CANADIAN ANTI-FRAUD CENTRE

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

BUSINESSES

2022 Fraud Prevention Toolkit

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

Table of Contents

Introduction	---	3
RCMP Videos	---	4
OPP Videos	---	4
Competition Bureau of Canada Videos	---	4
CAFC Fraud Prevention Video Playlists	---	4
CAFC Logo	---	4
Calendar of Events	---	5
About the CAFC	---	7
Statistics	---	7
Reporting Fraud	---	8
Most Common Frauds Targeting Businesses	---	8
• Spear Phishing	---	9
• Extortion	---	10
• Vendor Fraud	---	11
• Purchase of Merchandise or Service	---	13
• Loan	---	14
Be Fraud Aware and Cyber Safe Checklist	---	15

Introduction

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

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

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

Thank you,

Your CAFC Fraud Prevention Team

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

This Toolkit Includes:

1) RCMP Videos

The Face of Fraud 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

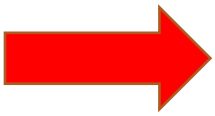
3) Competition Bureau of Canada Videos

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 week aimed at highlighting the top impersonation scams reported to CAFC in 2021.

Bulletins

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

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

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

March 2022

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

7) About the CAFC

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

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

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

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

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

8) Statistics

In 2021, the CAFC received 104,295 fraud reports involving over $379 million in reported losses. Moreover, 2,368 of the reports were from Canadian businesses, that reported losses totalling more than $72.2 million.

Top 10 frauds affecting businesses based on number of reports in 2021:

Fraud Type	Reports	Victims	Dollar Loss
Spear Phishing	531	239	$49.3 M
Extortion	309	99	$0.4 M
Vendor Fraud	301	209	$3.0 M
Service	150	72	$1.1 M
Job	109	33	$5.3 M
Merchandise	108	77	$4.5 M
Phishing	66	10	N/A
False Billing	45	9	$0.07 M
Foreign Money Offer	26	0	0
Loan	21	17	$5.6M

Top 10 frauds affecting businesses based on dollar loss in 2021:

Fraud Type	Reports	Victims	Dollar Loss
Spear Phishing	531	239	$49.3 M
Loan	21	17	$5.6 M
Job	109	33	$5.3 M
Merchandise	108	77	$4.5 M
Vendor Fraud	301	209	$3.0 M
Investments	29	16	$1.7 M
Service	150	72	$1.1 M
Extortion	309	99	$0.4 M
Recovery Pitch	2	2	$0.3 M
Grant	4	2	$0.1 M

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

9) Reporting Fraud

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

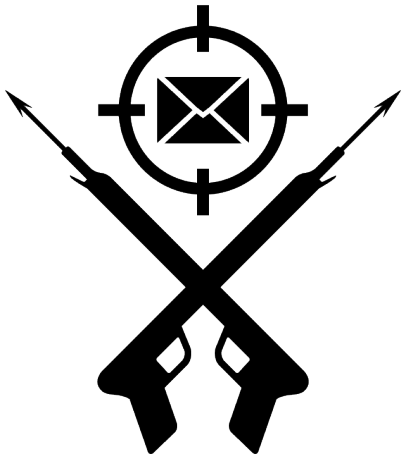
Step 1: Gather all information pertaining to the fraud.
Step 2: Write out a chronological statement of events.
Step 3: Report the incident to your local law enforcement.
Step 4: Report the incident to the CAFC through the Fraud Reporting System (FRS) or toll free at 1-888-495-8501.
Step 5: Report the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

10) Most Common Frauds & How to Protect Yourself

Below are the most common frauds affecting 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

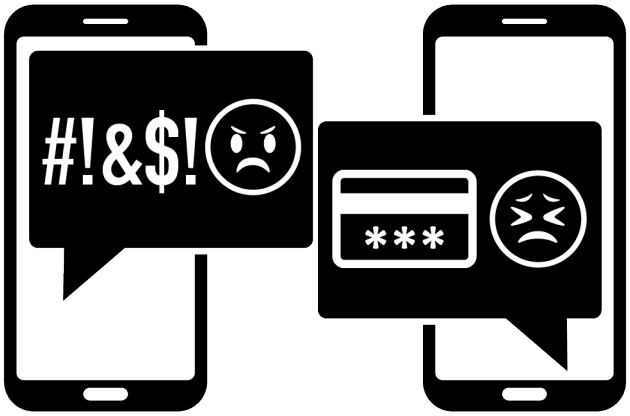
- Unsolicited emails.
- Direct contact from a senior official you are not normally in contact with.
- Pressure or a sense of urgency.
- Unusual requests that do not follow internal procedures.
- Threats or unusual promises of reward.

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.

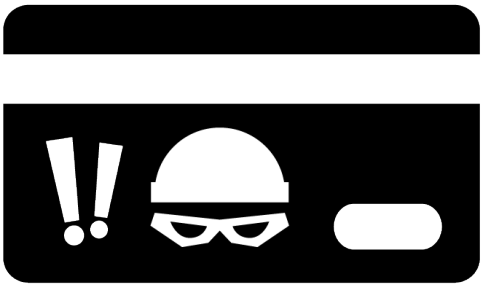
Warning Signs – How to Protect Yourself

- 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.

Loan

Many Canadians are experiencing financial hardship as a consequence of the current pandemic. While funding options are available through the Government of Canada, some Canadians are looking for loans. Unfortunately, the reporting of fraudulent loan websites is increasing.

These websites are designed to look like legitimate lending institutions. Their fraudulent loan applications are used to collect your personal information. This can result in identity theft and fraud. Once quickly approved, the fraudsters will request a fee to secure the loan. The victim never receives any money.

Warning Signs – How to Protect Yourself

- In most provinces, it is illegal for a company to request an upfront fee before you receive your loan. You should never send money first.
- Beware of companies that offer guaranteed loans; even if you have bad credit or no credit.
- Beware of instant approvals.
- Do your research before you provide your personal information.
- Contact your provincial consumer protection agency and/or financial regulator to confirm that a company is a legitimate lender.
- End all contact if the company requests payment by email money transfer, money service businesses or pre-paid credit cards.

Be Fraud Aware and Cyber Secure

- ✓ Train your employees about cyber security and fraud
- ✓ Have policies or a plan in place to help employees
- ✓ Know who you're dealing with. Consider compiling a list of companies your business uses to help employees know which contacts are real and which aren't.
- ✓ Watch out for invoices using the name of legitimate companies. Scammers will use real company names like Yellow Pages to make the invoices seem authentic. Make sure you inspect invoices thoroughly before you make a payment.
- ✓ Don't give out information on unsolicited calls or to unsolicited emails
- ✓ Educate employees at every level to be wary of unsolicited calls. If they didn't initiate the call, they shouldn't provide or confirm any information, including:
    - The business address
    - The business phone number
    - Any account numbers
    - Any information about equipment in the office (e.g., make and model of the printer, etc.)
- ✓ Limit your employees' authority by only allowing a small number of staff to approve purchases and pay bills.
- ✓ Beware of spear phishing. Have policies in place to verbally confirm requests for urgent wire transfers or purchases.
- ✓ Review potentially fraudulent orders. Watch for:
    - Larger than normal orders
    - Multiple orders for the same product
    - Orders made up of "big-ticket" items
    - Use of multiple credit cards to pay
- ✓ Review the Get Cyber Safe guide for businesses. Consider getting your business certified with CyberSecure Canada.