CITY OF LANGLEY

CRIME PREVENTION TASK GROUP

THURSDAY, MARCH 25, 2021 AT 6:00 p.m.

Via Video Conference

A G E N D A

1) AGENDA

Adoption of the March 25, 2021 agenda.

2) MINUTES

a) Adoption of the minutes of the Crime Prevention Task Group meeting held February 25, 2021.

3) DISCUSSION

a) Presentation from Wei Liu, Analyst, RCMP
   i. Analytical highlight of the Call for Service Data Spreadsheet

b) Incentivize Businesses to Target Harden
   i. Report back if a reduction in property tax can be used to incentivize target hardening;
   Dave Selvage, Manager of Community Safety

   ii. RCMP incentives to promote implementation of CPTED principles.
   S/Sgt. Brown, RCMP

4) UPDATES

a) Block Watch Program – How does the RCMP connect with new residents.
S/Sgt. Brown, RCMP

b) RCMP February Property Crime Map

Langley City
THE PLACE TO BE

5) STANDING ITEM

a) Crime Prevention (seniors) Outreach Project

i. Flyer Content Review / Approval
   - COVID-19 Fraud Alert (submitted by Khesro) – for mid-May release

ii. Ideas for Outreach Flyer Topics
   - Online Reporting
   - Educate Property Managers and Strata Councils about how to reduce mail theft
   - Green Dot Program (partner with Langley Division of Family Practice)

iii. Identify a volunteer to hand deliver Crime Prevention Tips for Business flyer (a monthly standing item when the first flyer is ready for distribution)

Tracking list of ideas for target hardening:

- Install a security system with surveillance cameras on the inside/outside of your business building
- Install an alarm system that is monitored off-site.
- Make sure that the outside of the business building is well lit at night.
- Keep front doors and windows clear of posters or signs for improved two-way visibility.
- To prevent vandalism keep the building clear.
- Use deadbolts for the exterior doors.
- Designate restricted areas with signs like "Employees Only" or "Private".
- Low counter displays allow employees to see over them.
- Keep side doors and back doors closed
- Keep limited cash in your registers. A sign indicating that there isn't much cash in the building might help.
- Be alert for customers who enter without a clear purpose.
- If cyber security is necessary, protect your customers online.
- Running security checks on staff and on potential new employees is an accepted practice.

b) 2020 “Know Your Neighbour” Campaign – deferred to 2021

6) FOR INFORMATION

a) GRIP Program – RCMP anti-gang education program – S/Sgt Brown

b) CPTED Video Link Information Sheet – S/Sgt Brown

c) Fraud Prevention Awareness / Information

7) ROUND TABLE

ADJOURNMENT

2021 MEETING DATES
Apr 29, May 27, Jun 24, Jul 29, Sep 30, Oct 28, Nov 25

Please notify Paula Kusack at pkusack@langleycity.ca if you are unable to attend the meeting.

CITY OF LANGLEY

MINUTES OF THE CRIME PREVENTION TASK GROUP

HELD REMOTELY VIA VIDEO CONFERENCE

THURSDAY, FEBRUARY 25, 2021
AT 6:03 P.M.

Present:	Councillor Nathan Pachal, Chair Valerie Frolander, Member at Large Jenny Hinch, Chamber of Commerce Mary Kydd, Senior Representative Khesro Amin, Member at Large Nadia Gugubauer, Member at Large Allen Yuarata, Member at Large Deborah MacLellan, Member at Large
Staff:	Paula Kusack, Deputy Corporate Officer Dave Selvage, Community Safety Manager S/Sgt. Dave Brown, RCMP
Absent:	Heather Giuriato, DLBA Lida Magnus, Youth Member

---

1) AGENDA

It was MOVED and SECONDED

THAT the February 25, 2021 agenda be adopted as circulated.

CARRIED

2) MINUTES

It was MOVED and SECONDED

THAT the January 28, 2020 minutes of the Crime Prevention Task Group meeting be adopted as circulated.

CARRIED

Due to technical difficulties with the zoom connection the group consensus was to proceed through the agenda out of order to allow time for staff to fix the connection issue.

3) DISCUSSION

d) CPTED Videos – Marketing Status

The Community Safety Manager advised that the link to the CPTED videos has been updated and has a permanent location on the City's website. Information sheets with the link to the videos have been printed and will be delivered by RCMP members as they make visits to businesses, starting with those on the Fraser Highway one-way section. The RCMP have reported that so far, the information has been well received.

b) Crime Prevention Tips for Business Outreach Flyer Content Ideas

ii. Discuss content ideas for a one-page flyer related to business crime prevention.

The chair advised that Ms. Gugubauer submitted the following ideas for content consideration:

- Install a security system with surveillance cameras on the outside and maybe on the inside of your business building
- Install an alarm system that is monitored off-site.
- Make sure that the outside of the business building is well lit at night.
- If possible keep front doors and windows clear of posters or signs for improved two-way visibility.
- To prevent vandalism keep the building clear.
- Use deadbolts for the exterior doors.
- Designate restricted areas with signs like "Employees Only" or "Private".
- Low counter displays allow employees to see over them.
- Keep side doors and back doors closed
- Keep limited cash in your registers. A sign indicating that there isn't much cash in the building might help.
- Be alert for customers who enter without a clear purpose.
- If cyber security is necessary, protect your customers online.
- Running security checks on staff and on potential new employees is an accepted practice.

Ms. Hinch suggested creating a one-page flyer for each of the CPTED video content topics. Break down the subject matter into key concepts and put them on the flyer and include a link to the video series online. Send out one per month.

ACTION: Ms. Hinch, Ms. Gugubauer and Ms. Giuriato will summarize the CPTED video content into text and create a one-page flyer for each video. Once ready, they will send them to the Deputy Corporate Officer for inclusion on a future CPTG agenda for review by the group and subsequent distribution.

It was noted that studies suggest that people need to hear things seven times before it sinks in. Therefore, it is effective to promote key messages several times in different ways to get the message to stick.

Discussion continued about the following:

- Ways to incentivize business owners to implement some of the CPTED suggestions
- Collaborate with local businesses to provide incentives to target harden
- Consider property tax reduction when improvements are installed, if possible
- Find out what incentive offers are already in the marketplace and highlight them to business owners/operators (ie: installing security cameras gets owners a reduction on home insurance)
- Promote crime stats and prevention in high problem areas
- Do statistics indicate if the B & E locations have security systems in place

ACTION: City staff will inquire with the Finance department to see if it is possible to use property tax incentives to encourage businesses to enhance security.

ACTION: Are there ways the RCMP can incentivize the public to implement CPTED principles to reduce crime? S/Sgt Brown will inquire and report back.

iii. Discuss ideas about how we can distribute the Crime Prevention Tips for Business flyer.

Ms. Hinch offered to distribute/post the flyers on the Chamber of Commerce website and social media outlets. She was confident that Ms. Giuriato would do the same on the Downtown Langley Business Association outlets as well.

ACTION: Ms. Gugubauer volunteered to hand deliver flyers to local businesses as they are released.

ACTION: Staff to add a standing item to the agenda related to identifying a volunteer to hand deliver the Crime Prevention Tips for Business flyer each month.

It was noted that the DLBA ambassadors may be able to deliver the flyers as well.

S/Sgt Brown suggested that the Community Police Office liaison officer can also hand out flyers as the RCMP are looking for opportunities to connect and build a rapport with local business owners.

ACTION: When the Crime Prevention Tips for Business flyer is ready for distribution the Deputy Corporate Officer will forward copies to S/Sgt Brown and he will provide them to the Community Police Office for distribution.

ACTION: S/Sgt Brown will forward a copy of the CPTED video link information sheet to the Deputy Corporate Officer to share with the group.

i. S/Sgt Brown to provide crime statistics/Calls for Service for the business areas north of 54 Avenue.

This item was captured in item 3a) i.

a) Calls for Service Data

i. S/Sgt Brown will review Calls for Service data to help determine high call areas, types of calls etc. to assist with determining target areas to share information and educate the public.

S/Sgt Brown reviewed the data sheet which offered detailed information about the types of calls for service. Data can be analyzed by location, type of call etc.

The Chair noted that if the data provided can be filtered it would be very useful in targeting specific crime prevention campaign ideas in specific areas, maximizing value and effectiveness.

ACTION: S/Sgt Brown advised that the analyst that created the spreadsheet could attend the next meeting and explain how to filter out the desired information.

c) Crime Prevention Education Among Youth

S/Sgt Brown provided an information update related to what the RCMP are currently doing to educate youth in general, and relation to gang violence. The current gang conflict involves three different groups and this level of activity is unprecedented in the Lower Mainland. In response, many specialized RCMP teams are working together and he is encouraged by what is happening on the enforcement front.

On the education side he advised that officers are identifying at-risk, vulnerable youth through school counsellors and administrators and are providing specific support to them. They have learned that doing group intervention is not very effective as the kids that come to assemblies of that nature are not the kids most at risk. Providing at-risk kids with direct support is more effective.

ACTION: S/Sgt Brown will forward an email with more details about the GRIP program for information.

4) UPDATES

a) RCMP January Property Crime Map

A brief review of the crime map was provided and discussion ensued about how to connect new people in redeveloped areas to the Block Watch program. S/Sgt Brown advised that door to door is the best way to engage new residents in the Block Watch program. He will brainstorm with his staff to try to think of other effective ways.

Ms. Kydd noted that strata councils can request a presentation from Florence, the Block Watch Coordinator at the main RCMP detachment. Perhaps property management companies can be engaged as well.

ACTION: S/Sgt Brown will report back if the RCMP reaches out to new residents about the Block Watch program.

Mr. Amin noted that he has seen posters from the CPO office in many local buildings that has information about crime prevention. He felt like the RCMP are actively reaching out to the community.

5) STANDING ITEM

a) Seniors Outreach Project

i. Flyer Content Review /Approval
- Phone Fraud – for early April release

The group consensus was that the content for the phone fraud flyer was well done. It was noted that the Canadian Anti-Fraud website has a lot of valuable information.

ii. Community Feedback Information

The Chair noted that the City has been receiving great feedback about the flyers from the public and distribution partners. He has seen the flyers in business windows around town as well. He thanked Ms. Kydd for delivering 40 flyers door to door around the downtown core.
This small gesture is having a big impact in our community and is meaningful to our community members.

iii. Ideas for Flyer Topics
- Online Reporting
- COVID-19 Fraud Alert
- Educate Property Managers and Strata Councils about how to reduce mail theft

- Green Dot Program (partner with Langley Division of Family Practice)

Ms. Hinch noted that the Canadian Anti-Fraud website has a lot of good information related to COVID-19 fraud, fake vaccines, how fraudsters are using COVID to take advantage of seniors.
The group agreed that the next flyer should be related to COVID-19 fraud and there was a suggestion to include the Canadian Anti-Fraud website link again.

Mr. Amin volunteered to create content for the next flyer related to COVID-19 fraud. It is scheduled for mid-May distribution.

b) 2020 “Know Your Neighbour” Campaign – deferred to 2021

6) ROUND TABLE

There was discussion about door to door canvassers and how to tell if they are legitimate. S/Sgt Brown reminded members that if someone comes to their door and seems suspicious, call the RCMP. They will do patrols and locate them. He asked that members share the message with their contacts that the RCMP want you to call if there is any suspicious activity in your area.

Discussion about the reasons for increased mail theft, which leads to identity theft.

Ms. Hinch advised that she will be opening a retail storefront location for her business, Lucid Water, on Fraser Highway in Aldergrove. She welcomed members to stop by and say hi if they are in the area.

S/Sgt Brown advised that officers from the CPO office will be visiting locations that have been victims of break & enter to discuss target hardening. He will report back on how those visits are going and if there has been any uptake in the CPTED, target hardening process.

MOVED AND SECONDED

THAT the meeting adjourn at 7:30pm.

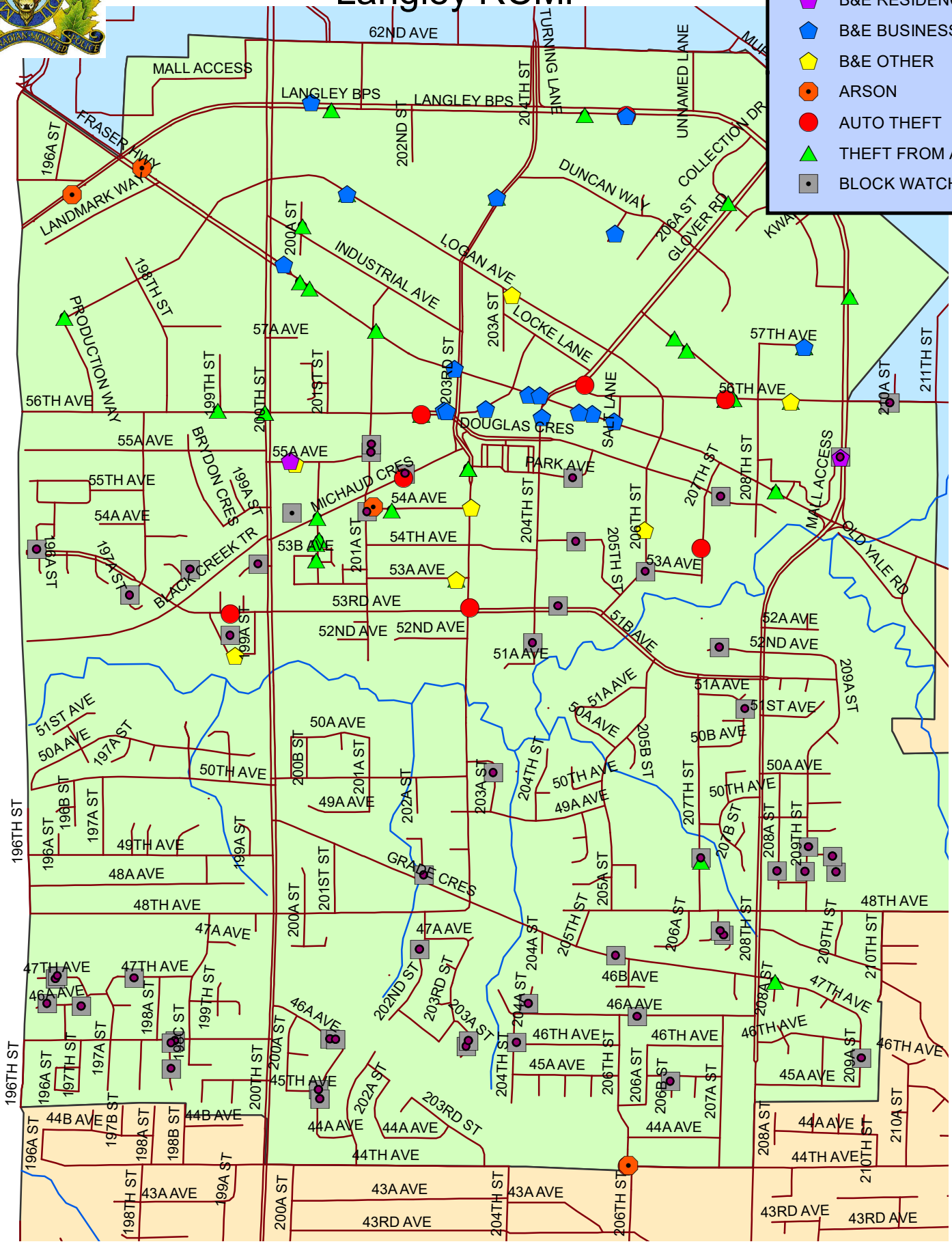
CARRIED

_____
CHAIR

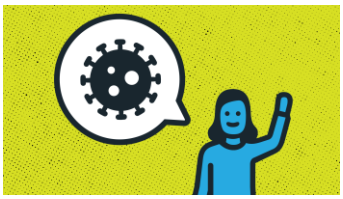
Certified Correct:
pdk

_____
DEPUTY CORPORATE OFFICER

Langley City Property Crime
2021-Feb-01 to 2021-Feb-28
Langley RCMP



COVID 19 Fraud Alert



The COVID-19 pandemic continues to provide scammers with opportunities to take advantage of Canadians.

Do not buy COVID-19 vaccines online or from unauthorized sources. The only way to access safe and effective COVID-19 vaccines is through clinics organized or endorsed by your local public health authority. If you have questions about getting vaccinated, contact your family physician or local health care providers.

Protect yourself, beware of:

An email containing links or content related to COVID-19 vaccines and once you click on them it freezes your computer, makes you call a toll-free number and then they demand money from you to unfreeze your account

Coronavirus-themed emails or text messages and COVID-19 vaccination themed emails or text messages that are trying to:

  - trick you into installing malicious COVID-19 notification apps
  - trick you into opening malicious attachments

- Unsolicited calls claiming to be from a private company or health care providers offering home vaccination kits for an up-front fee
- Phone calls offering home vaccination kits
  - A phone call from someone claiming to work for a pharmaceutical company and offering a "6 shot vaccine system" which you receive by mail after paying large sums of money
- Fraudulent Cleaning or heating companies
  - offering duct cleaning services or air filters to protect from COVID-19
- Door-to-door salespeople
  - selling household decontamination services
- Private companies
  - offering fast COVID-19 tests for sale & selling fraudulent products that claim to treat or prevent the disease

Trusted resources and advice

If you didn't initiate contact, you don't know who you're communicating to

Never respond or click on suspicious links and attachments

If you have been a victim of fraud, **report it to the Canadian Anti-Fraud Centre at 1-888-495-8501**. Don’t be afraid to come forward. You are not alone. We are here to help you.

Paula Kusack

Subject: FW: Crime Prevention meeting with the City

From: Craig VANHERK <craig.vanherk@rcmp-grc.gc.ca>
Sent: February 9, 2021 5:22 PM
To: Brown, David <david.r.brown@rcmp-grc.gc.ca>
Cc: Don Davidson <000043818.RICHMOND.EDIV_LMD@rcmp-grc.gc.ca>
Subject: Re: Crime Prevention meeting with the City

Hi Dave,

Hopefully the following will provide some background and information on our (Youth Unit) involvement with gang awareness activity/education, the local School District's activity/involvement and what is currently available to us, our local schools and to the public. We have some good things in place also have areas to improve upon. For example, we have yet to tap into our local analysts for potential early or ongoing indicators and some of the existing training could be updated.

A couple years ago, after several gang related incidents within and in close proximity to the community, the BC Education Minister designated Langley School District (SD35) as one of a handful of districts in the province that were required to have a gang reduction strategy in place. Gang Reduction through Informed Practice (GRIP) is a strategy that has been implemented by Safer Schools Together (SST) in partnership with the B.C. Ministry of Education. Safer Schools together is the same group that delivers our Digital Threat Assessment training and support, the Violence Threat Risk assessment training as well as the provinces anonymous online bullying reporting tool. The GRIP strategy is "comprehensive training designed to deliver proven prevention and intervention strategies to communities throughout B.C. in response to youth gangs" *(Safer School Together and Govt B.C. website)*

Administrators and Counsellors within SD35 have received training in the GRIP approach, particularly in seeking out early identification of youth that are 'at risk' by the behaviours they are exhibiting or by their life circumstances. The primary focus of the strategy is early identification. Once identified, the school based team develops a response specific to the youth and the situation. These student(s) are sent to a three day program consisting of assessments, interviews and education hosted at Vanguard Secondary by GRIP trained staff. SD35's GRIP team attends regular meetings with other districts and is responsible for ongoing training and support within SD35. SST GRIP also run a program known as "Game Ready" where SLO's and schools can refer the same at risk youth to. The program grew from the Surrey Wrap Around program and pairs the at risk youth with an ex/retired professional athlete mentor.

The SD35 GRIP team is currently working closely with SST on an updated early identification program and a more intentional District wide program to identify and combat students engaging in or susceptible to gang activities. This is expected to be in place around the upcoming March break.

AT Langley Detachment, each of the SLO's is assigned a 'family' of schools (High school and schools that feed up to it) and they communicate with the admin and staff at their assigned schools on a regular basis. The SLO team assists in conversations, relationship building and focused education/interventions at the school level. As situations and/or student(s) arise displaying at risk behaviours, the team focuses on a specific intervention, tailored for that student or group of students. At times, this is a one on one conversation with the SLO or at other times we bring in a SST GRIP resource, CFSEU or SGET member to speak with them. If it is a class or

group we will utilize recourses like CFSEU "End Gang Life" or SGET or SST GRIP to come in and present. All three of these groups bring an 'ex' gang member to provide further perspective and information.

In all reality it is conceivable, even likely, that a large portion of students will not have been part of a formal larger group assembly on gang intervention/prevention. They will have been a part of smaller discussions or less formal information sharing strategies. Like most of our school talks on specific topics (gangs, drugs, drinking/driving), we have found it far more effective to speak strategically with smaller groups based on the needs of the school/group. In the past we would have simply held a school wide assembly however these have been shown to have little impact on most students as they don't deal with or connect with the topic.

Currently CFSEU End Gang Life/SGET are not doing any in person presentations do to COVID. They are updating their online resources bot for police and also some on the public side. If a member of the public, a parent or youth, did wish resources for themselves or for a 'friend' the following are great resources:

https://saferschoolstogether.com

https://www.cfseu.bc.ca/end-gang-life/

Cpl. Craig van Herk
NCO i/c Youth Unit
Langley RCMP / Government of Canada
craig.vanherk@rcmp-grc.gc.ca Tel: 604 532-3209
Cell: **778 987-4931**
Fax: 604 532-3365

RCMP·GRC

ROYAL CANADIAN MOUNTED POLICE • GENDARMERIE ROYALE DU CANADA

Crime Prevention Through Environmental Design (CPTED)

The following link contains a power point presentation that you and your staff can view in part or whole that covers the key topics of CPTED;

1. Natural Access Control
2. Natural Surveillance
3. Territoriality and Defensible Space
4. Target Hardening
5. Maintenance and Management

Each topic will give you and your team an overview of how we can work together towards decreasing criminality and ensuring all the users of your space feel increasingly safe. Please click on this link or enter into your web browser to view the https://langleycity.ca/city-services/public-safety/langley-rcmp

Important contact numbers and information

Langley RCMP-GRC

- 911- The crime is happening in the moment
- 604-532-3200
- Online reporting https://ocre-sielc.rcmp-grc.gc.ca/langley/en

City of Langley Bylaws

- https://city.langley.bc.ca/cityhall/bylaws-policies/bylaw-enforcement
- 604-514-2819

Downtown Langley Business Association

- https://www.downtownlangley.com
- 604-539-0133

Lookout Housing-Needle and Drug Paraphernalia pick up

- 604-812-5277

Every business, location, and set up is unique therefore the Langley RCMP presentation will provide different recommendations that you could implement in and around your business. The common goal is to reduce the opportunities for crime and victimization while increasing the legitimate use of your business.

Sincerely,

Mike BHATTI, Insp.
A. OIC
Langley RCMP Detachment

2024/02/10.

Paula Kusack

From: Brown, David <david.r.brown@rcmp-grc.gc.ca>
Sent: March 19, 2021 11:11 PM
To: Paula Kusack
Subject: FW: Everyone_Must Know_Fraud Material
Attachments: 2021.03.08 - Financial Scams.pdf; Show Me The Fraud.pdf; Young Adults.pdf; Middle Agers.pdf; Seniors.pdf; Businesses.pdf; CAFC Resource Materials Request Form.doc; 2021.03.15 - Protecting Your Information.pdf

Here is some helpful fraud prevention information/awareness for our groups information and action where needed. Thanks,

Dave

From: Kiehlbauch, Desmond <desmond.kiehlbauch@rcmp-grc.gc.ca>
Sent: March 16, 2021 12:56 PM
To: Everyone_Ediv_Langley <Everyone_Ediv_Langley@rcmp-grc.gc.ca>
Subject: Everyone_Must Know_Fraud Material

Hello,

As some of you may be aware, March is the Canadian Anti-Fraud Centre's (CAFC) Fraud Prevention month. I have attaced some documents that relate to prevention and some of the scams that are out there. These documents can be released to the public and the CAFC is an excellent resource for investigators and victims of fraud. There is also a resource request form should anyone want material related to fraud prevention.

Regards,

Sgt. D. Kiehlbauch
Strike Force
Langley RCMP
Desk: 604-532-3374
Cell: 604-362-6502

CANADIAN ANTI-FRAUD CENTRE BULLETIN

2021 Fraud Prevention Toolkit 2021-02-15

FRAUD: RECOGNIZE, REJECT, REPORT

SHOW ME THE FRAUD

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 this toolkit to reduce fraud through public awareness and education. We encourage everyone 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.

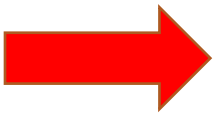
Thank you,

Your CAFC Fraud Prevention Team

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

This Toolkit Includes:

1) **CAFC Logo**



2) **Graphics Library**
https://www.facebook.com/pg/canantifraud/photos/?tab=album&album_id=2840141142692133

3) **Video Library**
https://www.youtube.com/channel/UCnvTfqttCb4K6wyVC6rMJkw/playlists

4) **The Little Black Book of Scams, 2nd edition**
The Competition Bureau will continue promoting *The Little Black Book of Scams, 2nd edition,* an online resource about 12 common frauds with tips to recognize, reject and report them. *The Little Black Book of Scams* is available in English, French, Mandarin, Cantonese, Punjabi, Tagalog, Arabic, and Spanish. Further resources are available on the Competition Bureau's website, including a quiz to test Canadians' knowledge of the common frauds.

5) **Presentation**
CAFC PowerPoint presentations are available by request to partners@antifraudcentre.ca.

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, 67,294 of the reports were from Canadian consumers and businesses, that reported losses totalling more than $104.2 million.

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

Fraud Type	Reports	Victims	Dollar Loss
Extortion	17,390	6,689	$12.5 M
Identity Fraud	16,970	16,970	N/A
Personal Info	6,649	4,386	N/A
Phishing	3,672	1,167	N/A
Merchandise	3,354	2,728	$8.7 M
Vendor Fraud	2,320	1,478	$4.2 M
Job	2,297	1,035	$2.5 M
Service	2,009	1,241	$8.5 M
Spear Phishing	1,049	525	$14.4 M
Emergency	924	310	$1.0 M

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

Fraud Type	Reports	Victims	Dollar Loss
Romance	899	620	$18.5 M
Investments	501	428	$16.5 M
Spear Phishing	1,049	525	$14.4 M
Extortion	17,390	6,689	$12.5 M
Merchandise	3,354	2,728	$8.7 M
Service	2,009	1,241	$8.5 M
Vendor Fraud	2,320	1,478	$4.2 M
Prize	754	240	$3.5 M
Bank Investigator	835	340	$3.0 M
Job	2,297	1,035	$2.6 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) Key Messaging and Slogans

A) Fraud: Recognize, Reject, Report.

Many frauds today are designed to play on a potential victim's emotions and get them to respond without thinking. They attempt to illicit responses based on panic, fear, desperation, elation, love which are often escalated by presenting urgent situations requiring immediate action. The slogan for fraud prevention is geared

toward getting citizens in Canada to slow down and not react to potential fraud solicitations. We encourage people to **recognize** that fraudsters are using every means at their disposal to target them; telephone, email, text messaging, social media, internet and mail. We ask that they change how they react to the unsolicited offers or demands.

Rejecting fraud involves protecting your personal information and money. Routine practices to develop include checking credit profiles, monitoring accounts for unauthorized activities, updating operating systems and antivirus software, and not doing business over the phone. We want people to slow down, to think about and assess the situation before reacting. This can involve saying no, doing due diligence, researching and confirming information, and talking to family members and friends. We want to encourage people to take their time, and to scrutinize all offers and demands.

Reporting fraud means speaking up, even when no money was lost. Like other crimes, if fraud is not reported, we don't know what is happening and can't warn other people. The information from one fraud occurrence (a bank account, email address, virtual currency address, telephone number, etc) can be investigated and is useful in linking other occurrences. Moreover, reporting provides other opportunities for disruption. By reporting the information to the banks, money service businesses, email providers, telephone companies, dating websites, social media networks; steps can be taking to block or remove these fraudulent accounts and their content.

- Fraud Prevention Checklist: A few questions to ask yourself every time you are contacted for personal information. If any of the following apply, do not provide your information and seek advice.
    - Is the call unsolicited? Was it expected or out of the blue?
    - Are they asking you to confirm personal information such as your name, address, or account details?
    - Are they looking for a fast or instant response?
    - Are they asking you for money?
    - Is the caller avoiding using the actual name or the company or financial institution?
    - Are they offering you a prize, free gift, or trial?
    - Are they claiming to be the police or investigating something?
    - Does the email have an odd email address?

- Is the formatting strange or are there spelling mistakes?
- Are you being asked to change your password despite not sending a request to do so?

B) Fraud in 3D – Detect, Denounce, Discourage

Developed by police services in Quebec in partnership with the Bank of Canada, Fraud in 3D is another slogan or campaign aimed at getting people to be vigilant to avoid the devastating effects of fraud. For more information, visit: https://www.sq.gouv.qc.ca/services/campagnes/mpf/. For the PDF booklet: https://www.bankofcanada.ca/wp-content/uploads/2020/02/fraud-3d.pdf

C) Take Five to Stop Fraud

Take Five is a national campaign, led by UK Finance and the UK Government, that offers straight-forward and impartial advice to help everyone protect themselves from preventable fraud. This includes email deception and phone-based scams as well as online fraud – particularly where fraudsters impersonate trusted organizations.

Take Five urges consumers to:

STOP: Taking a moment to pause and think before parting with your personal information or money could keep you safe.
CHALLENGE: Could it be fake? It is okay to reject, refuse or ignore requests. Only fraudsters will try to rush or panic you.
PROTECT: If you believe you are the victim of a fraud, contact your local police, the Canadian Anti-Fraud Centre and your financial institution immediately.

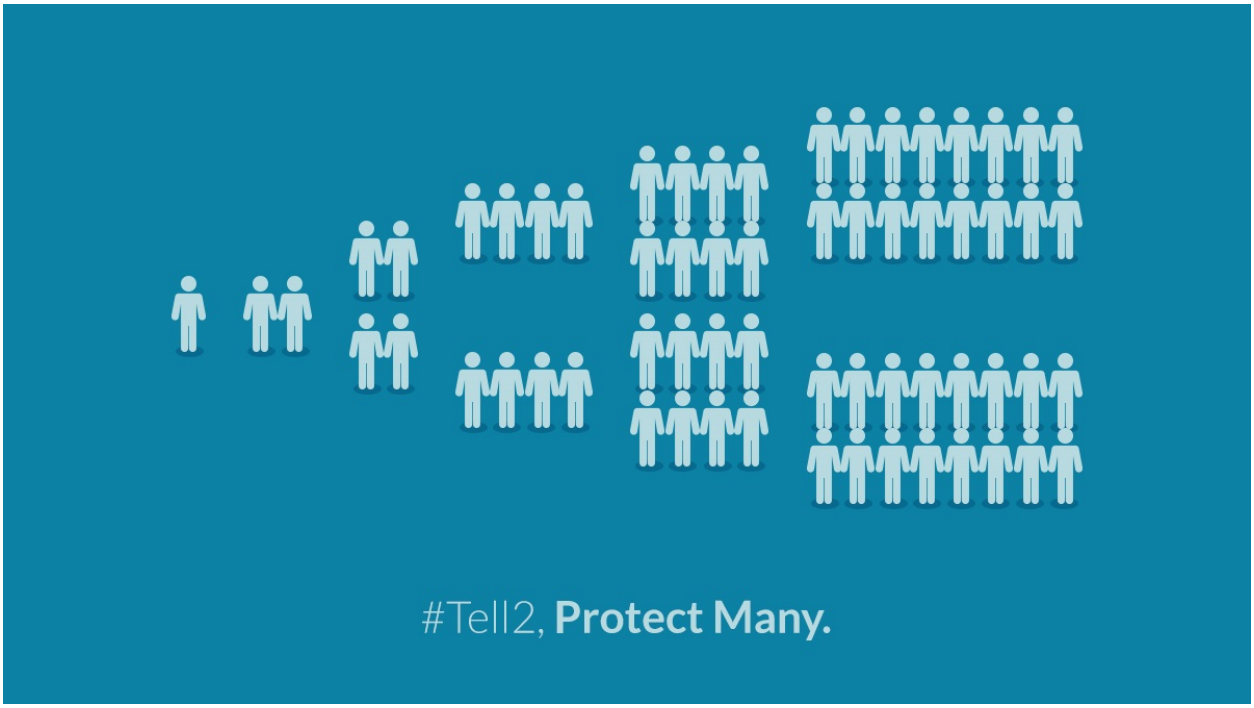
For more information on Take Five, visit: https://takefive-stopfraud.org.uk/

D) Tell Two

Developed by UK Detective Constable Tony Murray, the #Tell2 campaign started from a strong desire to protect consumers from fraud. He deconstructed fraud by using a problem solving approach and is attacking it from the consumer standpoint. His communication strategy engages others to spread the fraud prevention messaging that focuses on the 5 key routes (home phone, internet, mobile, mail,

door-to-door) fraudsters will take into consumer's lives. This strategy is working, has won awards and is gaining traction worldwide.

The primary goal behind this strategy is for consumers to share fraud prevention messaging with two people and ask them to do the same. An uninterrupted chain of 20 tell2'ers would reach over a million people. A chain of 25 tell2'ers would reach more than 33.5 million people; that is just short of reaching the entire population of Canada.



We encourage our partners to share the following messages with the tag **#Tell2, protect many**.

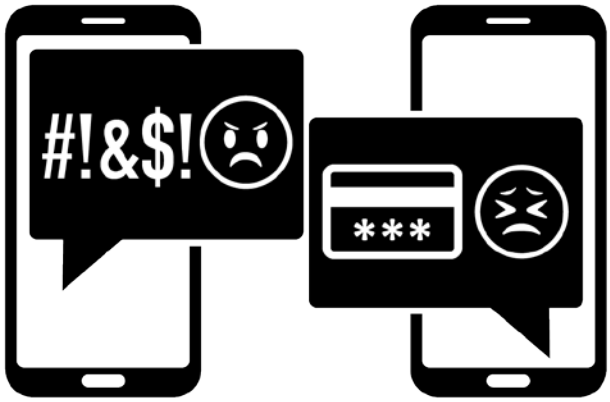
- Do you really know who's calling? Fraudsters lie and claim to be legitimate companies. They will also spoof the information on your call display to make the call seem reliable.
- The landline is a lifeline for some. For fraudsters, it is a direct line. Don't recognize the number? Don't answer. Not a friendly voice on the other end of the line? Hang up.
- Who is that email really from? Fraudsters lie and claim to be legitimate companies. Hover over an email address to see if it is hiding the real one underneath.

- Won a prize through the mail? You cannot win a contest or lottery you did not enter.
- Weren't expecting visitors? Don't answer the door.
- Don't assume everyone knows. Tell two offline to keep everyone safe.
- Tell two over a brew.

11) Common Frauds & How to Protect Yourself

Below are the most common frauds affecting Canadians:

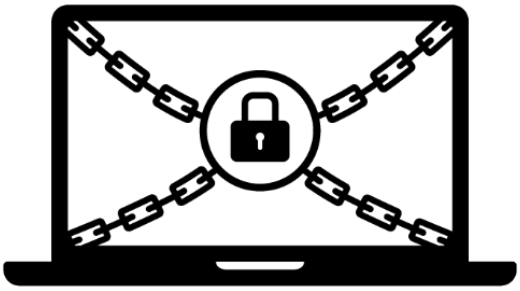
Extortion
Extortion happens when someone unlawfully obtains money, property or services from a person, entity or institution through coercion.



SIN Scam: Consumers are receiving recorded messages about their Social Insurance Number (SIN) being linked to fraudulent or criminal activity. The fraudsters are claiming to be different federal government agencies and stating that the SIN has been blocked, compromised or suspended. There may be threats of an arrest warrant or imprisonment, if the consumer does not cooperate with the fraudster's demands. They may request personal information (SIN, date of birth, address etc.) or request that consumers empty their bank accounts and deposit the funds elsewhere. The fraudsters claim to want to clear the money from illegal activity and that it will be returned once their investigation is complete.

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

- Fraudsters use call-spoofing to mislead consumers. This technology is easily available. Never assume that the phone numbers appearing on your call display are accurate.
- No government agency will contact you and tell you that your SIN is blocked or suspended, nor will they threaten you with legal action.
- Never provide personal information over the phone to an unknown caller.
- No government or law enforcement agency will demand an immediate payment or to submit all of your money for investigation.
- No government or law enforcement agency will request payment by Bitcoin, a money service business, or gift cards (ie. iTunes, Google Play, Steam).
- How to recognize government frauds: https://www.canada.ca/en/revenue-agency/corporate/security/protect-yourself-against-fraud.html
- 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.

Phishing & Smishing

Traditional phishing emails and smishing text messages are techniques designed to trick the victim into thinking they are dealing with a reputable company (i.e. financial institution, service provider, government). Phishing/Smishing 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.

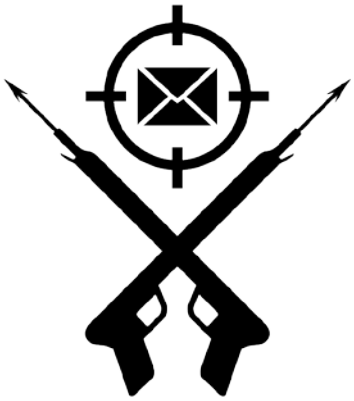
- Look for spelling and formatting errors.
- Verify the hyperlink behind the link's text or button by hovering over the text.
- Do not click on any suspicious links as they can contain malware.

Spear Phishing

Spear phishing is one of the most common and most dangerous attack methods currently used to conduct fraud, usually on businesses and organizations.

In preparation of a spear phishing attack, fraudsters take their time to collect information on their intended targets, so they can send convincing emails seemingly from a trusted source. Fraudsters will infiltrate or spoof a business email account. They create a rule to forward a copy of incoming emails to one of their own accounts. They comb through these emails to study the sender's use of language and look for patterns linked to important contacts, payments, and dates.

Fraudsters launch their attack when the owner of the email account cannot be easily contacted by email or by phone. If the fraudsters haven't infiltrated the executive's email account, they may set up a domain similar to the company's and use the executive's name on the account. The contact information they need is often found on the company's website or through social media.



Common Variations

- A top executive requests their Accounts Payable to make an urgent payment.
- A business receives a duplicate invoice with updated payment details supposedly from an existing supplier or contractor.
- An accountant or financial planner receives a large withdrawal request that looks like it's coming from their client's email.
- Payroll receives an email claiming to be from an employee looking to update their bank account information.
- Members of a church, synagogue, temple, or mosque receive a donation request by email claiming to be from their religious leader.
- An email that seems to come from a trusted source asks you to download an attachment, but the attachment is malware that infiltrates an entire network or infrastructure.

Warning Signs

- Unsolicited emails.
- Direct contact from a senior official you are not normally in contact with.
- Requests for absolute confidentiality.
- Pressure or a sense of urgency.
- Unusual requests that do not follow internal procedures.
- Threats or unusual promises of reward.

How to Protect Yourself

- Remain current on frauds targeting businesses and educate all employees. Include fraud training as part of new employee onboarding.
- Set detailed payment procedures. Encourage a verification step for unusual requests.
- Establish fraud identifying, managing and reporting procedures.
- Avoid opening unsolicited emails or clicking on suspicious links or attachments.
- Take time to hover over an email address or link and confirm that they are correct.
- Restrict the amount of information shared publicly and show caution with regards to social media.
- Upgrade and update technical security software.

Purchase of Merchandise

Fraudsters may place advertisements on popular classified sites or social networks. They may also 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. Additionally, businesses must do their due diligence before purchasing products or services from new and unknown suppliers.

Vehicle for Sale: Vehicles are advertised at a lower than average price. Fraudsters claim to be located overseas and a third-party agency will deliver the vehicle. The victim is asked to submit payments for the vehicle and delivery. Nothing is ever delivered.

Animal for Free: Fraudsters will often advertise animals for free; puppies and kittens are used most often. They will claim that the animal is free; however, the victim will be required to pay shipping. Once the payment is received, the fraudsters will begin to request additional payments for: transportation cage, vaccinations, medication, insurance, customs and brokerage fees, etc.

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.

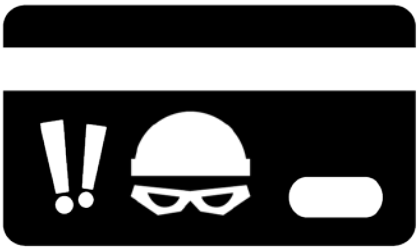
Warning Signs/ How to Protect Yourself

- 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.
- 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 any money before viewing the property and signing an agreement.
- Verify the URL and seller information's legitimacy.
- Educate your staff on the current frauds that affect businesses.
- Do not provide any information pertaining to the make and model of any office equipment to any organization other than your normal supplier.
- Review suspicious invoices as fraudsters will send false invoices for products or services that were never purchased.

Vendor Fraud

Consumers and businesses selling merchandise or offering their services online are at risk of receiving fraudulent payments. In many 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.



Card Not Present (CNP): CNP fraud can happen when a business accepts orders and payments over the phone, online or by email. Fraudsters use stolen credit cards to pay for the products or services. They will request express shipping, so that they can receive the order before the card owner discovers the unauthorized charge. When the actual card owner disputes the unauthorized charge, the business must issue a chargeback to the victim's stolen card.

Warning Signs

Customer Flags

- Orders made from one IP address, but using different names, addresses, and payments.
- Email addresses from free email service.
- Many card numbers provided for one order (cards keep getting declined).
- Purchaser name and cardholder name are different.

Product / Order Flags

- Larger than normal orders.
- Many orders for the same product; especially "big ticket" items.
- Orders from repeat customers that differ from their regular spending patterns.

- Orders using the same customer or payment information, but many IP addresses.

Delivery Flags

- Customer requests “rush” or “overnight” delivery.
- Single payment information used for many shipping addresses.
- Billing address different than shipping address.
- Request that extra funds be sent to a third party.

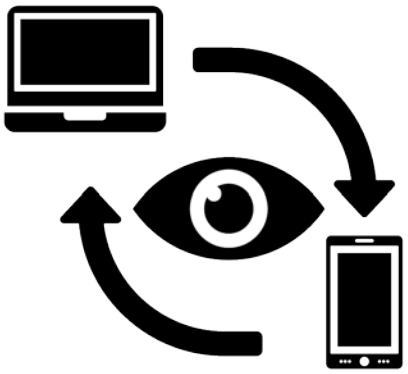
How to Protect Yourself

- Know the Red Flags and verify every order request received.
- Before shipping merchandise, verify the information provided by the customer (telephone number, email address, shipping address, etc.).
- Be aware of request for priority shipments for fraud-prone merchandise.
- Verify priority shipping requests when the shipping and billing addresses do not match.
- For suspicious orders, contact your payment processor. Verify the security measures to prevent victimization and reduce unwanted chargebacks.
- Never accept overpayments to forward funds to a third party.

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.

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 withdraw the funds in cash and to complete other transactions through a financial institution, money service business or bitcoin ATM. Victims are asked to document their experiences and evaluate customer service. Eventually, the fake payment is flagged as fraudulent and the victim is responsible for the money spent.

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.
- Take 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.

Investment

Any false, deceptive, misleading or fraudulent investment opportunity, often offering higher than normal or true monetary returns. Victims often lose most or all of their money. Investors run the added risk of having their identity stolen, accumulating losses for unauthorized withdrawals on their credit cards and incurring high interest payments on investments that do not exist.

Initial Coin Offerings: The virtual currency market is constantly changing. New virtual currencies are developed monthly. Like an Initial Public Offering (IPO), an Initial Coin Offering (ICO) is an attempt to raise funds to help a company launch a

new virtual currency. In an ICO fraud, the fraudsters solicit investment opportunities with fake ICOs. They provide official looking documentation, use buzz words and may even offer a real "token". In the end, everything is fake, and you lose your investment.

Pyramids: Similar to a Ponzi scheme, a pyramid scam focuses primarily on generating profits by recruiting other investors. A common pyramid scam today takes the form of a “gifting circle”. Participants gift a sum of money to join and ultimately must recruit others to make their money back. These schemes may offer products, but they usually have very little value.

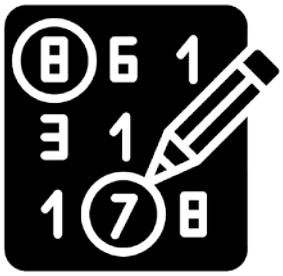
Pyramid selling is illegal in Canada. It’s a criminal offence to establish, operate, advertise or promote a scheme of pyramid selling.

Warning Signs – How to Protect Yourself

- Be careful when asked to provide personal or financial information to reclaim your investment profits.
- Beware of opportunities offering higher than normal returns.
- Beware of any urgency pressuring you to make an investment so that you don’t miss out.
- Prior to investing, ask for information on the investment. Research the team behind the offering and analyze the feasibility of the project. Check the registration and enforcement history.
- The Canadian Securities Administrators (CSA) encourages all investors to visit their National Registration Search Tool (www.aretheyregistered.ca).

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.
- Never send or accept money under any circumstances. You may, unknowingly, be participating in money laundering which is a criminal offence.

12) Identity Theft and Identity Fraud

A victim of identity fraud has previously been the victim of identity theft.

Identity theft occurs when a victim's personal information is stolen or compromised. This can happen as a result of volunteering personal or financial information, a phishing fraud, a stolen wallet, a database breach, etc.

Identity fraud occurs when the fraudster uses the victim's information for fraudulent activity. Fraudsters may create fake identity documents, submit unauthorized credit applications and open financial accounts in your name, re-route your mail, purchase mobile phones, takeover your existing financial and social accounts, etc.

If you are a victim of identity theft and/or fraud, you should immediately complete the following steps:

- **Step 1:** Gather the information pertaining to the fraud.
- **Step 2:** Contact the two major credit bureaus to obtain a copy of your credit report and review with reports.
    - **Equifax Canada:** http://www.consumer.equifax.ca/home/en_ca, 1-800-465-7166
    - **TransUnion Canada:** http://www.transunion.ca, 1-877-525-3823
- **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:** Review your financial statements and notify the affected agency if you notice any suspicious activity.
- **Step 6:** Notify your financial institutions and credit card companies, and change the passwords to your online accounts.
- **Step 7:** If you suspect that your mail has been redirected, notify Canada Post (www.canadapost.ca, 1-866-607-6301) and any service providers.
- **Step 8:** Notify federal identity document issuing agencies:
    - **Service Canada:** www.servicecanada.gc.ca, 1-800-622-6232
    - **Passport Canada:** www.passport.gc.ca, 1-800-567-6868
    - **Immigration, Refugees and Citizenship:** www.cic.gc.ca, 1-888-242-2100
- **Step 9:** Notify provincial identity document issuing agencies.

13) Cutting Contact with the Fraudsters

All fraudsters have their *tools of the trade*. In order for their fraud to be successful, they require a way to communicate with their potential victims as well as a system to receive payments from victims. To better prevent fraud from the very beginning, the top contact methods and best practices are described below.

Telephone Call

The telephone was invented to allow individuals to instantly communicate with each other, without having to be in the same room. In the last 150 years, the telephone has evolved to today's mobile device that fit in your pocket and allows you to call anyone across the globe. In 2020, telephone calls were the #1 contact method used by fraudsters and this is largely due to advancements in technology.

Automated dialing: An automatic dialer (or auto dialer) is a device or software that automatically dials telephone numbers. The phone numbers are usually provided from large lists. Once the call is answered, the auto dialer either plays a recorded message or connects the call to a live person. These systems can be used by legitimate or fraudulent call centres. Fraudsters may use lists of phone numbers

(gained legally or illegally) or they may setup the dialer to call all possible configurations of phone number in a given region.

Robocalls: A robocall is a phone call that uses an auto dialer to deliver a pre-recorded message. The recording message may use a computerize/robotic voice or that of a real person's. There are no anti-robocall laws in Canada; however, they are subject to Canadian Radio-television and Telecommunications Commission (CRTC) regulations. If you are registered on Canada's National Do Not Call list, this should filter out a large number of unsolicited calls. The National **Do Not Call List** (DNCL) gives consumers a choice about whether to receive telemarketing calls. Exemptions of who can still cold call you: Canadian registered charities, political parties, persons collecting information for a survey, newspapers for the purpose of soliciting subscriptions, and organizations with whom you have an existing business relationships. If the recorded message you hear does not fall under the exemptions, it is most likely fraudulent.

Spoofing: Your Caller ID or Call Display normally indicates the phone number and name associated to the line used to call you. There are a number of legitimate purposes for altering the information provided on Caller ID. Unfortunately, there are just as many illegitimate reasons for fraudsters to manipulate the information displayed. The most common misrepresentations to trick Canadians into answering calls are: using the same area code to make it appear that it is a local call, mirroring your own phone number, displaying the recognized number of a specific organization (ie. law enforcement or government agency), or showing a phone number that cannot be dialed.

Delayed Disconnect: (Only occurs on landlines.) When trying to legitimize their call, fraudsters will sometimes ask you to end your current call and immediately call the number on the back of your card or another phone number they provide you. When you complete the second call, you are almost instantly connected to the same person you were just speaking with. That is because the original call was never completely disconnected.

How to Protect Yourself from Telephone Fraud

- Register your phone number for free with Canada's National Do Not Call List at: https://lnnte-dncl.gc.ca/en.
- If you're not expecting a call or do not recognize the Caller ID, let the call go to your answering machine.

- Caller ID information can be spoofed. Do not trust the information to be genuine.
- If you answer the phone and it is a recorded message, hang up. Do not press 1 or call back.
- Whenever you're asked to make a secondary call. Wait a few minutes after ending the original call or call back from a different phone number.
- Never provide your personal or financial information over the phone if you did not initiate the call.
- You should never feel pressured to provide personal or financial information over the phone.
- Ask questions. If the caller cannot or will not answer, hang up.
- If you're still unsure about the call, talk to someone about it.

Email and Text Message

Consumers have become increasingly available to fraudsters by accepting emails and text messages on their mobile devices which they carry with them at all times. While telephone calls may still be the #1 contact method fraudsters use, consumers are victimized much more often from frauds initiated by emails and text messages.

Spoofing: Like Caller ID spoofing, fraudsters are also able to alter the sender's information in emails and text messages. They use spoofing tactics to display the name, phone number or email they want you to see. In emails, you should be able to hover over the sender's name to reveal the sender's real email address.

Automation: Automated or scheduled emails and text messages were designed to help businesses save time by quickly and simultaneously engaging with their contact list. Fraudsters use the same applications and services to instantaneously message their lists. They can choose who the messages go to, decide when to send them and even personalize them depending on the information they have previously collected. Fraudsters may also setup auto-responders to send delayed messages for when consumers reply back.

Email Compromise: When fraudsters gain access to email accounts, they can impersonate the victim to attempt fraud. With consumer accounts, fraudsters may send an email to the victim's entire contact list asking for money urgently due to

an emergency. With business accounts, fraudsters may setup an email forwarding rule to receive a copy of all incoming emails to their own email account. They will comb through the information and impersonate the business when the timing is right. The fraudsters may send a repeat invoice to clients asking them to submit their payment to an "updated" bank account. They may also impersonate an executive and request payments be made from staff members for various reasons. The success of these frauds depends on the fraudsters' ability to spoof the victim.

How to Protect Yourself from Email and Text Message Fraud

- Canada's anti-spam legislation (CASL) protects consumers and businesses from the misuse of digital technology, including spam and other electronic threats. Report spam at https://www.fightspam.gc.ca/eic/site/030.nsf/frm-eng/MMCN-9EZV6S.
- Beware of unsolicited emails and text messages. Delete them.
- Do not open messages that claim to be from businesses or organizations with which you do not have an existing relationship.
- Most businesses and organizations have personalized domains. Meanwhile, fraudsters will use readily available and free domains for their email addresses (ie. @outlook, @hotmail, @gmail, @yahoo, @me, etc).
- Take the time to analyze the sender's email address by hovering over the sender's name or visible email address. Sometimes, fraudsters will purchase domains that are very close to legitimate ones. It may be as simple as changing an "m" with "rn".
- If an email or text message includes a sense of urgency, this is a telltale sign of fraud.
- Review the message for spelling, grammatical errors, unusual language or branding that isn't quite right.
- Do not click any links or attachments if you are unsure of the sender's identity.
- If you clicked a link and it requests personal or financial information, do not proceed, close the page and run a thorough scan of your device.
- Financial institutions and government agencies will not request personal or financial information through email or text message.
- If the message seems to be coming from one of your contacts but something doesn't feel right or sounds too good to be true, contact them through a different communication method.

Online

The internet is a network of electronic devices that spans the globe. It is easy to connect and, once online, you can access almost any information or communicate with anyone else that is connected. It is the perfect workplace for fraudsters.

Search Engine Optimization: When looking for information, many consumers will use a popular search engine to find answers quickly. Fraudsters will often pay for their information or websites to be listed among the top results.

Pop-Ups: Pop-ups are used to grab your attention and are known to have a reputation as annoying distractions. A few variations exist: pop-overs will appear on top of your current page, pop-ups will redirect you to a new window or tab, and pop-unders will open a new window or tab, but will not redirect you from your current window. There are three ways you can trigger a pop-up: time-driven pop-ups are setup to appear after you have clicked something and the set timer in the background has elapsed, behavior driven pop-ups will appear after specific conditions have been met, and exit pop-ups will appear when you close the browser or visit a website different than the current one.

Online Classifieds: Many fraudsters will camouflage themselves amongst these popular bargain hunting grounds. They will create advertisements for items (e.g. animal, rentals, vehicles) and list them at a discount. Fraudsters may also contact consumers saying that they are interested in purchasing their *item* and offer an overpayment. In some cases, they may take over a victim's account or they may offer false employment for others to post advertisements for them.

Fake Websites: Creating a website can be quick and easy; yet, they may not be up for long if they are flagged to be fraudulent. Fraudsters create websites for a number of frauds. They are all built to offer a sense of trust and legitimacy behind the information they have provided. Fraudsters may purchase "https://" precursors to indicate that their website is secure when transferring information. They may also purchase domain names that are very close to legitimate brands; especially when they are claiming to be affiliated to a business or when they are looking to sell counterfeit merchandise.

Fake Information: Fraudsters will create accounts and websites using stolen logos, information and photos of people and/or merchandise.

Stolen credit cards: Fraudsters will place online orders using stolen credit cards for payment.

How to Protect Yourself Online

- Before connecting to the internet, be sure to have basic internet security enabled on your device.
- Do not access password-protected accounts or share personal and financial information when connected on public Wi-Fi.
- Enabling private or incognito browsing on your internet browser should disable browser history, search history, download history, cookies and temporary internet files.
- Disable cookies and delete your browsing history, whenever it is not required.
- Use a search engine that doesn't collect your personal information, doesn't store your search history and doesn't track you in or out of private browsing.
- Avoid selecting paid results after running an online search.
- Verify that the contact information you have found is legitimate by completing a secondary search on the information itself.
- No technology or security company will warn you of potential viruses or malware and ask you to contact them for the solution.
- The safest method to exit a pop-up is to do so in your Task Manager. For computers, hold down Ctrl+Alt+Del on your keyboard, select Task Manager, locate the appropriate Process, select and click End Task.
- If you are unable to exit the pop-up, proceed with a force shut down of your device.
- Regularly scan your devices for viruses or malware.
- Keep the software on your device updated.
- Meet in-person to thoroughly inspect a product before providing your payment.
- If a buy and sell website offers secured chat & payment options, use these to take advantage of any available protection programs. If you are asked to continue the conversation elsewhere or send a different payment method to avoid fees, proceed with caution.

- Be wary of unsolicited messages asking you to confirm your account details, password, and personal or financial information.
- Be aware of common classified frauds.
- Flag and report any fraudulent listings or messages to the website owner.
- If it sounds too good to be true, it probably is.
- When visiting a website, pay attention to the address bar.
- Websites that use "https://" do not guarantee that a website is not fraudulent, but it is something to look for.
- Use https://www.whois.net to find information about a domain's registration. Be wary of newer websites as counterfeit websites tend to only be active for a short amount of time.
- Look for poor grammar and spelling.
- Look for reliable contact information (ie. phone, email, physical address).
- Read reviews before making a purchase.
- Use a major credit card when shopping online as they provide the best fraud protection programs.
- Be wary of online orders that request express shipping with different mailing & shipping addresses.
- Never accept an overpayment with a request to transfer funds to a third party.

Social Networks

Social media was designed to allow users to create and share content, as well as participate in social networking. The 10 most popular websites or applications in Canada are: Facebook, YouTube, Instagram, Pinterest, Twitter, Snapchat, LinkedIn, Reddit, Twitch, and Tumblr. Even dating websites and application are included within this contact method.

Fake Accounts: Fraudsters will create their accounts typically using stolen photos and information from legitimate people. Most recently, Facebook announced that, between January and March 2019, it removed 2.19 billion fake accounts from their platform[1].

Social media bots: This type of bot uses fake accounts to automatically generate and amplify specific messaging, such as advertising and fake reviews (aka astro

[1] https://fbnewsroomus.files.wordpress.com/2019/05/cser-press-call-5.23.19.pdf

turfing). These may mostly be used to create convincing personas capable of influencing real people. Since bots are automated, they work 24/7.

Compromised Accounts: When fraudsters gain access to social media accounts, they also gain access to all of the information associated to the account. If they find compromising information or photos of the victim, they may blackmail them. Additionally, they will likely impersonate the victim to attempt fraud. Fraudsters may send messages to the victim's contact list informing them that they found their name on a winner's list or ask for money urgently due to an emergency. They may also use these accounts to publish their fake ads.

Advertisements: Fraudsters recognize that consumers spend a lot of time on social media and will post ads for free trials, discounted merchandise, or fake job opportunities. They may also use the names and photos of well-known individuals or companies to fake endorsements of their products.

How to Protect Yourself from Social Network Frauds

- Do not accept request from people you do not know. You do not know if they have malicious intent.
- Be wary of profiles that seem perfect in their photos.
- Complete a reverse image search to see where the same photo is being used online. https://images.google.com and https://tineye.com are great options.
- Ask specific questions and look for inconsistencies in the responses.
- Be wary of those who always have an excuse as to why you cannot meet in person.
- Never send money to someone you have never met.
- Beware of profiles that do not have many friends connected to it.
- If someone is harassing or threatening you, remove, block and report their account.
- Spot other fake accounts when: they have a high follower count but low engagement, the engagement rate is too fast, they have a large following but very few posts, they have maxed out their following count, or they only share spam content.
- Accounts that only push out information and do not engage in conversations likely have a bot behind them.
- Keep an eye out for wording or messages that seem unnatural.
- Do not click on suspicious links.

- Adjust your social account privacy settings from Public to a more restricted option.
- Do not overshare sensitive information (ie. personal, financial, when you're away, etc).
- Recognize that what you share online, will always be online.
- Do not provide your login details to anyone.
- Use a strong password or passphrase to protect your account.
- Remember to logout when you're done.
- Protect your account and your device by updating your software and applications regularly.

Mail & In-Person

Frauds initiated by mail or in-person may be the oldest ones in the book as these communication methods have existed for thousands of year.

Personalized Templates: While the surname in the greeting and some smaller details may change, fraudsters have been using template letters for a long time. A standard message informs the receiver that someone who shares their surname has passed and left millions in a bank account. If the sender and receiver work together, they can split the money. Another typical message states that the recipient is the winner of a large lottery or sweepstakes.

Stamps: Fraudsters have to get their letters delivered somehow. Every year, fake stamps cost Canada Post up to $10 million. Fraudsters may purchase rolls of legitimate stamps from Canada Post; yet, they will do so while using stolen credit cards.

Fraudulent Indicia: Fraudsters will also attempt to use a corporate postal indicium to have their mail delivered. These *paid* postal markings identify the service name and customer number.

Employees: Door-to-door fraudsters will often claim to be employees or students. They may wear a uniform and will often have an ID badge and clipboard.

High Pressure Sales: Fraudsters will often offer products and services that you do not need. They may advise you that, based on their inspection, your health is in immediate danger. They may claim that the majority of the quote they have

prepared for you can be refunded by a government grant program. When they arrive at their final price, they will tell you that the quote has been heavily discounted and that it is only available until they leave.

How to Protect Yourself from mail and in-person frauds

- You can reduce the amount of mailed marketing offers you receive by registering with the Canadian Marketing Association's Do Not Mail Service at: https://cmadnm.cawebhosting.ca/submit.asp. Your name will be kept on their list for six years.
- You cannot win a contest, lottery or sweepstakes you did not enter.
- You cannot enter a lottery from a different country without first buying a ticket within that country.
- Do not respond to offers of free trials, prizes or jobs that require advance payment.
- Any fees associated to winnings will never be requested in advance of receiving the funds. Instead, they will be removed from the total winnings.
- In Canada, the rules vary by province; yet, it is up to the executor of the will to notify beneficiaries.
- Legitimate estates do not look for trustees or heirs.
- Do not respond to requests looking for help to move large sums of money outside of another country.
- Discard any offers of a percentage from a supposed fortune in exchange for your financial information.
- Verify that a cheque you received is not counterfeit before depositing it into your bank account. If possible, contact the account owner listed on the cheque.
- In Alberta, unsolicited door-to-door sales of household energy products have been banned. In Ontario, unsolicited door-to-door sales have been banned. In many other provinces, door-to-door salespersons or direct sellers are required to have a permit or a licence to operate.
- Install a security camera near your doorway to deter criminals.
- Before you invite someone into your home or hear a sales pitch, ask for photo ID, the name of the person and the name and contact information for the business.
- If you ask a salesperson to leave, they must leave immediately. If you feel unsafe, call your local police.

- Do not rely on an individual's opinion that something in your home is unsafe or must be replaced. Get a second opinion.
- Before you sign anything, make sure you have received all of the answers to your questions, in writing.
- You never have to sign a contract on the spot.
- Provincial Consumer Protection laws often include a cooling off period where consumers can cancel a contract signed within their home up to 10 days after they have received a copy of the signed agreement. The contract has to include specific information about the goods or service and your rights as a consumer. If it doesn't, you can cancel the contract within 1 year of entering into the agreement. You can also cancel the agreement, regardless of its value, up to one year after you entered into it, if the business or salesperson you've signed your contract with made a false or misleading statement about the contract.
- If you believe a business has broken the law regarding a contract signed in your home, contact your respective Consumer Affairs/Protection authority.

14) Keeping More Money in Your Wallet

In 2020, fraudsters asked for the following payment methods most frequently.

Wire Transfer

A wire transfer is the electronic transfer of funds between financial institutions around the world. As a result, both the sender and the recipient must have bank accounts. Fraudsters may temporarily take control of somebody else's account for a few days or they may open accounts using stolen identities. Wire transfers are useful as the money moves rather quickly (within 72 hours). The main risk is that you send money, the recipient withdraws the cash and you do not realize it is part of a fraud until it is too late. You should always know who you are sending money to. If you need to reverse a wire transfer, contact the remitting financial institution as soon as possible.

Cryptocurrency

Cryptocurrencies are the latest form of digital or virtual money. They operate independently from a central financial institution and are currently unregulated in

Canada. While many coin offerings exist, the most recognized currency is Bitcoin. While an increasing number of businesses are accepting cryptocurrency as a form of payment, government agencies are not. If you submitted money into a Bitcoin ATM following a fraudulent request, return to the ATM and contact the owner immediately. Some ATMs have scheduled delayed deposits.

Credit Card

Credit cards can be used a variety of fraudulent ways. If stolen, fraudsters may make a number of small purchases within a short amount of time by taking advantage of the physical card's tap feature. If the information on the card is compromised (cardholder name, card number, expiry date and CVC code), fraudsters may impersonate you to complete Card-Not-Present purchases or fraudulent merchants may apply unauthorized transactions onto your account. It is important to use a major credit card when shopping online as these offer higher levels of purchase protection. If you have received counterfeit or lesser quality product, a different product or nothing at all, dispute the associated charges with your credit card provider.

Victims of identity fraud may have a number of unauthorized credit cards issued in their name. These victims are not responsible for debts that may accrue in their name as a direct result of identity fraud.

Cheque/Money Order/Bank Draft

Victims are asked to write a cheque and send it in the mail. The money will likely be shipped to a money mule. A money mule transfers money for others (aka money laundering). These mules may be willing members within the fraud network or they may be unsuspecting victims assuming they are receiving funds as part of a job, prize or even on behalf of "friend".

Prepaid Gift Cards

Prepaid Gift cards are a popular and convenient way to give someone a gift. Gift cards are for gifts and not payments. As a result, anyone who demands a payment by gift card is always a fraudster. Fraudsters most commonly pose as government agencies, law enforcement, or service providers when making these demands. The cards they request the most are: Amazon, Apple iTunes, Google Play, and Steam. The fraudsters do not need the physical cards to access the funds. Instead, all they require is the number on the back of the card which is revealed after scratching the

card. Once the card has been used or the numbers on the back revealed, you probably cannot get your money back. To report the fraud or attempt to recover funds, contact the number on the back of the card.

Email Money Transfer (EMT)

Similar to wire transfers, email money transfers are made between two bank accounts. The sender initiates the transfer through their online banking account and only requires the recipient's email address or mobile phone number. The funds are instantly debited from the sender's account and are deposited into the recipient's account once they answer the security question. It is important to create a hard-to-guess answer that you provide only to the recipient. Funds may be instantly deposited if the recipient has setup auto-deposit on their account. EMTs may be cancelled or reversed, but strictly before the funds are deposited.

Cash

Whether given in person or sent in the mail, cash provided to fraudsters is non-refundable. Fraudsters may ask you to hide cash in books or magazines when sending it through the mail. If you have sent cash in the mail as a result of a fraud, contact the courier company immediately with the tracking number to attempt to return the parcel.

Money Service Businesses

Money Service Businesses (e.g. MoneyGram and Western Union) facilitate money transfers between individuals or organizations within minutes. Senders may pay for the transfer online or in-store. Meanwhile, money can be sent to a bank account or provided to the recipient in cash at any worldwide retail location. A fraudster only requires an identity document to recover the cash in person.

All victims should report and dispute fraudulent transactions with the store, agency or financial institution that facilitated the payment. Follow the appropriate resolution process as soon as possible as some of them are time limited. Restitution is never guaranteed.

CANADIAN ANTI-FRAUD CENTRE BULLETIN

Financial Scams 2021-03-08

FRAUD: RECOGNIZE, REJECT, REPORT

The COVID-19 pandemic continues to pose financial challenges and uncertainty for many. Whether it is caused by illness or job loss, financial emergencies can be stressful and cause considerable hardship.

Financial scams pose a significant risk to Canadians. Loan scams, job scams, grant scams and investment scams often target people experiencing financial hardship.

Loan scams are typically advertised online through social media or websites that are designed to look like legitimate lending institutions. Their fraudulent loan applications are used to collect your personal information which can lead to identity fraud. Once quickly approved, the fraudsters will request a fee, or several, to secure the loan. The victim never receives any money.

Job Scams are most often received through an email offer where the suspect claims to have found your resume online. In many job scams, consumers are asked to receive or process payments on behalf of the prospective employer. In these cases, victims receive cheques (by mail or mobile deposit) or e-transfers deposited into their bank account. They are told to send money back to the suspect company through money service businesses (Western Union or MoneyGram), cryptocurrency (Bitcoin) or buy gift cards.

Grant scams are offers of guaranteed free money. Yet, fraudsters will collect personal and financial information, upfront fees, and leave consumers with empty promises. Common grant scams involve ads stating that you may qualify for free money that you can spend on anything. All you have to decide is how much money you would like, and pay the fee based on that amount. The promise is that the more you can pay upfront, the more you will receive.
In a popular variation of the scam, the consumer receives a message from one of their trusted friends. The message states that they received a free grant and encourages the consumer to follow their lead. Unfortunately, the messages are from the fraudster who has hacked their friend's account.

Investment scam reports received by the CAFC include initial coin offerings, Ponzi schemes, franchise opportunities, futures trading, multi-level marketing opportunities, mortgage investment opportunities and pump and dump schemes. In most of these cases, the investment opportunities offer higher than normal, or true monetary, returns which often result in investors losing most, or all, of their money.

Warning signs

- Investment opportunities with higher than normal returns.
- Unsolicited telephone, email or social media investment offers.
- Displays of urgency so you don't miss out.
- Companies that offer guaranteed loans; even if you have bad credit or no credit.
- Instant approvals.
- Unsolicited messages offering employment.
- Government grants are available to specific demographics for specific reasons.
- All grants require an application. Government grant applications are readily available and free.
- Grant applications are not guaranteed to be accepted; even if you meet the eligibility requirements.
- There are no upfront fees for legitimate grants.

How to protect yourself

- Do your research before you provide your personal information.
- In most provinces, it is illegal for a company to request an upfront fee before you receive your loan. You should never send money first.
- Contact your provincial consumer protection agency and/or financial regulator to confirm that a company is a legitimate lender.
- Be mindful where you post your resume. Scammers use legitimate websites to seek out victims.
- Take the time to research an employer and confirm that they are hiring.
- If you receive a suspicious message from a trusted friend, reach out to them through a different means of communication to confirm that it is them.
- Do not trust offers of guaranteed free money. If you have to pay money for a free grant, it really isn't free.
- Information for grants and funding from the Government of Canada is available at: https://www.canada.ca/en/government/grants-funding.html.
- Contact your provincial securities regulator if you suspect an investment scam.
- If you receive funds for any reason from an unknown individual or company and you are asked to forward it elsewhere - DON'T!
- Learn more tips and tricks for protecting yourself.

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 www.antifraudcentre-centreantifraude.ca.

CANADIAN ANTI-FRAUD CENTRE BULLETIN

Protecting Your Information 2021-03-15

FRAUD: RECOGNIZE, REJECT, REPORT

Working from home, online banking, and socializing online have all increased over the pandemic period creating new opportunities for fraudsters to capture your personal and financial information. Fraudsters can then use this information to access your accounts, apply for government benefits, credit cards, bank accounts, cell phone accounts or even take over your social media and email accounts. It is important that Canadians take steps to secure their personal and financial information and know what to do when identity fraud occurs.

Recognize…

- Missing bills and other mail.
- Suspicious activity on your bank or credit card statements.
- Letters stating that you are approved or declined credit that you did not apply for.
- Unauthorized applications or accounts on your credit report.
- Creditor or collection agency calls about an application or account you do not have.
- Bills from service providers that you do not use.
- Phishing emails asking you to click on links or open attachments.
- What information has been compromised when you are notified of a database breach.

Reject…

- Unsolicited emails, phone calls or mail asking for personal or financial information.
- Requests for your social insurance number (SIN). It's virtually a key to your identity and credit reports.
- Links in any email that looks suspicious. Never open an attachment from spam or sender not known to you.
- Automatic login features that save your username and password. Take the time to re-enter your password each time.
- Sharing everything through email and social networking sites.
- Default privacy settings on your social accounts.
- Weak passwords. Create strong and unique passwords for every online account including social networks, emails, financial and other accounts.
- Simple login measures. Where possible, set-up multi-factor authentication on your accounts.
- Check your credit report at least once a year. To get a free copy of your report, contact: Equifax Canada and TransUnion Canada.

Report…

- A lost or stolen wallet.
- Compromised government identification to the affected government agency.
- Re-routed mail requests to Canada Post.
- Suspicious bank account activity to your financial institution.
- Unauthorized activity on your credit report to the credit bureaus: Equifax and TransUnion.
- Loss of account access to the appropriate company.
- Learn more tips and tricks for protecting yourself.

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 www.antifraudcentre-centreantifraude.ca

CANADIAN ANTI-FRAUD CENTRE BULLETIN

2021 Fraud Prevention Toolkit - Businesses 2021-02-15

FRAUD: RECOGNIZE, REJECT, REPORT

BUSINESSES

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 use by businesses to further raise public awareness and prevent victimization. We encourage all our partners 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, 2,190 of the reports were from Canadian businesses, that reported losses totalling more than $24.5 million.

Top 10 frauds affecting Canadian businesses based on number of reports in 2020:

Fraud Type	Reports	Victims	Dollar Loss
Spear Phishing	419	157	$11.2 M
Extortion	373	77	$0.6 M
Vendor Fraud	281	185	$2.9 M
Identity Fraud	189	189	N/A
Merchandise	133	91	$4.7 M
Job	116	30	$0.3 M
Service	105	47	$0.3 M
Personal Info	89	36	N/A
Phishing	64	11	N/A
False Billing	40	10	$6,000

Top 10 frauds affecting Canadian businesses based on dollar loss in 2020:

Fraud Type	Reports	Victims	Dollar Loss
Spear Phishing	419	157	$11.2 M
Merchandise	133	91	$4.7 M
Vendor Fraud	281	185	$2.9 M
Investments	16	10	$0.8 M
Extortion	373	77	$0.6 M
Job	116	30	$0.3 M
Service	105	47	$0.3 M
Loan	16	5	$0.3 M
Fraudulent Cheque	6	4	$60,000
Office Supplies	7	2	$20,000

➔ 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:

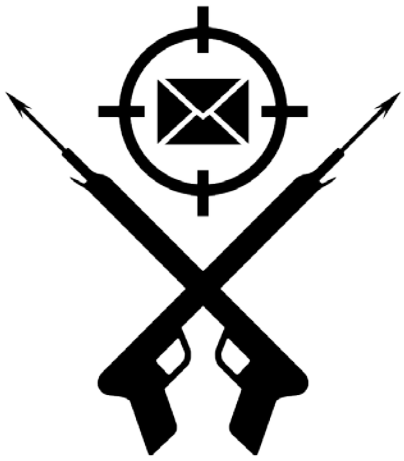
Step 1: Gather all information pertaining to the fraud.
Step 2: Write out a chronological statement of events.
Step 3: Report the incident to your local law enforcement.
Step 4: Report the incident to the CAFC through the Fraud Reporting System (FRS) or toll free at 1-888-495-8501.
Step 5: Report the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

Spear Phishing

Spear phishing is one of the most common and most dangerous attack methods currently used to conduct fraud, usually on businesses and organizations. In preparation of a spear phishing attack, fraudsters take their time to collect information on their intended targets, so they can send convincing emails seemingly from a trusted source. Fraudsters will infiltrate or spoof a business email account. They create a rule to forward a copy of incoming emails to one of their own accounts. They comb through these emails to study the sender's use of language and look for patterns linked to important contacts, payments, and dates.



Fraudsters launch their attack when the owner of the email account cannot be easily contacted by email or by phone. If the fraudsters haven't infiltrated the executive's email account, they may set up a domain similar to the company's and use the executive's name on the account. The contact information they need is often found on the company's website or through social media.

Common Variations

- A top executive requests their Accounts Payable to make an urgent payment to close a private deal.
- A business receives a duplicate invoice with updated payment details supposedly from an existing supplier or contractor.
- An accountant or financial planner receives a large withdrawal request that looks like it's coming from their client's email.
- Payroll receives an email claiming to be from an employee looking to update their bank account information.
- Members of a church, synagogue, temple, or mosque receive a donation request by email claiming to be from their religious leader.
- An email that seems to come from a trusted source asks you to download an attachment, but the attachment is malware that infiltrates an entire network or infrastructure.

Warning Signs

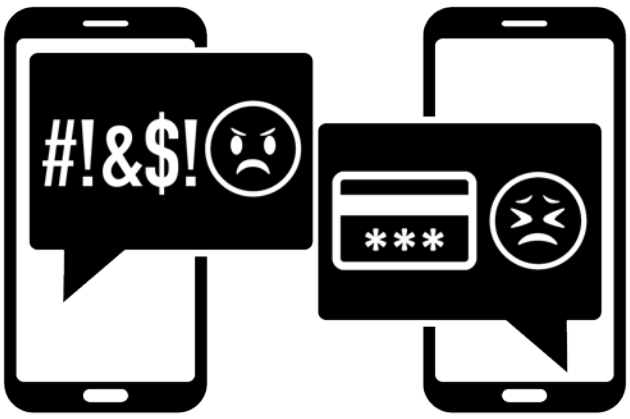
- Unsolicited emails.
- Direct contact from a senior official you are not normally in contact with.
- Requests for absolute confidentiality.
- Pressure or a sense of urgency.
- Unusual requests that do not follow internal procedures.
- Threats or unusual promises of reward.

How to Protect Yourself

- Remain current on frauds targeting businesses and educate all employees. Include fraud training as part of new employee onboarding.
- Put in place detailed payment procedures. Encourage a verification step for unusual requests.
- Establish fraud identifying, managing and reporting procedures.
- Avoid opening unsolicited emails or clicking on suspicious links or attachments.
- Take time to hover over an email address or link and confirm that they are correct.
- Restrict the amount of information shared publicly and show caution with regards to social media.
- Upgrade and update technical security software.

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.

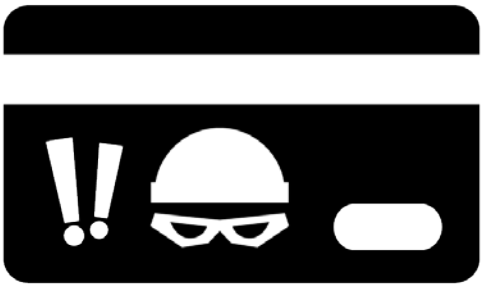
Warning Signs – How to Protect Yourself

- 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).

Vendor Fraud

Business selling merchandise or offering their services online are at risk of receiving fraudulent payments. In many 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.

Card Not Present (CNP): CNP fraud can happen when a business accepts orders and payments over the phone, online or by email. Fraudsters use stolen credit cards to pay for the products or services. They will request express shipping, so that they can receive the order before the card owner discovers the unauthorized charge. When the actual card owner disputes the unauthorized charge, the business must issue a chargeback to the victim's stolen card.



Warning Signs

Customer Flags

- Orders made from one IP address, but using different names, addresses, and payments.
- Email addresses from free email service.
- Many card numbers provided for one order (cards keep getting declined).
- Purchaser name and cardholder name are different.

Product / Order Flags

- Larger than normal orders.
- Many orders for the same product; especially “big ticket” items.
- Orders from repeat customers that differ from their regular spending patterns.
- Orders using the same customer or payment information, but many IP addresses.

Delivery Flags

- Customer requests “rush” or “overnight” delivery.
- Single payment information used for many shipping addresses.
- Billing address different than shipping address.
- Request that extra funds be sent to a third party.

How to Protect Yourself

- Know the Red Flags and verify every order request received.
- Before shipping merchandise, verify the information provided by the customer (telephone number, email address, shipping address, etc.).
- Be aware of request for priority shipments for fraud-prone merchandise.
- Verify priority shipping requests when the shipping and billing addresses don’t match.
- For suspicious orders, contact your payment processor. Verify the security measures to.
- prevent victimization and reduce unwanted chargebacks.
- Never accept overpayments to forward funds to a third party.

Purchase of Merchandise or Service

Businesses must do their due diligence before purchasing products or services from new and unknown suppliers. Fraudsters may place advertisements on popular classified sites or send their advertisements by mail or fax. 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. Buyers may receive counterfeit products, lesser valued & unrelated goods, or nothing at all.

Canadian businesses are also being contacted by fraudsters offering debit and credit card processing services and office supplies at discounted price. In some cases, the fraudsters misrepresent themselves as the business' regular supplier. Businesses may receive an invoice for products they never ordered.

Warning Signs – How to Protect Yourself

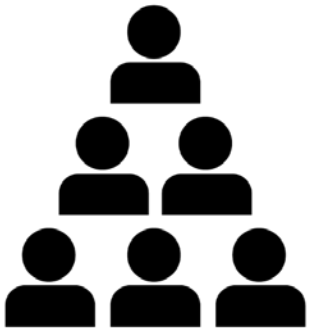
- If it sounds too good to be true, it probably is.
- Verify the URL and seller information's legitimacy.
- Search for any warnings posted online and read reviews before making a purchase.
- Spelling mistakes and grammatical errors are indicators of a fraudulent website.
- Use a credit card when shopping online. Buyers 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.
- Educate your staff on the current frauds that affect businesses.
- Do not provide any information pertaining to the make and model of any office equipment to any organization other than your normal supplier.
- Review suspicious invoices as fraudsters will send false invoices for products or services that were never purchased.

Investment

Any false, deceptive, misleading or fraudulent investment opportunity, often offering higher than normal or true monetary returns. Victims often lose most or all of their money. Investors run the added risk of having their identity stolen, accumulating losses for unauthorized withdrawals on their credit cards and incurring high interest payments on investments that do not exist.

Initial Coin Offerings: The virtual currency market is constantly changing. New virtual currencies are developed monthly. Like an Initial Public Offering (IPO), an Initial Coin Offering (ICO) is an attempt to raise funds to help a company launch a new virtual currency. In an ICO fraud, the fraudsters solicit investment opportunities with fake ICOs. They provide official looking documentation, use buzz words and may even offer a real "token". In the end, everything is fake, and you lose your investment.

Pyramids: Similar to a Ponzi scheme, a pyramid scam focuses primarily on generating profits by recruiting other investors. A common pyramid scam today takes the form of a “gifting circle”. Participants gift a sum of money to join and ultimately must recruit others to make their money back. These schemes may offer products, but they usually have very little value.



Pyramid selling is illegal in Canada. It’s a criminal offence to establish, operate, advertise or promote a scheme of pyramid selling.

Warning Signs – How to Protect Yourself

- Be careful when asked to provide personal or financial information to reclaim your investment profits.
- Beware of opportunities offering higher than normal returns.
- Beware of any urgency pressuring you to make an investment so that you don’t miss out.
- Prior to investing, ask for information on the investment. Research the team behind the offering and analyze the feasibility of the project. Check the registration and enforcement history.
- The Canadian Securities Administrators (CSA) encourages all investors to visit their National Registration Search Tool (www.aretheyregistered.ca).

CANADIAN ANTI-FRAUD CENTRE BULLETIN

2021 Fraud Prevention Toolkit – Young Adults 2021-02-15

FRAUD: RECOGNIZE, REJECT, REPORT

YOUNG ADULTS

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 young adult Canadians (born 1987-2005) 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, 16,340 of the reports were from young adult Canadians, that reported losses totalling more than $16.6 million.

2020 young adult Canadians Top 10 frauds based on number of reports:

Fraud Type	Reports	Victims	Dollar Loss
Identity Fraud	4,772	4,772	N/A
Extortion	4,114	2,295	$4.6 M
Personal Info	1,894	1,426	N/A
Job	1,031	573	$0.9 M
Merchandise	974	834	$0.8 M
Vendor Fraud	832	688	$0.6 M
Phishing	717	371	N/A
Service	311	233	$0.3 M
Romance	139	103	$0.9 M
Investments	130	116	$1.8 M

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

Fraud Type	Reports	Victims	Dollar Loss
Extortion	4,114	2,295	$4.6 M
Investments	130	116	$1.8 M
Job	1,031	573	$0.9 M
Romance	139	103	$0.9 M
Merchandise	974	834	$0.8 M
Vendor Fraud	832	688	$0.6 M
Service	311	233	$0.3 M
Loan	103	93	$0.2 M
Spear Phishing	116	91	$0.2 M
Prize	46	24	$83,000

➔ 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 young adult Canadians:

Identity Theft and Identity Fraud
A victim of identity fraud has previously been the victim of identity theft.

Identity theft occurs when a victim's personal information is stolen or compromised. This can happen as a result of volunteering personal or financial information, a phishing fraud, a stolen wallet, a database breach, etc.

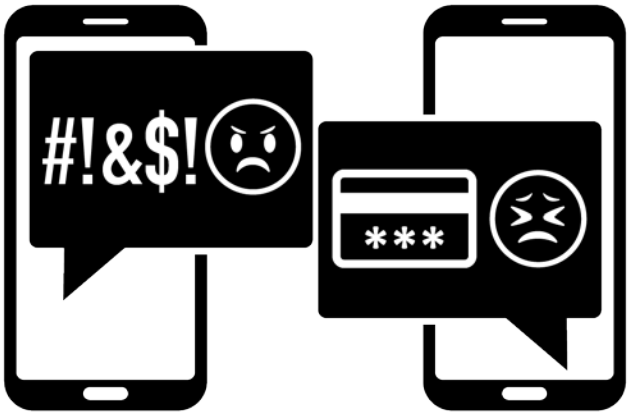
Identity fraud occurs when the fraudster uses the victim's information for fraudulent activity. Fraudsters may create fake identity documents, submit unauthorized credit applications and open financial accounts in your name, re-route your mail, purchase mobile phones, takeover your existing financial and social accounts, etc.

If you are a victim of identity theft and/or fraud, you should immediately complete the following steps:

- **Step 1:** Gather the information pertaining to the fraud.
- **Step 2:** Contact the two major credit bureaus to obtain a copy of your credit report and review with reports.
    - **Equifax Canada:** http://www.consumer.equifax.ca/home/en_ca, 1-800-465-7166
    - **TransUnion Canada:** http://www.transunion.ca, 1-877-525-3823
- **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:** Review your financial statements and notify the affected agency if you notice any suspicious activity.
- **Step 6:** Notify your financial institutions and credit card companies, and change the passwords to your online accounts.
- **Step 7:** If you suspect that your mail has been redirected, notify Canada Post (www.canadapost.ca, 1-866-607-6301) and any service providers.
- **Step 8:** Notify federal identity document issuing agencies:
    - **Service Canada:** www.servicecanada.gc.ca, 1-800-622-6232
    - **Passport Canada:** www.passport.gc.ca, 1-800-567-6868
    - **Immigration, Refugees and Citizenship:** www.cic.gc.ca, 1-888-242-2100
- **Step 9:** Notify provincial identity document issuing agencies.

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

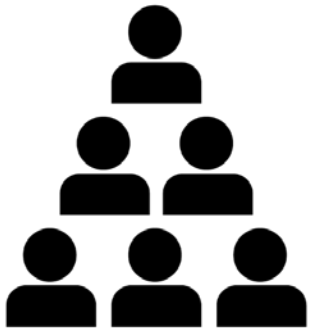
- Be familiar with your service provider's terms of service.
- Contact your service provider directly and verify that your account is in good standing.
- Do not open unsolicited emails and text messages.
- Do not click on suspicious links or attachments.
- Regularly back-up important files.
- Keep your 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).

Investment

Any false, deceptive, misleading or fraudulent investment opportunity, often offering higher than normal or true monetary returns. Victims often lose most or all of their money. Investors run the added risk of having their identity stolen, accumulating losses for unauthorized withdrawals on their credit cards and incurring high interest payments on investments that do not exist.

Initial Coin Offerings: The virtual currency market is constantly changing. New virtual currencies are developed monthly. Like an Initial Public Offering (IPO), an Initial Coin Offering (ICO) is an attempt to raise funds to help a company launch a new virtual currency. In an ICO fraud, the fraudsters solicit investment opportunities with fake ICOs. They provide official looking documentation, use buzz words and may even offer a real "token". In the end, everything is fake, and you lose your investment.

Pyramids: Similar to a Ponzi scheme, a pyramid scam focuses primarily on generating profits by recruiting other investors. A common pyramid scam today takes the form of a “gifting circle”. Participants gift a sum of money to join and ultimately must recruit others to make their money back. These schemes may offer products, but they usually have very little value.



Pyramid selling is illegal in Canada. It’s a criminal offence to establish, operate, advertise or promote a scheme of pyramid selling.

Warning Signs – How to Protect Yourself

- Be careful when asked to provide personal or financial information to reclaim your investment profits.
- Beware of opportunities offering higher than normal returns.
- Beware of any urgency pressuring you to make an investment so that you don’t miss out.
- Prior to investing, ask for information on the investment. Research the team behind the offering and analyze the feasibility of the project. Check the registration and enforcement history.
- The Canadian Securities Administrators (CSA) encourages all investors to visit their National Registration Search Tool (www.aretheyregistered.ca).

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 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.

Vehicle for Sale: Vehicles are advertised at a lower than average price. Fraudsters claim to be located overseas and a third-party agency will deliver the vehicle. The victim is asked to submit payments for the vehicle and delivery. Nothing is ever delivered.

Animal for Free: Fraudsters will often advertise animals for free; puppies and kittens are used most often. They will claim that the animal is free; however, the victim will be required to pay shipping. Once the payment is received, the fraudsters will begin to request additional payments for: transportation cage, vaccinations, medication, insurance, customs and brokerage fees, etc.

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.

CANADIAN ANTI-FRAUD CENTRE BULLETIN

2021 Fraud Prevention Toolkit – Middle Agers 2021-02-15

FRAUD: RECOGNIZE, REJECT, REPORT

MIDDLE AGERS

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 middle age Canadians (born 1962-1986) 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, 24,271 of the reports were from middle age Canadians, that reported losses totalling more than $36.3 million.

2020 Top 10 frauds affecting middle age Canadians based on number of reports:

Fraud Type	Reports	Victims	Dollar Loss
Identity Fraud	7,951	7,951	N/A
Extortion	6,189	2,169	$3.0 M
Personal Info	2,173	1,497	N/A
Merchandise	1,246	1,029	$2.7 M
Phishing	1,180	360	N/A
Job	651	267	$0.7 M
Vendor Fraud	595	320	$0.4 M
Service	587	379	$0.8 M
Romance	334	226	$7.5 M
Spear Phishing	226	132	$0.4 M

2020 Top 10 frauds affecting middle age Canadians based on dollar loss:

Fraud Type	Reports	Victims	Dollar Loss
Romance	334	226	$7.5 M
Investments	186	159	$3.9 M
Extortion	6,189	2,169	$3.0 M
Merchandise	1,246	1,029	$2.7 M
Service	587	379	$0.8 M
Job	651	267	$0.7 M
Loan	193	151	$0.6 M
Spear Phishing	226	132	$0.4 M
Vendor Fraud	595	320	$0.4 M
Bank Investigator	168	63	$0.3 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 middle age Canadians:

Identity Theft and Identity Fraud
A victim of identity fraud has previously been the victim of identity theft.

Identity theft occurs when a victim's personal information is stolen or compromised. This can happen as a result of volunteering personal or financial information, a phishing fraud, a stolen wallet, a database breach, etc.

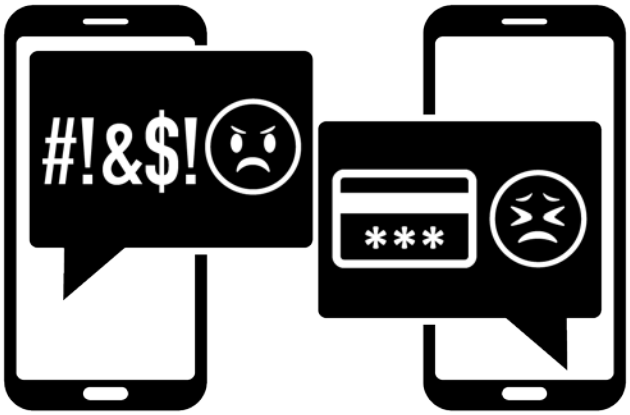
Identity fraud occurs when the fraudster uses the victim's information for fraudulent activity. Fraudsters may create fake identity documents, submit unauthorized credit applications and open financial accounts in your name, re-route your mail, purchase mobile phones, takeover your existing financial and social accounts, etc.

If you are a victim of identity theft and/or fraud, you should immediately complete the following steps:

- **Step 1:** Gather the information pertaining to the fraud.
- **Step 2:** Contact the two major credit bureaus to obtain a copy of your credit report and review with reports.
    - **Equifax Canada:** http://www.consumer.equifax.ca/home/en_ca, 1-800-465-7166
    - **TransUnion Canada:** http://www.transunion.ca, 1-877-525-3823
- **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:** Review your financial statements and notify the affected agency if you notice any suspicious activity.
- **Step 6:** Notify your financial institutions and credit card companies, and change the passwords to your online accounts.
- **Step 7:** If you suspect that your mail has been redirected, notify Canada Post (www.canadapost.ca, 1-866-607-6301) and any service providers.
- **Step 8:** Notify federal identity document issuing agencies:
    - **Service Canada:** www.servicecanada.gc.ca, 1-800-622-6232
    - **Passport Canada:** www.passport.gc.ca, 1-800-567-6868
    - **Immigration, Refugees and Citizenship:** www.cic.gc.ca, 1-888-242-2100
- **Step 9:** Notify provincial identity document issuing agencies.

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

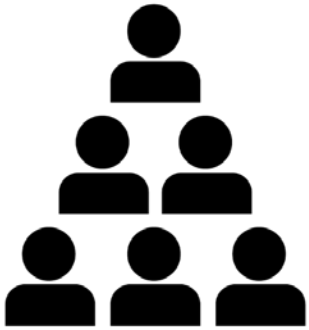
- Beware of individuals quickly professing their love for you.
- Beware of individuals who claim to be wealthy, but need to borrow money.
- When trying to setup an in-person meeting, be suspicious if they always provide you with reasons to cancel. If you do proceed, meet in a public place and inform 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.

Investment

Any false, deceptive, misleading or fraudulent investment opportunity, often offering higher than normal or true monetary returns. Victims often lose most or all of their money. Investors run the added risk of having their identity stolen, accumulating losses for unauthorized withdrawals on their credit cards and incurring high interest payments on investments that do not exist.

Initial Coin Offerings: The virtual currency market is constantly changing. New virtual currencies are developed monthly. Like an Initial Public Offering (IPO), an Initial Coin Offering (ICO) is an attempt to raise funds to help a company launch a

new virtual currency. In an ICO fraud, the fraudsters solicit investment opportunities with fake ICOs. They provide official looking documentation, use buzz words and may even offer a real "token". In the end, everything is fake, and you lose your investment.



Pyramids: Similar to a Ponzi scheme, a pyramid scam focuses primarily on generating profits by recruiting other investors. A common pyramid scam today takes the form of a “gifting circle”. Participants gift a sum of money to join and ultimately must recruit others to make their money back. These schemes may offer products, but they usually have very little value.

Pyramid selling is illegal in Canada. It’s a criminal offence to establish, operate, advertise or promote a scheme of pyramid selling.

Warning Signs – How to Protect Yourself

- Be careful when asked to provide personal or financial information to reclaim your investment profits.
- Beware of opportunities offering higher than normal returns.
- Beware of any urgency pressuring you to make an investment so that you don’t miss out.
- Prior to investing, ask for information on the investment. Research the team behind the offering and analyze the feasibility of the project. Check the registration and enforcement history.
- The Canadian Securities Administrators (CSA) encourages all investors to visit their National Registration Search Tool (www.aretheyregistered.ca).

Merchandise

Fraudsters may place advertisements on popular classified sites or social networks. They may also 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.

Vehicle for Sale: Vehicles are advertised at a lower than average price. Fraudsters claim to be located overseas and a third-party agency will deliver the vehicle. The victim is asked to submit payments for the vehicle and delivery. Nothing is ever delivered.

Animal for Free: Fraudsters will often advertise animals for free; puppies and kittens are used most often. They will claim that the animal is free; however, the victim will be required to pay shipping. Once the payment is received, the fraudsters will begin to request additional payments for: transportation cage, vaccinations, medication, insurance, customs and brokerage fees, etc.

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.

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:

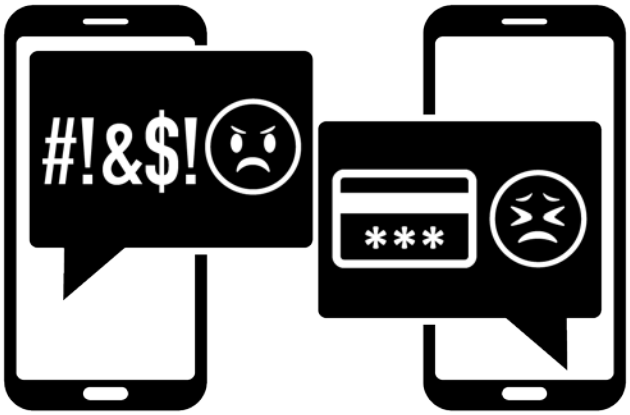
Step 1: Gather all information pertaining to the fraud.
Step 2: Write out a chronological statement of events.
Step 3: Report the incident to your local law enforcement.
Step 4: Report the incident to the CAFC through the Fraud Reporting System (FRS) or toll free at 1-888-495-8501.
Step 5: Report the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

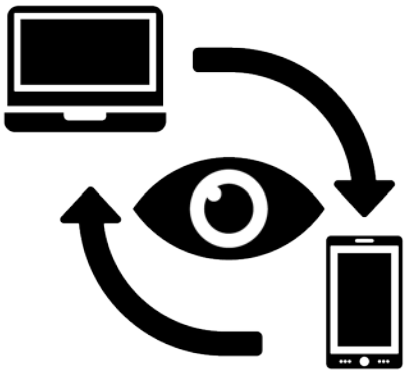
Warning Signs - How to Protect Yourself

- 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.

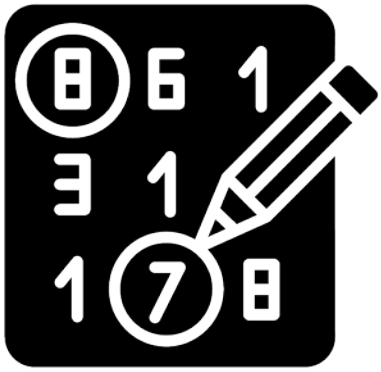
Bank Investigator

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.