CANADIAN ANTI-FRAUD CENTRE BULLETIN

2021 Fraud Prevention Toolkit - Businesses 2021-02-15

FRAUD: RECOGNIZE, REJECT, REPORT

BUSINESSES

2021 Fraud Prevention Toolkit

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

Table of Contents

Introduction

As fraud rates continue to increase in Canada, the world is going through a global pandemic. The COVID-19 has created an environment that is ripe for fraud and online criminal activity. The COVID-19 has resulted in never-before-seen numbers of people turning to the internet for their groceries, everyday shopping, banking and companionship. Coupled with the profound social, psychological and emotional impacts of COVID-19 on people, one could argue that the pool of potential victims has increased dramatically.

March is Fraud Prevention Month. This year's efforts will focus on the Digital Economy of Scams and Frauds.

The Canadian Anti-Fraud Centre (CAFC) has compiled a toolkit specifically designed for use by businesses to further raise public awareness and prevent victimization. We encourage all our partners to use the resources in this toolkit on their website, in print and on their social media platforms.

Throughout the year, the CAFC will be using the #kNOwfraud and #ShowmetheFRAUD descriptors to link fraud prevention messaging. We will also continue to use the slogan "Fraud: Recognize, Reject, Report".

During Fraud Prevention Month, the CAFC will post daily on its Facebook and Twitter platforms (#FPM2021). Our weekly bulletin will be published every Monday and, every Wednesday, we will host a #FraudChat at 1 p.m. (Eastern Time) on Twitter. Everyone is invited to join the conversation.

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

Thank you,

Your CAFC Fraud Prevention Team

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

This Toolkit Includes:

1) RCMP Videos

The Face of Fraud https://www.youtube.com/watch?v=0rlWUcc57dM
French: https://www.youtube.com/watch?v=cXXP35rICQY
A Cry from the Heart from Victims
https://www.youtube.com/watch?v=blyhHl8rc7g
French: https://www.youtube.com/watch?v=cHZfvpH2YW8
Telemarketing Fraud: The Seamy Side
https://www.youtube.com/watch?v=t7bhQJkelEg
French: https://www.youtube.com/watch?v=XteG_fdasdw

2) OPP Videos

Fraud Prevention Month Playlist
https://www.youtube.com/playlist?list=PLbecW3cjtFJ4gxFvi9vuGlh8hJR13y1-c
Senior Internet Scams Playlist
https://www.youtube.com/playlist?list=PLbecW3cjtFJ6jyMpBlsY1NQkrj0-59Kp2
French: https://www.youtube.com/user/OPPCorpCommFR/search?query=fraude

3) Competition Bureau of Canada Videos

Mass marketing fraud can take many forms. These videos help describe the way they work and how to avoid victimization. Videos are available in both official languages.
https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04272.html
https://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/04272.html

4) CAFC Fraud Prevention Video Playlists

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

5) CAFC Logo

6) Calendar of Events

Throughout the month of March, the CAFC will release a bulletin every Monday aimed at Recognizing Fraud and highlighting our weekly themes tied to the Digital Economy of Scams and Fraud. Every Wednesday, we will host a Twitter #FraudChat at 1 p.m. (Eastern Time) providing advice on breaking the contact with fraudsters.

Bulletins
Week 1: Buying and Selling Online
Week 2: Online Financial Scams
Week 3: Securing Your Accounts and Your Identity
Week 4: Email Scams
Week 5: Online Scams

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

On a daily basis, the CAFC will highlight a fraud topic on our social media accounts.
Like us on Facebook – Canadian Anti-Fraud Centre
Follow us on Twitter – @canantifraud

On **March 2, 2021** - Join us on Facebook for a live 13-hour Canada-wide Fraud Prevention Month launch event.

March 2021

Mon., March 1 Facebook & Twitter Bulletin - Buying & Selling Online	**Tues., March 2** Facebook **13-HR LIVE LAUNCH**	**Wed., March 3** Facebook & Twitter Puppy Scams **1 p.m. Eastern** #Fraudchat	**Thurs., March 4** Facebook & Twitter Rental Scams	**Fri., March 5** Facebook & Twitter Merchandise and Counterfeit scams
Mon., March 8 Facebook & Twitter Bulletin -Financial Scams	**Tues., March 9** Facebook & Twitter Investment Scams	**Wed., March 10** Facebook & Twitter Loan Scams **1 p.m. Eastern** #Fraudchat	**Thurs., March 11** Facebook & Twitter Grant Scams	**Fri., March 12** Facebook & Twitter Job Scams
Mon., March 15 Facebook & Twitter Bulletin -Protecting Your Information	**Tues., March 16** Facebook & Twitter Id Theft and Fraud	**Wed., March 17** Facebook & Twitter Social Media Scams **1 p.m. Eastern** #Fraudchat	**Thurs., March 18** Facebook & Twitter Securing your Accounts	**Fri., March 19** Facebook & Twitter Ransomware
Mon., March 22 Facebook & Twitter Bulletin – Email and Text Message Scams	**Tues., March 23** Facebook & Twitter Phishing	**Wed., March 24** Facebook & Twitter Spear Phishing **1 p.m. Eastern** #Fraudchat	**Thurs., March 25** Facebook & Twitter Extortion Scams	**Fri., March 26** Facebook & Twitter Prize Scams
Mon., March 29 Facebook & Twitter Bulletin – Prevalent Online Scams	**Tues., March 30** Facebook & Twitter Romance Scams	**Wed., March 31** Facebook & Twitter Immigration scams **1 p.m. Eastern** #Fraudchat	**Thurs April 1** Facebook & Twitter Fraud is no joke	

7) About the CAFC

The CAFC is Canada's central repository for information about fraud. We help citizens and businesses:

- report fraud;
- learn about different types of fraud;
- recognize the warning signs of fraud;
- protect themselves from fraud.

The CAFC does not conduct investigations but provides valuable assistance to law enforcement agencies by identifying connections all over the world. Our goals include:

- disrupting crime;
- strengthening the partnership between the private and public sectors;
- maintaining Canada's economy.

The CAFC is jointly managed by the Royal Canadian Mounted Police, the Competition Bureau, and the Ontario Provincial Police.

8) Statistics

In 2020, the CAFC received 101,483 fraud reports involving nearly $160 million in reported losses. Moreover, 2,190 of the reports were from Canadian businesses, that reported losses totalling more than $24.5 million.

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

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

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

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

➔ It is estimated that fewer than **5%** of victims file a fraud report with the CAFC.

9) Reporting Fraud

Fraud is evolving. A fraud can often carry on over an extended period of time and is a crime that is difficult to recognize and report. To make reporting easier the CAFC suggests completing the following six steps:

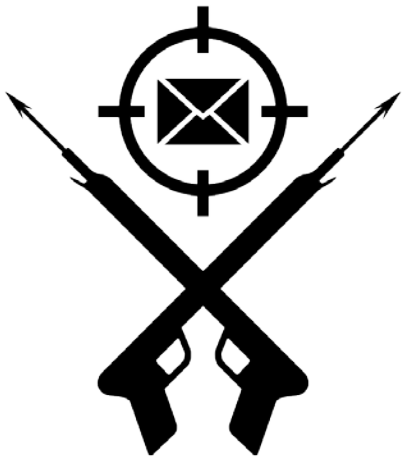
Step 1: Gather all information pertaining to the fraud.
Step 2: Write out a chronological statement of events.
Step 3: Report the incident to your local law enforcement.
Step 4: Report the incident to the CAFC through the Fraud Reporting System (FRS) or toll free at 1-888-495-8501.
Step 5: Report the incident to the Financial Institution or Payment Provider used to send the money.
Step 6: If the fraud took place online, report the incident directly to the appropriate website.

10) Most Common Frauds & How to Protect Yourself

Below are the most common frauds affecting Canadian businesses:

Spear Phishing

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



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

Common Variations

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

Warning Signs

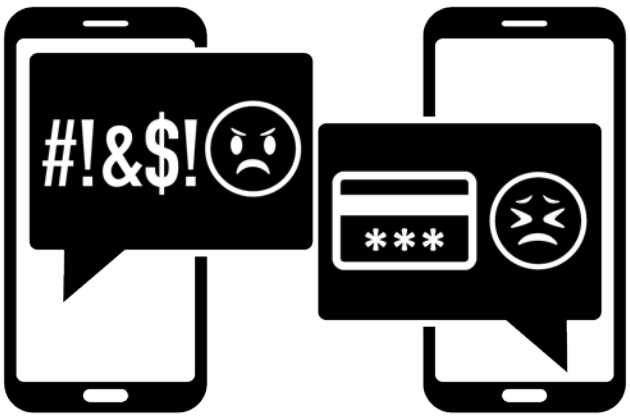
- Unsolicited emails.
- Direct contact from a senior official you are not normally in contact with.
- Requests for absolute confidentiality.
- Pressure or a sense of urgency.
- Unusual requests that do not follow internal procedures.
- Threats or unusual promises of reward.

How to Protect Yourself

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

Extortion

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



Hydro: The business receives a call claiming to be from their hydro provider. The fraudster demands an immediate payment, typically via Bitcoin, or their power will be disconnected.

Ransomware: A type of malware designed to infect or block access to a system or data. A device can be infected by a malware in a number of ways; but, most commonly, it starts with a

victim clicking on a malicious link or attachment. At present, the most common form of ransomware will encrypt data. Once the system or data is infected, victims will receive the demand for ransom. There may also be threats of distributing the data publicly if the ransom is not paid.

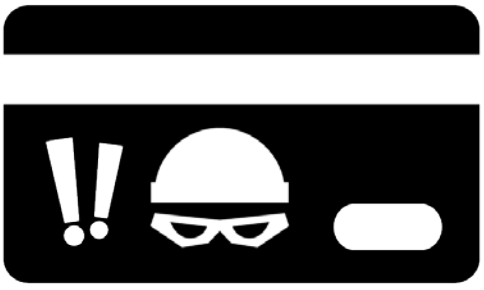
Warning Signs – How to Protect Yourself

- Be familiar with your service provider's terms of service.
- Contact your service provider directly and verify that your account is in good standing.
- Do not open unsolicited emails and text messages.
- Do not click on suspicious links or attachments.
- Regularly back-up important files.
- Keep your operating system and software updated.
- Paying a ransom request does not guarantee that your files and devices will be restored. Fraudsters may continue to request additional funds.
- Have your systems reviewed by local technicians.
- Report any database breach as per Canada's federal private sector privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA).

Vendor Fraud

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

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



Warning Signs

Customer Flags

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

Product / Order Flags

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

Delivery Flags

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

How to Protect Yourself

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

Purchase of Merchandise or Service

Businesses must do their due diligence before purchasing products or services from new and unknown suppliers. Fraudsters may place advertisements on popular classified sites or send their advertisements by mail or fax. They may also easily create websites that share the look and feel of legitimate manufacturers. Fraudsters will generate traffic to their products by advertising them at deep discounts. Buyers may receive counterfeit products, lesser valued & unrelated goods, or nothing at all.

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

Warning Signs – How to Protect Yourself

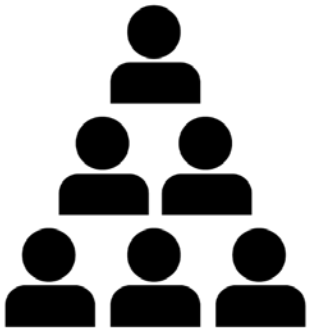
- If it sounds too good to be true, it probably is.
- Verify the URL and seller information's legitimacy.
- Search for any warnings posted online and read reviews before making a purchase.
- Spelling mistakes and grammatical errors are indicators of a fraudulent website.
- Use a credit card when shopping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

Investment

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

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

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



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

Warning Signs – How to Protect Yourself

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