SHOW ME THE FRAUD

2025 Fraud Awareness Toolkit

Contents

Introduction 4
Evolution of Fraud and Technology Over the Past 20 Years 6
Technology-Driven Fraud: 6
More Sophisticated Scams: 6
Globalization: 6
Data Breaches and Identity Theft: 6
Cryptocurrency: 6
Increased Awareness and Prevention Efforts: 6
Collaboration and Information Sharing: 7
Artificial Intelligence : 7
Phishing and Social Engineering: 7
Fraudulent Account Creation: 7
Data Analysis for Targeting: 7
Deepfake Technology: 7
QR Codes : 7
Vendor Fraud 7
Cryptocurrency QR Codes 8
Phishing 8
Resources 9
CAFC Logo 9
Video Library 9
Fraud Prevention Material 9
Competition Bureau of Canada FPM 2025 9
Presentation 9
About the CAFC 9
Statistics 10
Reporting Fraud 11
Key Message and Slogan 11
Fraud: Recognize, Reject, and Report It. 11
Fraud Prevention Checklist: 12

Most Common Frauds 12
Extortion 12
Romance and Relationship 14
Phishing and Smishing 16
Spear Phishing 17
Purchase of Merchandise 19
Vendor Fraud 20
Service 21
Job 22
Investment Scams 23
Prize 26
Emergency-Grandparent Scam 27
Bank Investigator 27
Identity Theft and Identity Fraud 29
Cutting Contact with the Fraudsters 30
Telephone Call 30
Email and Text Message 32
Online 33
Social Networks 35
Mail & In-Person 37
Keeping Your Money in Your Wallet 39
Wire Transfer 39
Cryptocurrency 39
Credit Card 39
Cheque, Money Order, Bank Draft 39
Prepaid Gift Cards 40
Email Money Transfer (EMT)/ E-Transfer 40
Cash 40
Money Service Businesses 40
Checklist: Be Cyber Secure and Fraud Aware 41
Be Fraud Aware 41

Be Cyber Secure 41
For Businesses 41

Introduction

As we mark the beginning of Fraud Prevention Month, we first want to reflect on the significant strides we've made in combating, and protecting Canadians, from fraud.

Since its inception 21 years ago, Fraud Prevention Month has been a collaborative effort between government agencies, law enforcement, businesses, media and consumer advocates to raise awareness and empower Canadians to recognize, reject and report fraud.

Over the past two decades, the landscape of fraud has evolved dramatically; driven by advancements in technology, changes in consumer behavior and sophisticated social engineering tactics used by criminals. What once may have been a simple email phishing scam has now transformed into complex cybercrime operations that exploit vulnerabilities in digital platforms. Furthermore, these criminals are masters of exploiting human psychology; by creating scenarios that deceive victims quickly and by relying on manipulation tactics.

This year, we will be ***uncovering fraud*** by revealing the tactics criminals use to create convincing identities, by looking at the impact on victims and discussing what we are doing to fight this scourge of fraud. Fraudsters are experts at disguising themselves and creating false identities to manipulate, deceive, and steal from their victims. By exposing their practices, we aim to empower Canadians to spot fraud before it happens.

The Canadian Anti-Fraud Centre (CAFC), in collaboration with its partners, has played a pivotal role in this ongoing battle. By providing timely and accurate information on emerging fraud trends, offering support to victims, and coordinating with law enforcement agencies across Canada and internationally, the CAFC has been central to many fraud reduction efforts.

We know that fraud will continue to evolve in regards to both technological and social aspects requiring a proactive and adaptive approach to prevention. As technology advances and new forms of fraud emerge, it is crucial for Canadians to train themselves and exercise safety precautions in order to adopt best practices for protecting themselves against fraud.

This Fraud Prevention Month, let us renew our commitment to reducing fraud in all its forms. By working together and staying informed, we can build a safer and more secure future for all Canadians.

Your CAFC Fraud Prevention Team
Follow us on Twitter – @canantifraud Like us on Facebook – Canadian Anti-Fraud Centre

Evolution of Fraud and Technology Over the Past 20 Years

Over the last 20 years, fraud has evolved significantly. Here's an overview of some key trends and challenges:

Technology-Driven Fraud: Data from Statistics Canada shows that the use of the internet for individuals in Canada has increased from 68% in 2006[1] to 95.6% in 2022[2]. The increase in internet use and the evolution of technology has created a higher-risk fraud related environment for Canadians. Criminals are targeting Canadians who may be new to the cyber environment, less tech-savvy or businesses that may not have adequate cyber protection or procedures in place.

More Sophisticated Scams: Fraud schemes have become more complex; leveraging advanced tsocial engineering tactics, malware, and encryption to evade detection and deceive victims. These scams often target individuals and businesses alike.

Globalization: Globalization is a term used to describe how trade and technology have made the world into a more connected and interdependent place. Globalization also captures, in its scope, the economic and social changes that have come about as a result. Cheaper communication costs and the use of money service businesses or cryptocurrency have made it easier for fraudsters to transit between more than one country. For example, victims can be located in a specific country, while fraudulent call centres can be located in another country and the funds can go to a third or fourth country.

Data Breaches and Identity Theft: The proliferation of data breaches has exposed millions of individuals' personal and financial information leading to a surge of related fraud. Fraudsters use stolen data to impersonate victims or commit financial fraud. As a result, we require enhanced measures to protect sensitive information and prevent unauthorized access and use of such data.

Cryptocurrency: The rise of cryptocurrencies has created new opportunities for fraudsters to engage in scams such as Ponzi schemes, fake initial coin offerings (ICOs), and ransomware attacks. These crimes often exploit the anonymity and decentralized nature of cryptocurrencies.

Increased Awareness and Prevention Efforts: Over the years, there has been a growing awareness of fraud risks among the public and businesses. Organizations,

[1] https://www150.statcan.gc.ca/n1/daily-quotidien/060815/dq060815b-eng.htm#:~:text=An%20estimated%2016.8%20million%20adult,well%20below%20the%20national%20average.
[2] https://madeinca.ca/internet-statistics-canada/#:~:text=Internet%20Use%20in%20Canada,a%20penetration%20rate%20of%2093.8%25

like the CAFC, have played a crucial role in educating the public about common fraud schemes and promoting preventive measures to mitigate the risk of victimization.

Collaboration and Information Sharing: To combat the evolving nature of fraud, there has been a greater emphasis on collaboration and information sharing among law enforcement agencies, financial institutions, and other stakeholders. This collaborative approach greatly improves information sharing and best practices to more effectively identify, investigate, and prosecute fraudsters.

Artificial Intelligence :Fraudsters are increasingly using artificial intelligence (AI) and related technologies to perpetrate various forms of fraud. Some ways in which AI is being used by fraudsters, as observed by the Canadian Anti-Fraud Centre (CAFC) and other organizations, include:

Phishing and Social Engineering: AI can be used to personalize phishing emails and messages by analyzing data from social media and other sources, making them more convincing and difficult to detect by traditional spam filters.

Fraudulent Account Creation: AI algorithms can be used to automate the creation of fake online accounts for various purposes, such as conducting fraud, or engaging in identity crimes.

Data Analysis for Targeting: AI can analyze large datasets to identify potential targets for fraud, such as individuals with specific demographics or behavioral traits that make them more susceptible to certain fraud schemes.

Deepfake Technology: While not strictly AI, deepfake technology, which uses machine learning algorithms to create realistic fake videos or audio recordings, can be used for various fraudulent purposes; including impersonating celebrities and developing more targeted attacks.

QR Codes : The CAFC is receiving reports of fraudsters using QR codes in various scams to steal your personal information and/or money. Similar to fraudulent links or URLs, QR codes can be inserted into emails and texts to direct potential victims to fraudulent or malicious websites. Below are some of the variations we have seen:

Vendor Fraud
Victims selling items online are being targeted. Fraudsters will send a fake payment notification stating that the victim must scan the QR code in order to

receive the payment. If the victim scans the QR code, they will be asked for their online banking information; putting them at risk of identity fraud.

In another variation, fraudsters will send a QR code to the victim claiming that they are *sending* a payment but, in reality, it is a *request* for payment. When the victim enters their banking information, fraudsters will receive the payment or may gain access to the victim's bank account.

Cryptocurrency QR Codes

Fraudsters are taking advantage of Canadians' general lack of knowledge related to cryptocurrency. Fraudsters will ask for cryptocurrency as a payment method in many different types of fraud. In many cases, fraudsters will send a cryptocurrency address in the form of a QR code. Victims are then directed to scan it to make a payment. In the end, payments will be sent to crypto wallets controlled by the fraudsters.

Phishing

Fraudsters may claim to be a service provider, government agency, or financial institution. Instead of asking the victim to click on a link or download an attachment, fraudsters will instruct the victim to scan a QR code.

In summary, fraud has evolved significantly over the last 21 years, driven by technological advancements, globalization, and changing criminal tactics. To effectively combat fraud in this evolving landscape, we must all continue to adapt our strategies and collaborate with our networks to stay ahead of fraudsters' tactics.

Resources

CAFC Logo 

Video Library

https://www.youtube.com/channel/UCnvTfqttCb4K6wyVC6rMJkw/playlists

Fraud Prevention Material

The CAFC has fraud prevention material and posters available. If interested, please send your request to partners@antifraudcentre.ca.

Competition Bureau of Canada FPM 2025

https://competition-bureau.canada.ca/en/fraud-and-scams/fraud-prevention-month

Presentation

CAFC PowerPoint presentations are available by request to partners@antifraudcentre.ca.

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.

Statistics

In 2024, the CAFC received 108,878 fraud reports involving over $638 million in reported losses.

Top 10 frauds based on number of reports in 2024:

Fraud Type	Reports	Victims	Dollar Loss
Identity Fraud[3]	9,487	9,487	N/A
Service	5,049	3,831	$19.8M
Investments	4,076	3,866	$310.5M
Extortion	3,927	935	$21M
Personal Information[4]	3,902	3,021	N/A
Phishing[5]	3,390	3,021	N/A
Merchandise	3,225	2,735	$9.1M
Bank Investigator	2,770	1,456	$16.3M
Job	2,649	2,179	$47.1M
Counterfeit Merchandise	1,245	1,222	$0.4M

Top 10 frauds based on dollar loss in 2024:

Fraud Type	Reports	Victims	Dollar Loss
Investments	4,076	3,866	$310.5M
Spear Phishing	937	608	$67.2M
Romance	1,172	1,030	$58.4M
Job	2,649	2,179	$47.1M
Extortion	3,927	935	$19.8M
Service	5,049	3,831	$16.3M
Bank Investigator	2,770	1,456	$16.3M
Recovery Pitch	545	314	$9.1M
Merchandise	3,225	2,734	$9.1M
Vendor Fraud	760	508	$8.2M

Age Range Breakdown for 2024:

Age Range	Reports	Victims	Dollar Loss
Young Adults (39 and under)	12,490	10,259	$55M
Middle Agers (40-59)	11,275	8,411	$147.4M
Seniors (60+)	12,614	8,209	$178.9M
Businesses	1,634	1,118	$125.3M

[3-5] Scams soliciting personal information, and phishing do not involve financial losses and the majority of people who are victims of identity fraud are not responsible for the fraud losses.
NOTE: It is estimated that only **5-10%** of victims file a fraud report with the CAFC.

Reporting Fraud

A fraud can often carry on over an extended period of time and is a crime that can be 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 online 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.

Key Message and Slogan

Fraud: Recognize, Reject, and Report It.

Many frauds today are designed to play on a potential victim's emotions and get them to respond before they have an opportunity to reflect and research the information provided to them. They try to illicit responses based on panic, fear, curiosity, excitement, desperation, elation, or love; which are often escalated by presenting urgent situations requiring immediate action. This slogan for fraud prevention is geared toward getting Canadians 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 recommend people to slow down, to reflect and assess the situation before reacting. This can involve saying no, doing due diligence, researching, confirming information, and talking to family members and friends. We encourage people to take their time and to scrutinize all offers and demands.

Reporting fraud means sharing the information; even for unsuccessful attempts. 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:

Below are 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. Seek further advice from trusted resources.

- Is the call unsolicited? Was it expected or out of the blue?
- Is the matter urgent? Does it quire immediate action?
- Are they threatening legal action?
- 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, refund or trial?
- Are they claiming to be the police or investigating something?
- Does the email have an odd email address?
- Is the formatting strange?
- Are there spelling mistakes?
- Are you being asked to change your password despite not sending a request to do so?

Most Common Frauds

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 Extortion Scam: Targets receive recorded phone calls about their Social Insurance Number (SIN) being linked to fraudulent or criminal activity. The recorded message claims to be from a federal government or law enforcement agency and states that your SIN has been blocked, compromised or suspended. There may be threats of an arrest warrant or imprisonment, if the target 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.

Sextortion: Since 2022, there has been a substantial increase in sextortion reports, primarily targeting young adults. Victims are lured into an online relationship through social media or dating websites. As the communication becomes more intimate, victims are encouraged to appear and expose themselves on camera. They may also be asked to share nude photos. Eventually, the fraudster will threaten to release the explicit material (on social media, other online platforms or send it directly to their friends and/or family members) unless a sum of money is paid.

Fake Law Enforcement/RCMP Extortion Email: The fraudulent email asks you to download or open an attachment to view the fraudulent letter. After opening the attachment, the letter often contains law enforcement logos, names of high-ranking law enforcement officials and claims that you are accused of serious criminal charges. Suspects provide a fake law enforcement email address to respond to. After communicating with suspects, they will ask you to send a payment to avoid going to jail.

Hydro Extortion: A business or individual gets a call claiming to be from their hydro provider. The fraudster demands an immediate payment, typically via Bitcoin, or threatens that your 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 it often starts with a victim clicking on a malicious link, attachment or scanning a QR code. 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

- Do not open unsolicited emails.

- If an email contains one of your passwords, change it immediately.
- Always use a different password for every account.
- Do not scan QR codes from unknown sources.
- Law Enforcement will never threaten you by email and will not demand a payment
- Beware of unsolicited text messages and emails from individuals or organizations asking you to click on a link or attachment
- Do not download attachments as these can contain viruses or malware that may infect your device
- Contact the agency directly to verify the legitimacy
- Enable multi-factor authentication as an added layer of protection for your online accounts.
- Recognize that live streaming can be recorded and that pre-recorded video can be livestreamed.
- Familiarize yourself with social media privacy settings and consider limiting who has access to your personal information (i.e. friends list, location).
- Unless you know the person offline, there is no way to confirm who is on the other end.
- Trust your instincts, be skeptical and cautious.
- Never send money to someone you haven't met.
- Avoid sharing intimate images online
- Don't get sextorted, send a naked mole rat (www.dontgetsextorted.ca) thanks to CyberTip.ca, a program of the Canadian Centre for Child Protection.
- Learn more and protect yourself from sextortion
- Learn more tips and tricks for protecting yourself.

***For sextortion involving youth under 18, also report to www.cybertip.ca**; Canada's tip line for reporting online child sexual abuse and exploitation and dedicated to reducing child victimization through technology, education, public awareness, along with supporting survivors and their families.*

Romance and Relationship

Victims are typically contacted on dating websites or social media, it is common for suspects to use real pictures found on social media of real people (ie. business people, members of the military, family photos), pet photos and hobbies. Fraudsters quickly profess their love to gain their victims' trust, affection, and money. Once a connection is made victims will be asked to switch to a different method of communication such as Whatsapp, Signal and others. 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 never end up repaying the victim and continue to make empty promises while asking for more money.

Common reasons fraudsters request money:

- a personal/family emergency,
- claims they have no access to their existing funds,
- unexpected business expenses, legal expenses or professional fees,
- investing in a new business and they need the victims' help, and
- travel fees to return home.

Some recent variations include the use conversational attacks where fraudsters send random text messages to victims. The messages often read "where are you?", "where have you been?" or something similar. Once the victim responds, a conversation is started and the fraudster attempts to build a relationship with the victim.

Relationship Investment Fraud: In these cases, fraudsters develop a relationship with the victim and convince them to invest into a fraudulent cryptocurrency platform with the promise of large monetary returns. In fact, fraudsters may even let the victim cash out some of their investment returns only to get them to invest a larger amount. Suspects will "coach" victims on how to invest in their fraudulent crypto currency platforms. Unfortunately, once the victim requests to withdraw their investment, they are unable to do so.

New Variation – Crypto Thefts: A newer variation being reported is often referred to as "approval phishing". While "approval phishing" has existed for some time now, more recently this fraud tactic is being adopted by fraudsters engaged in romance and relationship frauds. Suspects develop a relationship with the victims and convince them to invest into crypto, they are then deceived into granting access to their cryptocurrency accounts by those posing as trusted services. After being coached on how to acquire cryptocurrency such as Etherium or Tron, a fake request is sent by fraudsters that appears to come from the crypto service, asking the user to "approve" access to their wallet. By clicking "approve," the individual unknowingly gives control of their funds to the third party. The fake requests closely mimic legitimate apps and services, making them look authentic to the user. In some cases, victims may receive a transfer request asking them to click on a link to accept and victims may unknowingly be providing the "approval" to access their wallet.

Warning Signs

Beware of:

- profiles that seem too perfect,
- someone you haven't met in person professes their love to you,
- a suspect that tries to move communication to a more private or different method of communication (email, text, social media platform, etc.),

- any attempts to meet in person get cancelled or there's always an excuse to not meet-up,
- a person who discourages you from talking about them to friends and family,
- a suspect acting distressed or angry to force you into sending more money,
- poorly written messages or messages addressed to the wrong name,
- an individual who "introduces" you to their family on social media to legitimize the relationship,
- Someone offering to "coach" you on crypto investing
- Emails appearing to be from a crypto service provider asking you to click on links
- Get rich quick investment opportunities.
- Be wary of individuals met on dating sites or social media who attempt to educate and convince you to invest into crypto currency.

How to Protect Yourself

- Don't give out your personal information (name, address, DOB, SIN, banking credentials).
- Don't accept friend requests from people you do not know.
- Don't invest your money in platforms provided by people you don't know.
- Never send money to someone you haven't met.
- Enable Multi-Factor Authentication (MFA) on your accounts.
- 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!**
- If you have granted a suspect access to your crypto account, follow the OPP's checklist to revoke the token approval.

Phishing and 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 agency). These messages will direct you to click a link for various reasons, 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.

Victims of phishing are putting themselves at risk for:

Identity Fraud:
After stealing your personal information, fraudsters can use your identity to:

- Access your bank accounts

- Open new bank accounts
- Transfer bank balances
- Apply for loans and credit cards
- Buy goods and services
- Hide their criminal activities
- Get passports or receive government benefits

Ransomware:
Most ransomware incidents start with an email phishing campaign. The email will contain an attachment which can be an executable file, an archive, an image or a link. Once the attachment is opened or the link is clicked, the malware is then released onto the user's system. The malware can remain dormant for many days or months before files or systems are encrypted or locked.

Spear Phishing:
In many cases, suspects can gather the information required for a spear phishing attack after accessing the victim's system through a phishing campaign.

Warning Signs - How to Protect Yourself

- Beware of unsolicited text messages and emails from individuals or organizations asking you to click on a link or attachment
- Watch for spelling mistakes
- Look at the hyperlink behind the link's text or button by hovering over the text
- When in doubt, do not click on links or attachments; they can contain viruses or spyware
- The Government of Canada will never send funds by email or text message.
- Forward phishing text messages to 7726 which can help cellphone providers identify smishing messages.

Spear Phishing

Spear phishing fraud, commonly known as Business Email Compromise, is one of the most prevalent frauds targeting businesses and organizations**.** In 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 and can 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, processes and dates.

Fraudsters launch their attack when the owner of the email account cannot be easily contacted by email or 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.
- Unusual payment request from a senior official.
- Pressure or a sense of urgency to complete transaction.
- Unusual requests that do not follow internal procedures.

How to Protect Yourself

- Remain current on frauds targeting business and educate all employees.
- Include fraud training as part of new employee onboarding.
- Put in place detailed payment procedures.
- Encourage a verification step for unusual requests.
- Establish fraud identifying, managing and reporting procedures.
- Avoid opening unsolicited emails or clicking on suspicious links or attachments.
- Take a few seconds 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.
- Routinely update computer and network software.
- Consider getting your business certified with CyberSecure Canada.

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 great discounts. Consumers may receive counterfeit products, lesser valued and 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 or below market value: Fraudsters will often advertise animals for free; often, puppies and kittens. 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

- Be cautious of blowout sales or greatly reduced prices (e.g. 80%).
- Beware of rental units that are listed below fair market value.
- Notice text with spelling errors or references to the product as “the item”.

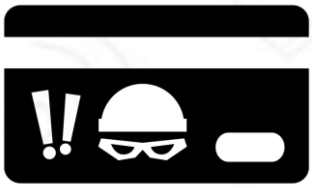
- Beware of pets being offered at below market value.

How to Protect Yourself

- Know the market value of the product you are looking for.
- Locate and verify the sellers contact information (address, phone number, email) before you buy.
- Look for customer reviews and ratings from third-party sources.
- Use a payment method with fraud protection (e.g. pay by credit card)
- Whenever possible, pick up items and provide the payment in person.
- Review all email information to make sure they are coming from a legitimate source.

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, such as a 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 and ultimately suffer the financial loss.

Fake VIN Report Websites: If you are selling a vehicle online, fraudsters may ask for a "VIN report" which provides an accident history of your vehicle. Fraudsters will send a link to a website that will ask for your credit card information to access the report. Once you provide your credit card information, your card can be used for fraudulent purchases or transactions

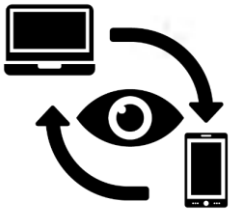
Warning Signs – How to Protect Yourself

- Beware of overseas buyers who want to buy without seeing the product first.
- Beware of overpayments for items you are selling.
- Beware of high-volume purchases that need to be shipped urgently.
- Never send money to get money.
- Do an online search to see if anyone has already reported the fraudulent buyer.

- Do your research and use reputable websites to purchase VIN reports.

Service

These frauds often involve offers for telecommunications, internet, finance, medical, and energy services. In addition, extended warranties, insurance and resales services may also fall under this category.



Tech Support: Consumers receive an email, 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.

Timeshare resale scams: A scammer calls with an offer to buy your timeshare. They promise a quick sale with a high profit margin. However, they ask for various fees up front before the final sale, including maintenance, escrow and taxes.

Home Repairs and 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.

Immigration: Online and social media ads are targeting victims looking to apply for a visa or immigrate to Canada. Fraudsters create fake websites which offer the immigration services or may even guarantee high paying jobs. The application will ask for your personal information and a payment to process the application.

Cellphone or existing service provider scam: Fraudsters call victims claiming to be from their cellphone service provider offering them a deal they "cannot pass on". The fraudsters proceed to ask for the victim's personal information including their Social Insurance Number (SIN) and Driver's License number in order to perform a "credit verification". In many cases, their personal information is used for identity fraud including having a cellphone ordered with their identity.

Warning Signs - How to Protect Yourself

- Be suspicious about unsolicited phone calls or pop-ups stating your computer/device is infected with a virus or a threat has been detected.
- Do not open or click on any link as malware could be installed.
- Always have your computer/device serviced by a reputable local business.

- Never allow an unknown person to gain remote access to your computer/device.
- Be wary of unsolicited offers to sell your timeshare. Do not agree to anything over the phone or online until you thoroughly research the buyer.
- Do your research and only use an accredited agency.
- Do not pay upfront fees! Many "businesses" claim to specialize in reselling timeshares. If you are interested in selling your timeshare, use a company that offers to sell for a fee after the timeshare is sold.
- If you receive a call from your service provider, advise them that you will call them back and end the call.
- Look up the legitimate phone number for the company and communicate with them directly by always making the outgoing call.
- Never provide personal information or banking details over the telephone unless you initiated the call.
- If you are asked to ship a cellphone, never ship it to an unknown address. If you are required to ship a cellphone, always send it to the verified address of your service provider.

Job

Fraudsters use popular job listing websites and social media sites 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.

"Boosting" Products, Apps or Videos: According to victim reports, fraudsters are contacting victims via text message, WhatsApp, email or Messenger after the victim has shared their resume and contact information on job recruitment websites. Using the names of real companies in Canada, the fraudsters are offering victims freelance job opportunities to "boost" products, apps or videos using software created by the fraudsters. After the victim installs the software and creates an account, they receive "orders" or "tasks" they have to complete. Victims might receive a small payment or commission in order to convince them that the job is legitimate. Victims can earn higher commissions or "move up a level" by boosting more products or videos but need to pay fees to gain access to the additional work. Victims deposit their funds into crypto accounts or wallets. Victims may also be asked to recruit other victims in order to increase their earnings. Similar to crypto investment scams, victims will see funds in their crypto account, but will not have the ability to withdraw the funds they have deposited and earned.

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.
- Fraudsters will oftentimes slightly alter the domain of a legitimate company in order to convince victims that they are communicating with a legitimate company.
- If you are asked to "boost" apps, videos or merchandise, you will more than likely be providing fake reviews to fraudulent products.
- Be careful when sending cryptocurrency. Once the transaction is completed, it is unlikely to be reversed.
- If you are asked to recruit, remember that pyramid selling is illegal in Canada. It's a criminal offence to establish, operate, advertise or promote a scheme of pyramid selling.
- If a job sounds too good to be true, it probably is.

Investment Scams

Investment scams were the highest reported scams based on dollar loss for the past four years. This scam is 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.

Crypto Investment Scams: The majority of the investment scam reports involve Canadians investing in crypto currency after seeing a deceptive advertisement. These scams typically involve victims downloading a trading platform and transferring crypto currency into their trading account. In many cases, fraudsters will send a cryptocurrency address in the form of a QR code. Victims are then directed to scan it to make a payment. In the end, payments are sent to crypto wallets controlled by the fraudsters and 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:

- In some cases, the scam starts as a relationship or romance scam and quickly turns into an "investment opportunity". Because suspects have gained the victim's trust, it can lead to significant financial losses 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 in 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.

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.

Brand Spoofing Investment Frauds: This fraud involves Canadians receiving fraudulent offers that appear to come from the actual companies offering higher than normal returns on fixed income investment products such as Guaranteed Investment Contracts (GIC) and saving bonds. Typically, these offers materialize after a consumer searches for an investment opportunity online and enters their information into an "investment finder" type ad. Consumer will then receive calls from the fraudulent operators claiming to be a legitimate company and offering a high return fixed income opportunity.

For any investment opportunities, investors are urged to verify information by looking up the company's website directly and/or calling the company at the phone number listed on its website. Do not rely on the website and phone number included in the unsolicited materials provided to you.

What is a GIC?
A Guaranteed Investment Contract (GIC) is a financial product normally between an investment and insurance company which guarantees a return. A GIC is normally used for retirement.

What is a Savings Bond?
A fixed income investment that allows you to earn a return on your investment by lending to the issuer for a period of time.

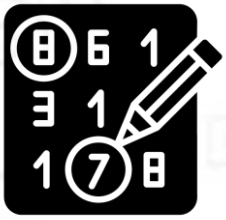
Warning Signs – How to Protect Yourself

- Be careful when sending cryptocurrency; once the transaction is completed, it is unlikely to be reversed.
- Be wary of individuals met on dating sites or social media who attempt to educate and convince you to invest into crypto currency.
- Canadians need do their research to ensure they are using reputable and compliant services.

- 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
- Prior to investing, ask for information on the investment. Research the team behind the offering and analyze the feasibility of the project
- Some fraudsters will use the name of legitimate companies to lend credibility to the fraud and convince victims to send money. Verify email addresses, URL's, phone numbers and their physical address.
- Verify if the investment companies are registered with your Provincial Securities Regulator or the National Registration Search Tool (www.aretheyregistered.ca).
- If you receive a suspicious or odd investment related message from a trusted friend, reach out to them through a different means of communication to confirm that it is them.
- 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!**
- Question why someone is reaching out to you about an investment offer: Is this a conversation I would usually have with an unknown person? Does it make sense to invest in an opportunity based on the communication I had? Should I feel pressure or urgency when deciding to invest?

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 or drug offence, 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.

Warning Signs - 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.

Bank Investigator

Victims are contacted by fraudsters claiming to be from a financial institution, law enforcement or an online merchant. Suspects claim that there have been suspicious and unauthorized charges on your credit card or funds have been stolen out of your bank account. They then state they need your credit card or bank card information including PIN number to stop the fraud.

In some cases, suspects will request access to the victims' computer to continue the "investigation". Victims are then shown a fraudulent transaction on their online bank account. The fraudsters state they want the victims' help in an ongoing "investigation" against the criminals who stole their money and request that the victims send funds as part of the "investigation".

Other Common Variations:

1) Fraudsters will convince victims that in order to protect their account until a new debit card is issued, the victim must send an Interac e-transfer transaction to their own cellphone number. The suspect will instruct the victim on the steps required to add themselves as a payee and to increase their daily Interac e-transfer limit to $10,000 (note that the maximum amount that a sender may send through the Interac e-transfer network may vary depending on the sender's financial institution. Interac will automatically refuse to complete any payment by a sender above the limit established by the financial institution). The suspect provides the e-transfer question and answer that the victim must use for the transfer. Once the victim sends the Interac e-transfer transaction to their own cellphone number, suspects will ask the victim for a "code" which is the last portion of the Interac e-transfer URL/link received. If the victim provides the URL, suspects will have the ability to deposit the funds into their own account.

2) Fraudsters go to the victim's residence in person to pick up their bank cards. Some recent reporting identified victims being directed to put their bank card and PIN number in an envelope and place on their front steps for pick-up by an "investigator". Fraudsters retrieve the card and proceed to complete unauthorized transactions.

In all variations, suspects may provide some of the victim's personal information which might include name, date of birth, phone number, address and debit card number to make the call seem legitimate. Additionally, suspects are spoofing financial institution phone numbers or are providing fraudulent call-back phone numbers which impersonate the financial institution.

Warning Signs – How to Protect Yourself

- Criminals use Call-Spoofing to mislead victims. Do not assume that phone numbers appearing on your call display are accurate.

- If you get an incoming call claiming to be from your financial institution, advise the caller that you will call them back. End the call and dial the number on the back of your bank debit card from a different phone if possible or wait 10 minutes before making the outgoing call.
- Never provide details of links or URL's received via text message or email to fraudsters.
- Don't share codes received via text message or email with anyone. In most cases, these are multi-factor authentication codes that will give fraudsters access to your account.
- Fraudsters will often provide the first 4 to 6 numbers of your debit or credit card. Remember that these numbers are used to identify the card issuer and are known as the Bank Identifier Number (BIN). Most debit and credit card numbers issued by specific financial institutions begin with the same 4 to 6 numbers.
- If your personal information has been compromised in the past through a breach or a phishing message, remember that the information can be used as a tool to make the communication appear legitimate.
- Never provide remote access to your computer.
- Financial institutions or online merchants will never request transferring funds to an external account for security reasons.
- Financial institutions or police will never request you to turn over your bank card nor attend your residence to pick up your bank card.
- Enabling Auto-Deposits for Interac e-transfers provides additional layer of security

Identity Theft and Identity Fraud

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 or a database breach.

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

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**
  - **TransUnion Canada**
- **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 and any service providers.
- **Step 8:** Notify federal identity document issuing agencies:
  - **Service Canada**
  - **Passport Canada**
  - **Immigration, Refugees and Citizenship:**
- **Step 9:** Notify provincial identity document issuing agencies.

Cutting Contact with the Fraudsters

All fraudsters have their *tricks of the trade and toolboxes*. 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

In the last 150 years, the telephone has evolved to today's mobile device that fits in your pocket and allows you to call anyone across the globe. In 2024, telephone calls remained 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 centers. Fraudsters may use lists of phone numbers (gained legally or illegally) or they may setup the dialer to call all possible configurations of phone numbers 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 computerized/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** (DNCL), this should filter out a large number of unsolicited calls. The 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 relationship. If the recorded message you hear does not fall under these 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 (i.e. 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

- 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. Hang up if the caller cannot or will not answer.
- If you're still unsure about the call, talk to someone you trust 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

- 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 (i.e. @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. They may simply change an "m" with "rn".
- If an email or text message includes a sense of urgency, this is a red flag.
- 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 as fraudulent. Fraudsters create websites for a number of frauds. They're 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

- 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 (i.e. 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 applications are included within this contact method.

Fake Accounts: Fraudsters will create their accounts typically using stolen photos and information from legitimate people. In 2019, Facebook announced that, between January and March, it removed 2.19 billion fake accounts from their platform[5].

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 victims. 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

- Do not accept requests from people you do not know. You do not know if they have malicious intent.
- Be wary of profiles that seem perfect in their photos.
- Complete a reverse image search to see where the same photo is being used online. https://images.google.com and https://tineye.com are great options.
- Ask specific questions and look for inconsistencies in the responses.
- Be wary of those who always have an excuse as to why you cannot meet in person.
- Never send money to someone you haven't 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.

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

- Do not click on suspicious links.
- Adjust your social account privacy settings from Public to a more restricted option.
- Do not overshare sensitive information (i.e. 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. Enable two factor or multi factor authentication.
- 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 years.

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

- You can reduce the amount of mailed marketing offers you receive by registering with the Canadian Marketing Association's Do Not Mail Service. 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.

Keeping Your Money in Your Wallet

In 2024, fraudsters asked for the following payment methods most frequently:

Wire Transfer

A wire transfer is the electronic transfer of funds between financial institutions. 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). 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 have become a prevalent payment method in fraud. 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 its owner immediately. Some ATMs have scheduled delayed deposits.

Credit Card

Credit cards remain the top reported payment mechanism for many online merchandise frauds. It is important to use a major credit card when shopping online as these may offer higher levels of purchase protection. For instance, if you have received counterfeit goods or lesser quality product, a different product or nothing at all, dispute the associated charges with your credit card provider. Make sure to review your terms of service on your credit card carefully.

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. These mules transfer money for others (aka money laundering). 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 a "friend".

Prepaid Gift Cards

Prepaid gift cards are a popular and convenient way to give someone a gift but should not be used for payments. Highly adopted by fraudsters who commonly pose as government agencies, law enforcement, or service providers when making requests for gift card payments. 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)/ E-Transfer

Similar to wire transfers, email money transfers are made between two bank accounts. The sender initiates the transfer through their online bank 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 recalling 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 since some transactions 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 to help Canadians be fraud aware and cyber secure in 2023.

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 keeping your operating system and security software 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 addresses
    - 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.
- ✓ Get your small or medium-sized business CyberSecure Certified: Get started (canada.ca)