Toolkit for March Fraud Prevention Month 2018

Middle Agers

FRAUD: Recognize. Reject. Report.

Table of Contents

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 actively be posting on Facebook and Twitter daily (#FPM2018, #MPF2018) 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. Victims who report to the CAFC are also encouraged to report directly to their local police. 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. Your information may provide the piece that completes the puzzle. The CAFC is a support agency to law enforcement.

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

Canadian Anti-Fraud Centre
CAFC
Centre antifraude du Canada
FRAUD: RECOGNIZE IT. REPORT IT. STOP IT. LA FRAUDE : IDENTIFIEZ-LA. SIGNALEZ-LA. ENRAYEZ-LA.

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

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/03809.html#tab2
- French - http://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/03809.html#tab2

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 2018

Sun	Mon	Tue	Wed	Thu	Fri	Sat
				1 **Facebook & Twitter** Introduction to #FPM2018 **Bulletin** What to do if you're a victim	2 **Facebook & Twitter** Importance of Reporting	3
4	5 **Facebook & Twitter** Counterfeit **Bulletin** Continuity Scams	6 **Facebook & Twitter** Phishing	7 **Facebook & Twitter** Merchandise	8 **Facebook & Twitter** Job	9 **Facebook & Twitter** Sale of Merchandise	10
11	12 **Facebook & Twitter** Service **Bulletin** Binary Options	13 **Facebook & Twitter** Extortion	14 **Facebook & Twitter** Personal Info	15 **Facebook & Twitter** Loan	16 **Facebook & Twitter** Investments	17
18	19 **Facebook & Twitter** Romance **Bulletin** ID Fraud	20 **Facebook & Twitter** Lottery	21 **Facebook & Twitter** Recovery Pitch	22 **Facebook & Twitter** Emergency	23 **Facebook & Twitter** Bank Investigator	24
25	26 **Facebook & Twitter** Card-Not-Present **Bulletin** Cryptocurrencies	27 **Facebook & Twitter** Grant	28 **Facebook & Twitter** Wire Fraud	29 **Facebook & Twitter** Directory	30 **Facebook & Twitter** #Whatthefraud	31

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

6) Statistics

In 2017, the CAFC received 71,793 mass marketing fraud complaints with a total reported dollar loss of $110,329,034.47. 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 2017:

Complaint Type	Complaints	Victims	Dollar Loss
Extortion	6,164	514	$2,591,581.89
Phishing	3,764	1,220	$138,060.91
Service	1,838	767	$1,168,187.40
Personal Info	1,767	956	$312,771.93
Merchandise	1,357	923	$2,059,273.27
Sale of Merchandise	1,078	609	$399,668.27
Counterfeit Merchandise	969	940	$261,690.81
Job	896	243	$1,614,083.29
Prize	640	105	$866,821.84
Romance	601	354	$8,820,424.31

Top 10 Middle Ager scams based on dollar loss in 2017:

Complaint Type	Complaints	Victims	Dollar Loss
Romance	601	354	$8,820,424.31
Investment	169	126	$4,766,713.04
Extortion	6,164	514	$2,591,581.89
Merchandise	1,357	923	$2,059,273.27
Job	896	243	$1,614,083.29
Wire Fraud	54	11	$1,378,994.42
Service	1,838	767	$1,168,187.40
Prize	640	105	$866,821.84
Timeshare	31	21	$814,133.87
Loan	405	272	$537,972.17

➔ It's believed that fewer than **5%** of victims file a report with the CAFC regarding Mass Marketing Fraud.

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 12th – 16th).

Theme 2 - Monday, March 12th, 2018 - **Scams Targeting Middle Agers**
Bulletin: **Binary Options**

Service

Microsoft/Windows Technician: Scammers call and purport 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.

Extortion

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 pre-paid 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.
- For more information about fraud scams involving the CRA, visit www.cra-arc.gc.ca
- 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.

Personal Information

Any solicitation where an individual is asked for – or to verify – private and personal information.

Warning signs—How to Protect Yourself

- Never provide your personal information over the telephone unless you initiated the call.
- Lock your financial documents and personal information in a safe place at home, and lock your wallet or purse in a safe place.
- Shred receipts, credit card offers, credit card applications, insurance forms, cheques, bank statements, and similar documents when you don't need them any longer.

Loan

Commonly, loan scam ads are found through online advertising or deceitful websites designed to look like a legitimate lending institution. Consumers who apply are asked to provide personal information, which can lead to ID fraud. Since all consumers are approved, fraudsters demand victims pay an upfront fee to secure the loan. Victims are assured the loan will be deposited into their account within 24 hours of sending the fees. Once a victim sends money, communication with the fraudster usually stops and no money is ever received.

Warning Signs - How to Protect Yourself:

- If you are asked to make payments via email money transfer, money service business, or pre-paid credit cards cease all contact immediately.
- Contact consumer protection agencies and regulators to ensure that the company is a legitimate lender.
- It is illegal for a company to request an upfront fee prior to obtaining your loan.
- Beware of companies offering a guaranteed loan even if you have bad or no credit.
- Advertising through a recognized media outlet does not ensure that the ad was placed by a legitimate company.

Investment

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.

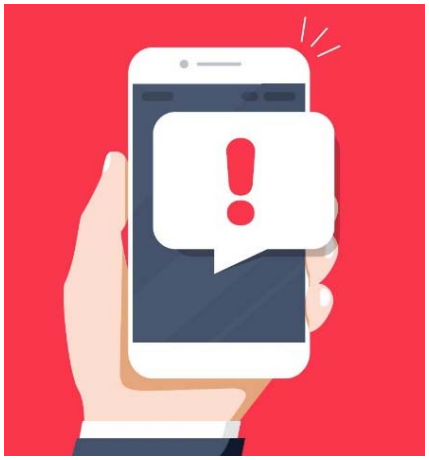
Investors who buy into Binary Options are at risk of identity theft and substantial losses.

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

Text Message

With the popularity of text messaging, the Canadian Anti-Fraud Centre warns consumers to be on the lookout for unsolicited and unwanted text message scams. Text messaging scams occur when scammers use deceptive text messages to lure consumers into providing personal or financial information. The scammers send text messages impersonating government agencies, banks, telephone providers or other companies. Like other types of phishing scams, these text messages typically ask consumers to provide usernames, passwords, credit/debit, PINs and other sensitive information that can be used to commit financial crimes. These scam messages can also offer job opportunities i.e. Mystery Shopper/Car Wrapping.



Warning Signs – How to Protect Yourself

- Beware of unsolicited text messages from individuals or organizations prompting you to click on an attachment or link. Do not click on "ANY" links.
- Watch for spelling and formatting errors.
- Do your research. A simple search on the internet can save you thousands of dollars.

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 at http://www.antifraudcentre.ca