CANADIAN ANTI-FRAUD CENTRE

Royal Canadian Mounted Police | Gendarmerie royale du Canada | Competition Bureau Canada | Bureau de la concurrence Canada | Ontario Provincial Police | Canada

YOUNG ADULTS

2022 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

While we know that the COVID-19 pandemic exposed new vulnerabilities and increased the potential of fraud victimization, we did not expect to see fraud losses more than double from 2020 to 2021. Losses reported to the Canadian Anti-Fraud Centre reached an all- time high of 379 million in 2021, with Canadian losses accounting for 275 million of this. Fraud Prevention Month is a campaign held each March to inform and educate the public on the importance of protecting yourself from being a victim of fraud. This year's theme is impersonation, and focuses on scams where fraudsters will claim to be government official, critical infrastructure companies, and even law enforcement officials.

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 on its Facebook and Twitter platforms, using #FPM2022. Bulletins will also be published weekly on social media.

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
English: https://www.youtube.com/watch?v=0rlWUcc57dM
French: https://www.youtube.com/watch?v=cXXP35rICQY
A Cry from the Heart from Victims
English:https://www.youtube.com/watch?v=blyhHl8rc7g
French: https://www.youtube.com/watch?v=cHZfvpH2YW8
Telemarketing Fraud: The Seamy Side
English: 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 week aimed at highlighting the top impersonation scams reported to CAFC in 2021.

Bulletins

Week 1: Investments
Week 2: Extortion Scams & Emergency Scams
Week 3: Phishing
Week 4: Spear Phishing

CAFC will highlight the weekly bulletin topic throughout each week.
Like us on Facebook – Canadian Anti-Fraud Centre
Follow us on Twitter – @canantifraud

March 2022 – A FPM video will be shared on social media highlighting ways to protect yourself from being a victim.

March 2022

	Tues March 1 Facebook & Twitter: #FPM2022 Introduction and Kick-Off	Wed March 2 Facebook & Twitter #FPM2022 Launch Video	Thurs March 3 Facebook & Twitter Bulletin- Investment Scams	Fri March 4 Facebook & Twitter Social Media Impersonation Investment Scams
Mon March 7 Facebook & Twitter Fake crypto investment websites	Tues March 8 Facebook & Twitter Share partner #FPM2022 posts	Wed March 9 Facebook & Twitter Request to transfer crypto investments to fraudulent platforms	Thurs March 10 Facebook & Twitter Share partner #FPM2022 posts	Fri March 11 Facebook & Twitter Pyramid, job and investment scams.
Mon March 14 Facebook & Twitter Bulletin: Extortion Scams	Tues March 15 Facebook & Twitter Threatening automated CBSA phone calls	Wed March 16 Facebook & Twitter Bulletin: Emergency/Grandparents Scam	Thurs March 17 Facebook & Twitter Share partner #FPM2022 posts	Fri March 18 Facebook & Twitter Threatening letters impersonating RCMP
Mon March 21 Facebook & Twitter Bulletin: Phishing	Tues March 22 Facebook & Twitter Share partner #FPM2022 posts	Wed March 23 Facebook & Twitter Phishing messages impersonating government agencies	Thurs March 24 Facebook & Twitter Share partner #FPM2022 posts	Fri March 25 Facebook & Twitter Phishing messages impersonating financial institutions
Mon March 28 Facebook & Twitter Bulletin: Spear Phishing	Tues March 29 Facebook & Twitter Spear Phishing stats and warning signs	Wed Mar 30 Facebook & Twitter Share partner #FPM2022 posts	Thurs March 31 Facebook & Twitter How to protect yourself from Spear Phishing scams	

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 2021, the CAFC received 104,295 fraud reports involving over $379 million in reported losses. Moreover, 11,024 of the reports were from young adults that reported losses totalling more than $26.6 million.

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

Fraud Type	Reports	Victims	Dollar Loss
Extortion	2238	1087	$4.9 M
Personal Info	1913	1609	$0.02M
Job	1149	722	$1.1M
Vendor Fraud	1101	863	$2.0M
Merchandise	994	871	$1.1M
Phishing	798	372	$0.01M
Service	570	434	$0.8M
Investments	536	504	$11.8M
Romance	227	185	$3.7M
Spear Phishing	139	110	$0.2M

Top 10 frauds affecting young adults based on dollar loss in 2021:

Fraud Type	Reports	Victims	Dollar Loss
Investment	536	504	$11.8M
Extortion	2238	1087	$4.9M
Romance	227	185	$3.7M
Vendor Fraud	1101	863	$2.0M
Job	1149	722	$1.1M
Merchandise	994	871	$1.1M
Service	570	434	$0.8M
Loan	106	99	$0.2M
Spear Phishing	139	110	$0.2M
Bank Investigator	128	74	$0.1M

➔ 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.

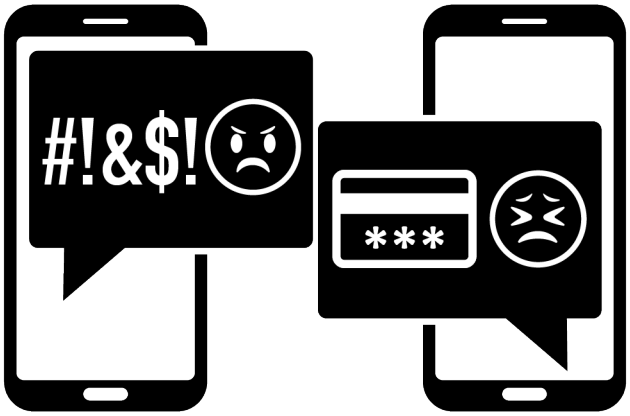
If you are a victim of identity theft and/or fraud, you should immediately complete the following steps:

- **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.

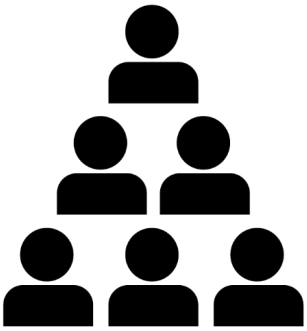
Warning Signs – How to Protect Yourself

- 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 Scams

Investment scams were the highest reported scams based on dollar loss in 2021. Victims of investment scams reported a total loss of $169.9 Million to CAFC. Investment Scams are defined as 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.

Crypto Investment Scams: The majority of the investment scam reports involve Canadians investing in crypto currency after seeing a deceptive advertisement. It typically involves victims downloading a trading platform and transferring crypto currency into their trading account. In most cases, victims are not able to withdraw their funds. It is very likely that many of the trading platforms are fraudulent or controlled by fraudsters

Variations of Crypto Investment Scams

- The victim is approached on a dating or social media website. In some cases, the scam starts as a romance scam and quickly turns into an "investment opportunity". Because suspects have gained the victim's trust, it can lead to a high dollar loss for the victim.
- In some reports, suspects have compromised victim's friend's social media accounts. Because the victim believes they are communicating with a friend or a trusted person, they are easily convinced to take advantage of the "investment opportunity".
- The suspect calls a victim directly and convinces them to invest into crypto currency. In many cases, the suspect asks for remote access to the victim's computer. The suspect shows the victim a fraudulent crypto investing website and convinces the victim to invest based on the potential exponential growth of the investment. In many cases, the victim will invest over a long period of time and, in the end, will realize that the funds can not be withdrawn.
- An email is received by the victim offering a crypto investment opportunity.
- The victim comes across an advertisement on social media. After the victim clicks on the ad and provides their contact information, suspects contact the victim by telephone and convince them to invest.

Warning Signs – How to Protect Yourself

- Be careful when sending cryptocurrency. Once the transaction is completed, it is unlikely to be reversed.
- As proceeds of crime and anti-money laundering regimes around the world create regulatory frameworks that treat businesses dealing in crypto currencies as money service businesses, Canadians need do their research to ensure they are using reputable and compliant services.
- 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.

- Verify if the investment companies are registered with your Provincial Securities Agency or the National Registration Search Tool (www.aretheyregistered.ca).
- Prior to investing, ask for information on the investment. Research the team behind the offering and analyze the feasibility of the project.
- Be weary of individuals met on dating or social media who attempt to educate and convince you to invest into crypto currency.
- Beware of fraudsters asking you to open and fund new crypto currency accounts. They will direct you to send it to wallets they control. Don't!

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.

Checklist: Be Cyber Secure and Fraud Aware

With fraud and cybercrime reporting going up again this year, the CAFC created the following checklists so that Canadians can be fraud aware and cyber secure in 2022.

Be Fraud Aware

- ✓ Don't be afraid to say no.
- ✓ Don’t react impulsively, scrutinize urgent requests.
- ✓ Don't be intimidated by high-pressure sales tactics.
- ✓ Ask questions and talk to family members or friends.
- ✓ Request the information in writing.
- ✓ If in doubt, hang up.
- ✓ Watch out for urgent pleas that play on your emotions.
- ✓ Always verify that the organization you're dealing with is legitimate.
- ✓ Don't give out personal information.
- ✓ Beware of unsolicited calls or emails (e.g. phishing) that ask you to confirm or update your personal or financial information.

Be Cyber Secure

- ✓ Protect your computer by ensuring your operating system and security software are up-to-date.
- ✓ Secure your online accounts, use strong passwords and, where possible, enable two-factor authentication.
- ✓ Secure your devices and internet connections
- ✓ Some websites, such as music, game, movie, and adult sites, may try to install viruses or malware without your knowledge.
- ✓ Watch out for pop-ups or emails with spelling and formatting errors.
- ✓ Beware of attachments and links as they may contain malware or spyware.
- ✓ Never give anyone remote access to your computer
- ✓ Disable your webcam or storage devices when not in use.
- ✓ If you are having problems with your device, bring it to a local technician

For Businesses

Be Fraud Aware and Cyber Secure

- ✓ Train your employees about cyber security and fraud.
- ✓ Have policies or a plan in place to help employees.
- ✓ Know who you're dealing with. Consider compiling a list of companies your business uses to help employees know which contacts are real and which aren't.
- ✓ Watch out for invoices using the name of legitimate companies. Scammers will use real company names like Yellow Pages to make the invoices seem authentic. Make sure you inspect invoices thoroughly before you make a payment.
- ✓ Don't give out information on unsolicited calls or to unsolicited emails
- ✓ Educate employees at every level to be wary of unsolicited calls. If they didn't initiate the call, they shouldn't provide or confirm any information, including:
    - The business address
    - The business phone number
    - Any account numbers

- Any information about equipment in the office (e.g., make and model of the printer, etc.)

✓ Limit your employees' authority by only allowing a small number of staff to approve purchases and pay bills.

✓ Beware of spear phishing. Have policies in place to verbally confirm requests for urgent wire transfers or purchases.

✓ Review potentially fraudulent orders. Watch for:

- Larger than normal orders
- Multiple orders for the same product
- Orders made up of "big-ticket" items
- Use of multiple credit cards to pay

✓ Review the Get Cyber Safe guide for businesses. CyberSecure Canada….