2020 Fraud Prevention Toolkit:

Young Adults

#KNOWFRAUD
#SHOWMETHEFRAUD
FRAUD: Recognize. Reject. Report.

Table of Contents

Introduction

The Canadian Anti-Fraud Centre (CAFC) has compiled a toolkit specifically designed for young adult Canadians 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 encourage our partners to make use of these hashtags as well as #Take5 and #Tell2, protect many. Take Five is a successful national campaign that was first launched by UK Finance; it encourages consumers to pause, reflect and not react under the pressure of fraudsters. #Tell2 is a movement that was started by D.C. Tony Murray from Durham Fraud (UK). The initiative asks consumers to prevent fraud by sharing anti-fraud messaging with at least two people and encouraging them to do the same. An unbroken chain of 25 Tell2'ers would cover the entire population of Canada.

During Fraud Prevention Month (March), the CAFC will post daily on its Facebook and Twitter platforms (#FPM2020). Our weekly bulletin will be published on Mondays and, on Wednesdays, we will host a #FraudChat at 1PM Eastern on Twitter. Everyone is invited to join the conversation.

The CAFC is Canada's central repository for data, intelligence and resource material as it relates to fraud. The CAFC does not conduct investigations but provides valuable assistance to law enforcement agencies by identifying connections all over the world. Victims who report to the CAFC are also encouraged to report directly to their local police. The information provided may be the clue needed to solve the puzzle.

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

Comments, questions or feedback on fraud prevention are always welcomed.

Thank you,
The 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 on Mondays. On Wednesdays, we will host a Twitter #FraudChat at 1PM (Eastern). Both will be based on the following weekly fraud prevention themes:

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

On a daily basis, the CAFC will highlight a "Fraud of the Day" on our social network accounts. See the calendar below for more details.

On **March 2, 2020** - Join us on Facebook for a live 13-hour Canada-wide Fraud Prevention Month launch event.

March 2020

Sun	Mon	Tue	Wed	Thu	Fri	Sat
1 Tools used by Fraudsters	2 Personal Information **LIVE LAUNCH** **Bulletin**	3 Directory	4 Charity **Fraudchat**	5 Gift Cards for Payments	6 Prize	7 Vacation
8 Phishing	9 ID Theft & Fraud **Bulletin**	10 Spear Phishing	11 Extortion **Fraudchat**	12 Ransomware	13 SIM Swap	14 Emergency
15 Subscriptions	16 Job **Bulletin**	17 Sale of Merchandise	18 Merchandise **Fraudchat**	19 Overpayments	20 Investment	21 Rental
22 Service	23 Puppy **Bulletin**	24 Account Takeover	25 Gifting Circle **Fraudchat**	26 Grant	27 Romance	28 Sextortion
29 Inheritance	30 Winner winner **Bulletin**	31 Card-Not-Present	April 1 Fraud is no joke **Fraudchat**			

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

7) Statistics

In 2019, the CAFC received 46,465 fraud reports from Canadian consumers and businesses. The total reported Canadian losses were $96,163,328.64. The top 10 reported scams affecting young adults during this time are listed below.

Top 10 frauds affecting young adults based on number of reports in 2019:

Fraud Type	Reports	Victims	Dollar Loss
Extortion	2,094	836	$2,696,254.65
Personal Info	1,565	1,215	
Sale of merchandise	882	775	$485,689.38
Job	715	335	$868,806.57
Phishing	668	329	
Merchandise	632	511	$545,856.57
Service	373	256	$285,936.04
Loan	105	87	$165,480.08
Romance	90	73	$403,089.31
Spoofing	61	41	

Top 10 frauds affecting young adults based on dollar loss in 2019:

Fraud Type	Reports	Victims	Dollar Loss
Extortion	2,094	836	$2,696,254.65
Job	715	335	$868,806.57
Merchandise	632	511	$545,856.57
Sale of merchandise	882	775	$485,689.38
Investments	49	44	$425,119.55
Romance	90	73	$403,089.31
Service	373	256	$285,936.04
Loan	105	87	$165,480.08
Inheritance	9	3	$99,753.78
Spear Phishing	41	34	$55,769.66

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

8) Reporting Fraud

The Canadian Anti-Fraud Centre (CAFC) estimates that less than 5% of mass marketing fraud is ever reported. In an effort to increase this number, the CAFC suggests following the six steps below.

Step 1: Gather all information pertaining to the fraud.
Step 2: Report the incident to your local law enforcement.
Step 3: Report the incident to the CAFC online through the Fraud Reporting System (FRS) or toll free at 1-888-495-8501.
Step 4: Report the incident to the Financial Institution or Payment Provider used to send the money.
Step 5: If the fraud took place online, report the incident directly to the appropriate website.
Step 6: Follow the RCMP Identity Theft and Fraud Assistance Guide: http://www.rcmp-grc.gc.ca/scams-fraudes/victims-guide-victimes-eng.htm

9) Common Frauds & How to Protect Yourself

Below are a few common frauds affecting young adults:

Phishing

Traditional phishing emails and text messages are designed to trick the victim into thinking they are dealing with a reputable company (i.e. financial institution, service provider, government). Phishing messages will direct you to click a link for various reason, such as, updating your account information, unlocking your account, or accepting a refund. The goal is to capture personal and/or financial information, which can be used for identity fraud.

Warning Signs - How to Protect Yourself

- Do not open or click the link in unsolicited emails or text messages.
- Look for spelling and formatting errors.
- Verify the hyperlink behind the link's text or button by hovering over the text.
- Do not click on any suspicious attachments as they can contain malware.

Job

Fraudsters use popular job listing websites to recruit potential victims. The most common fraudulent job advertisements are for: Personal Assistant or Mystery Shopper, Financial Agent or Debt Collector, and Car Wrapping. In many cases, the fraudsters will impersonate legitimate companies.

Personal Assistant or Mystery Shopper: The victim receives a fake payment (unknowingly) with instructions to complete local purchases and send funds through a financial institution or a money service business. Victims are asked to document their experiences and evaluate customer service. Eventually, the payment is flagged as fraudulent and the victim is responsible for the money spent and sent to a third party.

Financial Agent, Administrative Assistant or Debt Collector: Consumers are offered a job that features a financial receiver/agent component. Victims are told to accept payments into their personal bank account, keep a portion, and forward the remaining amount to third parties. Victims are eventually informed that the original payment was fraudulent and any debts accrued are the responsibility of the victim. Fraudsters will attempt to process many payments in a short amount of time before the victim's financial institution recognizes the fraud.

Car Wrapping: Consumers receive an unsolicited text message promoting an opportunity for them to earn $300-$500 per week by wrapping their vehicle with advertisement. Interested victims are sent a fraudulent payment (unknowingly) with instructions to deposit and forward a portion of the funds to the graphics company. With time, the payment is flagged as fraudulent and the victim is responsible for the funds sent to a third party.

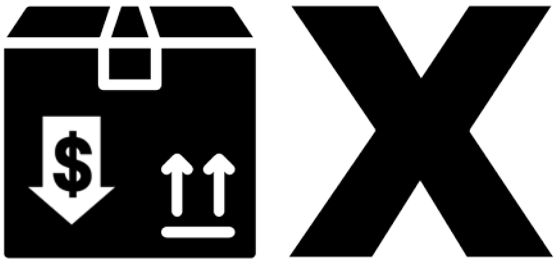
Warning Signs - How to Protect Yourself

- Be mindful of where you post your resume.
- Beware of unsolicited text messages offering employment.
- Most employers will not use a free web-based email address to conduct business.
- That the time to research a potential employer.
- Never use your personal bank account to accept payments from strangers.
- A legitimate employer will never send you money and ask you to forward or return a portion of it.

Merchandise

Fraudsters may place advertisements on popular classified sites or social networks. They may also easily create websites that share the look and feel of legitimate manufacturers. Fraudsters will generate traffic to their products by advertising them at deep discounts. Consumers may receive counterfeit products, lesser valued & unrelated goods, or nothing at all.

Warning Signs/ How to Protect Yourself



- If it sounds too good to be true, it probably is.
- Beware of pop-ups that direct you away from the current website.
- Consumers should verify the URL and seller contact information.
- Search for any warnings posted online and read reviews before making a purchase.
- Spelling mistakes and grammatical errors are other indicators of a potentially fraudulent website.
- Use a credit card when shopping online. Consumers are offered fraud protection and may receive a refund. If you have received anything other than the product you ordered, contact your credit card company to dispute the charge.

Rental Scam

Fraudsters will use online classified websites and social media networks to post advertisements for rentals. The property is usually located in a desirable area with a below average price. Interested consumers are asked to complete an application with their personal information.

Often, the supposed landlord claims to be out of the country and is in a hurry to rent the property to the right person. Victims are asked to place a deposit to secure a viewing or to receive the keys. Funds are often sent electronically or through money service businesses. Unfortunately for the victim, the property is not for rent and may not exist at all. Fraudulent listings are often created from listings for properties that are for sale or have recently sold.

Warning Signs/ How to Protect Yourself

- Research local market property values.
- Verify the property's address on an interactive map and search for duplicate posts.
- Whenever possible, physically visit the property.
- Request a lease agreement and review it thoroughly.
- Do not send money to strangers.

Sale of Merchandise

Consumers offering service or selling merchandise are at risk of receiving fraudulent payments. In most cases, victims will receive an overpayment with instructions to forward the difference to a third party (i.e. shipping company) to complete the transaction. Victims that comply are subsequently left without their merchandise or payment.

Warning Signs - How to Protect Yourself

- Fraudsters will often use the word "item" instead of what is being sold.
- Beware of buyers that try to change the shipping address at the last minute.
- Authenticate payments before shipping the goods.
- Never send payments to a third party.


Canadian Anti-Fraud Centre
C A F C
Centre antifraude du Canada
FRAUD: RECOGNIZE IT. REPORT IT. STOP IT.
LA FRAUDE : IDENTIFIEZ-LA. SIGNALEZ-LA. ENRAYEZ-LA.
Competition Bureau Canada
Bureau de la concurrence Canada
Royal Canadian Mounted Police
Gendarmerie royale du Canada
Canada