

Toolkit for March Fraud Prevention Month 2019 Middle Agers

#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 Middle Agers	 7
 Telephone Extortion – CRA Scam 	 7
 Romance 	 8
 Investments 	 8
 Buying Online and Counterfeit Goods 	 9
 Merchandise 	 10
• Vacation	 11

Introduction

In preparation for March Fraud Prevention Month, the Canadian Anti-Fraud Centre (CAFC) has compiled a toolkit specifically designed for middle aged Canadians to further raise awareness and help prevent victimization. We encourage all partnering organizations to use the CAFC logo, contact points



and resource materials in this toolkit on their website, in print and on their social media platforms. The CAFC will post daily on Facebook and Twitter daily (#FPM2019, #MPF2019) and 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.

Middle Aged 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 Middle Agers will be highlighted in week 3.



March 2019

Sun	Mon	Tue	Wed	Thu	Fri	Sat
					1 Facebook & Twitter Importance of Reporting	
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	3
10	11 Facebook & Twitter Extortion Bulletin Extortion	12 Facebook & Twitter Romance	13 Facebook & Twitter Investments	14 Facebook & Twitter Merchandise (Counterfeit)	15 Facebook & Twitter Vacation	10
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	17
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	24

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

6) Statistics

In 2019, 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 reported scams affecting young adults during this time are listed below.



Top 10 middle agers scams based on number of complaints in 2018:

Complaint Type	Complaints	Victims	Dollar Loss
Extortion	12,964	888	\$6,387,477.67
Phishing	2,783	918	\$39,937.43
Personal Info	2,123	1,290	\$1,042,659.09
Service	1,700	762	\$1,971,270.24
Merchandise	1,079	754	\$990,863.56
Sale of Merchandise	742	466	\$325,987.58
Job	654	183	\$1,124,326.93
Romance	570	370	\$12,588,723.90
Counterfeit Merchandise	538	518	\$117,687.56
Prize	461	108	\$145,741.86



Top 10 middle ager scams based on dollar loss in 2018:



Complaint Type	Complaints	Victims	Dollar Loss
Romance	570	370	\$12,588,723.90
Extortion	12,964	888	\$6,387,477.67
Investments	120	80	\$4,925,095.41
Service	1,700	762	\$1,971,270.24
Job	654	183	\$1,124,326.93
Personal Info	2,123	1,290	\$1,042,659.09
Merchandise	1,079	754	\$990,863.56
Timeshare	22	16	\$601,044.87
Loan	352	225	\$598,277.83
Bank Investigator	142	37	\$373,219.39

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

7) Fraud Warnings / Bulletins

Below are a few common frauds targeting Middle agers, which will be highlighted during week 3 of Fraud Prevention Month (March $11^{th} - 15^{th}$).



Monday, March 11th, 2019 - **Scams Targeting Middle Agers** Bulletin: **Extortion**

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.
- If you have shared banking information with the scammers, contact your financial institution to place 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

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!

Investments

Any false, deceptive, misleading or fraudulent investment opportunity, often offering higher than normal or true monetary returns, in which consumers lose most or all of their money. One of the most common investment scams involves Binary Options. Similar to gambling, binary options work much like a wager. All or nothing "bets" are invested based on how an asset, stock, currency or commodity will perform within a certain timeframe.



Websites are designed to attract users to trade binary options by offering high rates of return and by claiming to be risk free. At the beginning, a gain is seen but there is no way to access the profits because they are virtually non-existent. There are currently no businesses registered or authorized to sell/market Binary Options in Canada. Investors who buy into Binary Options are at risk of identity theft and substantial losses.



Warning Signs – How to Protect Yourself

- Be cautious when asked to provide personal information and credit card details over the phone and internet.
- Do your due diligence, research an investment opportunity and seek the council of an independent third party as well as the security regulator for your province.
- Prior to investing, ask for information on the investment. Check the registration and enforcement history.
- The Canadian Securities Administrator (CSA) encourages all investors to visit www.aretheyregistered.ca

Buying Online and Counterfeit Goods

Canadians need to be cautious when buying merchandise online and are encouraged to fully review feedback and deal with companies or individuals that they know by reputation or past experience. If the buyer is not familiar with a particular seller, they should independently verify who they are. A good rule of thumb: if the asking price of a product is too good to be true, it is.



Counterfeiters have also become proficient in producing websites that have the same look and feel as the legitimate manufacturer. Counterfeit products are far inferior and in many cases could pose a significant health risk to consumers. For example: counterfeit jackets have been found to contain bacteria, fungus and mildew.

Everybody should do their due diligence and thoroughly research an online store or website prior to making a purchase. Confirm that you are dealing with the actual manufacturer and look for any warnings posted on their website.

Warning Signs - How to Protect Yourself

- Confirm you are dealing with the actual manufacturer and look for any warnings posted online.
- CAFC
- Use a credit card when shopping online. Customers are offered protection and may receive a refund.
- Inspect the website thoroughly. Often counterfeit sites will contain spelling mistakes and grammatical errors.
- Online manufacturers generally use their own company email account. If a web-based email like Gmail, Hotmail, or Yahoo is listed on the website under the contact details, this is a red flag.

Merchandise

These scams involve the non-delivery of goods purchased through classified ads over the internet or internet auction sites, through a catalogue or by mail order. Merchandise scams can vary depending what the consumer is purchasing. The most common variations include puppy, rental units, and motor vehicles.



Puppy: Classified ads target dog lovers with the promise of a puppy, but only once all the necessary fees are paid. Scammers advise they have recently moved and to facilitate a quick transaction, are giving the dog away. The catch? The buyer is responsible to pay for shipping, insurance, customs, etc.



Rental: Scammers post ads of desirable rental units at discounted rates. Victims who contact the "owner", are asked to provide a deposit on the rental – often by wire transfer. Consumers who attend the units may witness it's for sale and the scammer copied the pictures/details from the real estate listing.

Motor Vehicle: Scammers post ads selling vehicles at below cost. The scammers typically claim to be located overseas and that a third party agency would be used to ship the vehicle to the third party agency to hold until the vehicle is delivered. The car is never delivered and the money is lost.

Warning Signs - How to Protect Yourself

- Never send money to strangers. Reduce your risk of victimization.
- Know the average asking price. If it is too good to be true, it is.
- When searching for rentals, visit the address. Schedule a showing to confirm availability.
- Limit your risk and buy local. View the merchandise in person to validate the sale.
- Complete open source searches on the seller see if others have reported a scam.

Vacation

The victim received an unsolicited call, usually automated, advising that they have won a free or discounted vacation. Scammers use the names of well-known companies including WestJet, Air Canada, Transat and others. Once the *potential* victim proceeds with the call they are asked to provide personal information to book the trip. Victims are asked to provide a credit card number to make a deposit or payment to guarantee the trip. Victims either receive a trip of low quality at a higher price or no trip at all.

Another variation involves re-sold tickets. In this case, scammers post a vacation for sale online using a classified ads. The victim contacts the seller and agrees to purchase the vacation being sold; can include airline tickets and/ or accommodations. Fraudsters will urge the purchaser to pay in full before the tickets are transferred. Unbeknownst to the victim these tickets (were purchased fraudulently) are invalid/fake so when the victim goes to use them they are denied at the gate. Any ticket that can be re-sold is subject to this scam.

Warning Signs - How to Protect Yourself

- Be wary of unsolicited calls that advise you've won a contest you did not enter.
- Do not provide personal/ payment information on inbound calls.
- Verify the offer you are being presented.
- Purchase tickets direct from businesses or through legitimate resellers.





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