com/user/OPPCorpCommfr/search?query=scam

3) Competition Bureau of Canada Fraud Prevention 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.

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

4) CAFC Logo





5) Calendar of Events - Facebook and Twitter "Scam of the Day"

Every day in March, the CAFC will highlight a particular scam on both Facebook and Twitter that will link directly to the CAFC website (information is available in both official languages). See the calendar of events below. Scams involving Seniors will be highlighted in week 4.



March 2019

Sun	Mon	Tue	Wed	Thu	Fri	Sat
					1 Facebook & Twitter Importance of Reporting	2
3	4 Facebook & Twitter Sale of Merchandise Bulletin Loan	5 Facebook & Twitter Phishing	6 Facebook & Twitter Personal Info	7 Facebook & Twitter Loan	8 Facebook & Twitter Job	9
10	11 Facebook & Twitter Extortion Bulletin Extortion	12 Facebook & Twitter Romance	13 Facebook & Twitter Investments	14 Facebook & Twitter Merchandise (Counterfeit)	15 Facebook & Twitter Vacation	16
17	18 Facebook & Twitter Emergency Bulletin Service	19 Facebook & Twitter Prize	20 Facebook & Twitter Service	21 Facebook & Twitter Bank Investigator	22 Facebook & Twitter Recovery Pitch	23
24	25 Facebook & Twitter Wire Fraud Bulletin Card Not Present	26 Facebook & Twitter Card Not Present	27 Facebook & Twitter Grant	28 Facebook & Twitter Directory	29 Facebook & Twitter Spear Phishing	30

Follow us on Twitter – <u>@canantifraud</u> Like us on Facebook – <u>Canadian Anti-Fraud Centre</u>

6) Statistics:

In 2018, the CAFC received 59,009 fraud reports from Canadian consumers and businesses. The total reported Canadian losses were \$97,654,160.35. The top 10 scams affecting seniors during this time are listed below:



Top 10 senior scams based on number of complaints in 2018:

Complaint Type	Reports	Victims	Dollar Loss
Extortion	6,119	262	\$1,425,119.85
Service	2,284	967	\$1,419,699.12
Phishing	2,215	606	\$44,383.08
Personal Information	1,224	586	\$74,993.11
Prize	1,023	271	\$2,683,656.29
Unknown	638	34	\$42,732.32
Bank Investigator	517	189	\$1,169,217.16
Emergency	324	119	\$630,349.02
Romance	315	223	\$9,096,390.41
Merchandise	315	211	\$1,523,014.92



Top 10 senior scams based on dollar loss in 2018:



Complaint Type	Reports	Victims	Dollar Loss
Romance	315	223	\$9,096,390.41
Prize	1,023	272	\$3,270,419.49
Investments	62	51	\$2,683,656.29
Job	115	27	\$2,190,376.40
Merchandise	315	211	\$1,523,014.92
Service	2,284	967	\$1,419,699.12
Extortion	6,119	262	\$1,425,119.85
Inheritance	165	18	\$1,320,749.24
Bank Investigator	517	189	\$1,169.217.16
Emergency	324	119	\$630,349.02

→ Fewer than 5% of fraud victims will file a report with the CAFC.

7) Fraud Warnings / Bulletins

Below are a few common frauds targeting seniors, which will be highlighted during week 4 of Fraud Prevention Month (March 18th-22nd).



Monday, March 18Th, 2019 - Scams Targeting Seniors Bulletin: Service

Emergency

Scammers use social media, the internet and phones to target potential senior victims with the emergency pitch. Seniors receive a call claiming to be a family member or a close friend describing an urgent situation that requires immediate funds. Common themes have been that the family member was arrested or got into an accident while travelling abroad. Monies are required for hospital expenses, lawyer fees or bail. Usually the potential victim is instructed to send money via a money service business like Western Union or MoneyGram.



Warning Signs - How to Protect Yourself

- Confirm with other relatives the whereabouts of the family member or friend.
- Police, judges or legal entities will never make urgent requests for money.
- Never voluntarily give out family members' names or information to unknown callers.
- Always question urgent requests for money.

Prize

Canadians are solicited over the phone, by mail, email or through social media websites with claims that they are the winner of a large lottery or sweepstake. Prior to receiving any winnings, they must first pay an upfront fee. No winnings are ever received. The scammers constantly re-invent the wheel and come up with new twists to prey on potential victims. The CAFC continues to receive reports where seniors receive a call from an individual who claims to represent "Reader's Digest", or "Publisher's Clearing House". Scammers advise that you have won a prize (cash and car) and in



order to receive the winnings you are required to pay a *small* advance fee to cover taxes or legal fees associated to the win. Scammers target seniors, use their financial information to take over their accounts, which is then used to launder money and proceeds from other mass marketing fraud scams.



Warning Signs – How to Protect Yourself

- Legitimate lottery companies will never demand payments before releasing winnings.
- You must purchase a ticket to win the lottery.
- Consumers cannot win foreign lotteries unless they have specifically attended that country and purchased a ticket.
- Beware of counterfeit cheques or other forms of payment the fraudsters will send to help cover fees such as tax payment, lawyers' fees, customs, etc.

Service- Tech Support Scam

Microsoft/Windows Technician: Scammers call and claim to be a representative from a well-known tech company such as Microsoft or Windows. The scammers will claim that the victim's computer is sending out viruses or has been hacked and must be serviced. The scammer will remotely access the victim's computer and may run programs or alter settings. The scammer will advise that a fee is required for this service and request payment by credit card or money service business. In certain cases, the scammer will transfer funds from the victim's computer through a money service business such as Western Union or MoneyGram.





Warning Signs - How to Protect Yourself

- Do not provide personal information on incoming phone calls.
 Verify the caller.
- Microsoft and other well-known computer companies will not conduct proactive outbound calls for computer repair.
- Never provide unsolicited callers remote access to your computer.
- Request a call back number, verify and do your due diligence.

Romance

There are a growing number of people who are turning to the internet to find companionship and love. Unfortunately, scammers know this and use every type of dating or social networking site available to seek out potential victims.





The scammer will gain the trust of the victim through displays of affection and will communicate via phone, skype and email for months if needed to build trust. The scammer will often claim to be working abroad, usually in a lucrative business venture. Eventually the scammer will want to meet with the victim in person. It is at this time that the scammer will inform they cannot afford to travel and will ask for money to cover travel costs. Other variations include the scammer claiming that there is a medical emergency with a sick family member and will ask for money to cover medical expenses.

Warning Signs - How to Protect Yourself

- Fraudsters want to develop a quick relationship. Be suspicious when someone you have not met professes their love for you.
- Be wary when someone claims to be involved in a lucrative business but needs to borrow money for bills and expenses.
- Be cautious when chatting to an individual who claims to live close but works overseas.
- Do not cash any cheques or send the person any money for any reason, whatsoever!

Telephone Extortion - CRA Scam

Fraudsters call consumers impersonating the Canada Revenue Agency (CRA) claiming a recent audit has identified discrepancies from past filed taxes. Repayment is required immediately. Fraudsters threaten consumers that failure to pay will result in additional fees and/or jail time. Fraudsters often request payment by a money service business or prepaid cards or gift cards (iTunes).



Warning Signs – How to Protect Yourself

- Contact the CRA to confirm you owe back taxes or are entitled to a refund.
- Never provide personal information on inbound phone calls. Ask who is calling, document information and do your homework
- The CRA would never request payment by money service business or iTunes gift cards.
- If you have shared personal information, contact Equifax and Trans Union to place fraud alerts on your account.
- For more information from the CRA, visit:

https://www.canada.ca/en/revenue-agency/news/newsroom/tax-tips/tax-tips-2018/what-to-expect-cra-contacts-you.html

Bank Investigator

Fraudsters contact consumers by phone asking for their assistance to catch a bank employee who has been stealing money. The consumer is instructed to go to their bank and make a cash withdrawal from their account. They are told not to tell the bank teller what they are doing because the teller may be involved. The consumer is instructed to place the cash in an envelope and meet the "investigator" in a nearby parking lot where the cash is turned over.



In a variation of this scam, a consumer receives a call from fraudsters purporting to be from their bank or a major credit card provider. The fraudsters advise that they are investigating unauthorized charges on the consumer's account or that their account was compromised. In some cases, the fraudsters demand that the consumer provides their credit card information. They also instruct the consumer to send money as "bait money" to help catch the "employee", using a money wire service such as Western Union or MoneyGram.

Warning Signs - How to Protect Yourself

- Never share banking information over the phone unless you have called your bank.
- Financial institutions will never solicit assistance from their customers or the general public for an internal investigation.

Recovery Pitch

If you have been victimized in the past, you are likely to be contacted again by someone promising to get your money back. The imposter may claim to be an investigating agency, law enforcement representative or lawyer. The fraudster will claim a recent investigation has found a guilty party and money was recovered from a previous scam. Often, victims are promised a



portion or all of their lost funds, only if legal fees and taxes are paid. Scammers may purchase "lead lists", which include your information and involvement in past scams.



Warning Signs - How to Protect Yourself

- If you are the victim of a scam, you are likely to be called again by someone promising you a refund. Be careful not to lose more money.
- No government or law enforcement agency will ask you to participate in a sting operation to recover your lost funds.
- Do not pay money to get money.



If you think you or someone you know has been a victim of fraud, please contact the Canadian Anti-Fraud Centre at 1-888-495-8501 or report online through the Fraud Reporting Tool (FRS) at http://www.antifraudcentre-centreantifraude.ca/reportincident-signalerincident/index-eng.htm