CANADIAN ANTI-FRAUD CENTRE

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

SHOW ME THE FRAUD

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 --- 3
Resource Libraries --- 4
Calendar of Events --- 4
About the CAFC --- 6
Statistics --- 6
Reporting Fraud --- 7
Key Messages and Slogans --- 7
Most Common Frauds --- 11
- Extortion --- 12
- Romance --- 14
- Phishing & Smishing --- 15
- Spear Phishing --- 15
- Purchase of Merchandise --- 17
- Vendor Fraud --- 18
- Service --- 20
- Job --- 21
- Investment --- 22
- Prize --- 24
- Emergency --- 25

ID Theft & Fraud --- 26
Cutting Contact with the Fraudsters --- 27
- Telephone call --- 27
- Email or text message --- 29
- Online --- 31
- Social networks --- 34
- Mail or in person --- 36

Keeping More Money in Your Wallet --- 38
Checklist: Be Cyber Secure and Fraud Aware --- 41

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 Impersonation Scams. 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) **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 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 – An FPM video will be shared on social media highlighting ways to protect yourself from being a victim.

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 Share partner #FPM2022 posts	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/Grandparent 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.

Top 10 frauds based on number of reports in 2021:

Fraud Type	Reports	Victims	Dollar Loss
Identity Fraud	20849	30849	N/A
Extortion	14202	3160	$18 M
Personal Info	7566	4730	N/A
Phishing	7190	1597	N/A
Counterfeit Merchandise	5200	5151	$1.1 M
Service	5106	3223	$11.6 M
Merchandise	4994	4051	$12.3 M
Vendor Fraud	4038	2431	$7.8 M
Job	3796	1880	$9.4 M
Investments	3442	3077	$163.9 M

Top 10 frauds based on dollar loss in 2021:

Fraud Type	Reports	Victims	Dollar Loss
Investments	3442	3077	$163.9 M
Romance	1928	1365	$64.6 M
Spear Phishing	1817	871	$54 M
Extortion	14202	3160	$18 M
Merchandise	4994	4051	$12.3 M
Service	5106	3223	$11.6 M
Job	3796	1880	$9.4 M
Vendor Fraud	4038	2431	$7.7 M
Loan	570	434	$6.9 M
Bank Investigator	2212	734	$4.6 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.

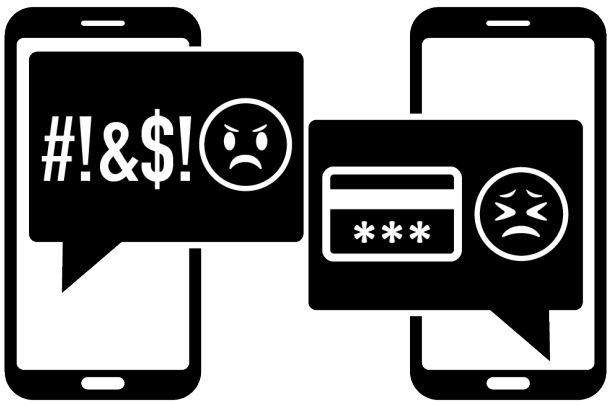
We encourage our partners to share the following messages with the tag **#Tell2, protect many**.

- 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:

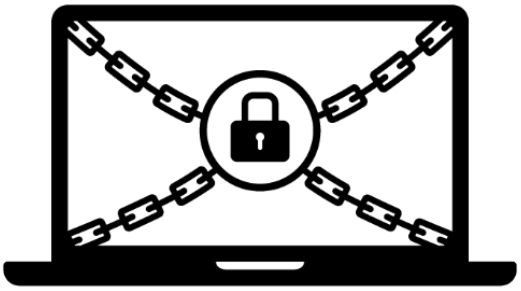
Extortion
Extortion happens when someone unlawfully obtains money, property or services from a person, entity or institution through coercion.



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

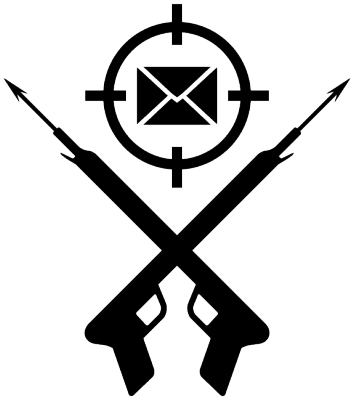
Traditional phishing emails and smishing text messages are techniques designed to trick the victim into thinking they are dealing with a reputable company (i.e. financial institution, service provider, government). Phishing/Smishing messages will direct you to click a link for various reason, such as, 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 fraud is one of the most prevalent frauds targeting 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 place advertisements on popular classified sites or social networks. They may also create websites that have 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.

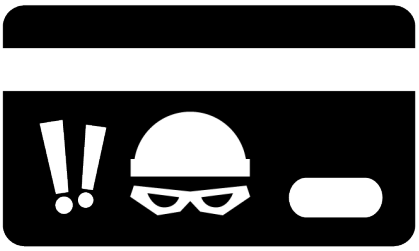
Warning Signs/ How to Protect Yourself

- 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

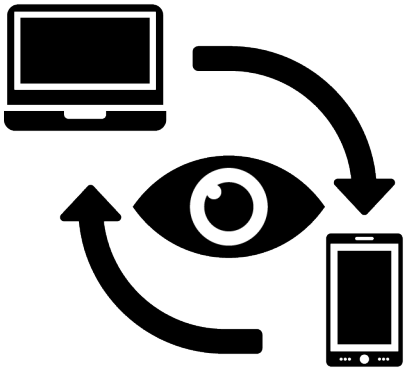
- Know the Red Flags and verify every order request received.
- Before shipping merchandise, verify the information provided by the customer (telephone number, email address, shipping address, etc.).
- Be aware of request for priority shipments for fraud-prone merchandise.

- 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.

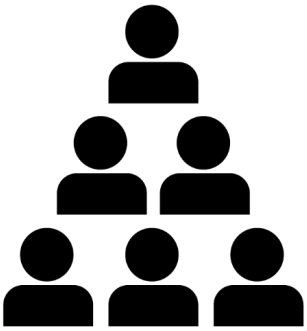
Warning Signs - How to Protect Yourself

- 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 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.

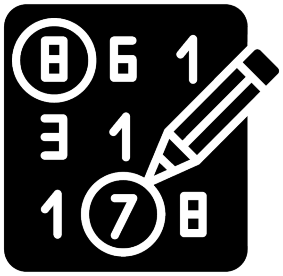
- The victim comes across an advertisement on social media. After the victim clicks on the ad and provides their contact information, suspects contact the victim by telephone and convince them to invest.

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 accounts. They will direct you to send it to wallets they control. Don't!

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.

Emergency/Grandparent Scam

Suspects contact seniors or family members claiming that their grandchild or family member was in an accident, charged with an offence such as a DUI and drug offences or, in some cases, is ill with COVID-19. Suspects will claim that they are law enforcement officials, lawyers and even impersonate the grandchild/family member. They will proceed to advise the victim that a payment for supposed bail or fine is required immediately in order for the family member to avoid going to jail. If the victim agrees to pay the requested amount, suspects will arrange to pick up the funds in person or will ask the victim to send cash in the mail.

How to protect yourself

- If you receive a suspicious phone call claiming to be from a family member in an emergency situation, hang up the phone and contact them directly.
- If the caller claims to be a law enforcement official, hang up and call your police directly.
- Listen to that inner voice that is screaming at you, "This doesn't sound right".

- Be careful what you post online. Scammers can use details shared on social media platforms and dating sites for targeting purposes. Suspects can easily gather names and details about your loved ones.
- Be suspicious of telephone calls that require you to immediately take action and request bail money for a family member in distress.
- Be careful with caller ID numbers that look familiar. Scammers use technology to disguise the actual number they are calling from (spoof) and make it appear as a trusted phone number.

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 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.

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

- 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 2021, 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. While many cryptocurrencies exist, the most recognized currency is Bitcoin. An increasing number of businesses are accepting cryptocurrency as a form of payment, while 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. For instance, 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. In most cases these victims are not responsible for debts that may accrue in their name as a direct result of identity fraud, however the onus is on them to prove it.

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. Additionally, 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.

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 system, 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. Add sentence to get business CyberSecure certified…