2020 Fraud Prevention Toolkit :

Businesses

#KNOWFRAUD
#SHOWMETHEFRAUD
Fraud: Recognize. Reject. Report.

Table of Contents

Introduction

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 encourage our partners to make use of these hashtags as well as #Take5 and #Tell2, protect many. Take Five is a successful national campaign that was first launched by UK Finance; it encourages consumers to pause, reflect and not react under the pressure of fraudsters. #Tell2 is a movement that was started by D.C. Tony Murray from Durham Fraud (UK). The initiative asks consumers to prevent fraud by sharing anti-fraud messaging with at least two people and encouraging them to do the same. An unbroken chain of 25 Tell2'ers would cover the entire population of Canada.

During Fraud Prevention Month (March), the CAFC will post daily on its Facebook and Twitter platforms (#FPM2020). Our weekly bulletin will be published every Monday and, every Wednesday, we will host a #FraudChat at 1PM Eastern on Twitter. Everyone is invited to join the conversation.

The CAFC is Canada's central repository for data, intelligence and resource material as it relates to fraud. The CAFC does not conduct investigations but provides valuable assistance to law enforcement agencies by identifying connections all over the world. Victims who report to the CAFC are also encouraged to report directly to their local police. The information provided may be the piece that completes the puzzle.

Consumers and businesses can report directly to the CAFC through our online Fraud Reporting System (FRS) or toll free at 1-888-495-8501.

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

Thank you,
The 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. Every Wednesday, we will host a Twitter #FraudChat at 1PM (Eastern). Both will be based on the following weekly fraud prevention themes:

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

On a daily basis, the CAFC will highlight a "Fraud of the Day" on our social network accounts. See the calendar below for more details.

On **March 2, 2020** - Join us on Facebook for a live 13-hour Canada-wide Fraud Prevention Month launch event.

March 2020

Sun	Mon	Tue	Wed	Thu	Fri	Sat
1 Tools used by Fraudsters	2 **13-HR LIVE LAUNCH** **Bulletin**	3 Personal Information	4 Charity **#Fraudchat**	5 Payment Methods	6 Prize	7 Vacation
8 Phishing	9 ID Theft & Fraud **Bulletin**	10 Spear Phishing	11 Extortion **#Fraudchat**	12 Ransomware	13 SIM Swap	14 Emergency
15 Subscription Traps	16 Job **Bulletin**	17 Sale of Merchandise	18 Merchandise **#Fraudchat**	19 Card-Not-Present	20 Investment	21 Rental
22 Stay Safe Online	23 Puppy **Bulletin**	24 Service	25 Pyramid **#Fraudchat**	26 Grant	27 Romance	28 Sextortion
29 Inheritance	30 Overpayments **Bulletin**	31 Brand Protection	April 1 Fraud is no joke **#Fraudchat**			

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

7) Statistics

In 2019, the CAFC received 46,465 fraud reports from Canadian consumers and businesses. The total reported Canadian losses were $96,163,328.64. The top 10 frauds reported during this time are listed below.

Top 10 business scams based on number of reports in 2019:

Fraud Type	Reports	Victims	Dollar Loss
Spear Phishing	452	204	$20,131,958.34
Extortion	285	55	$91,656.81
Sale of Merchandise	277	170	$1,268,287.68
Service	143	41	$381,026.04
Directory	85	7	$4,964.56
Spoofing	74	38	
Personal Info	58	15	
False Billing	32	5	$8,515.70
Merchandise	28	21	$125,430.15
Fraudulent Cheque	26	16	$43,070.04

Top 10 business scams based on dollar loss in 2019:

Fraud Type	Reports	Victims	Dollar Loss
Spear Phishing	452	204	$20,131,958.34
Sale of Merchandise	277	170	$1,268,287.68
Service	143	41	$381,026.04
Merchandise	28	21	$125,430.15
Extortion	285	55	$91,656.81
Fraudulent Cheque	26	16	$43,070.04
Counterfeit Merchandise	9	3	$21,703.80
False Billing	32	5	$8,515.70
Directory	85	7	$4,964.56
Loan	13	3	$4,675.00

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

8) Reporting Fraud

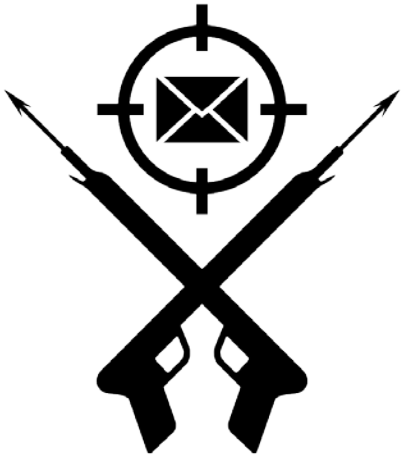
In an effort to mitigate the impact of fraud, the CAFC suggests following the six steps below.

Step 1: Gather all information pertaining to the fraud.
Step 2: Report the incident to your local law enforcement.
Step 3: Report the incident to the CAFC through the Fraud Reporting System (FRS) or toll free at 1-888-495-8501.
Step 4: Report the incident to the Financial Institution or Payment Provider used to send the money.
Step 5: If the fraud took place online, report the incident directly to the appropriate website.
Step 6: Follow the RCMP Identity Theft and Fraud Assistance Guide: http://www.rcmp-grc.gc.ca/scams-fraudes/victims-guide-victimes-eng.htm

9) Common Frauds & How to Protect Yourself

Below are a few common frauds affecting 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

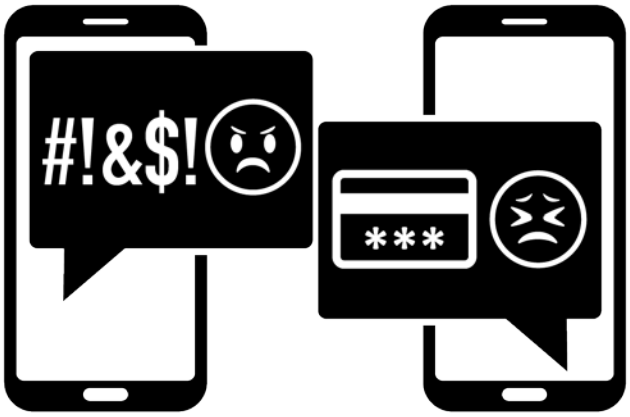
- Unsolicited emails
- Direct contact from a senior official you are not normally in contact with
- Requests for absolute confidentiality
- Pressure or a sense of urgency
- Unusual requests that do not follow internal procedures
- Threats or unusual promises of reward

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.

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).

Sale of Merchandise or Service

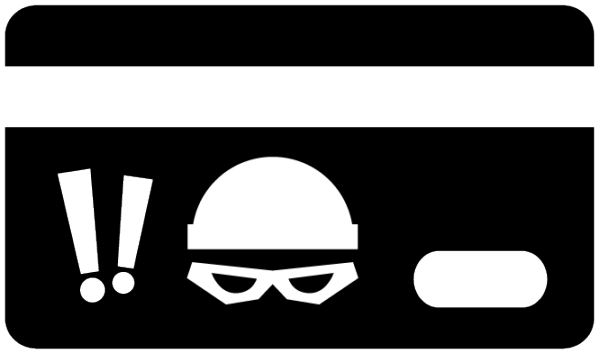
Business selling merchandise or offering their services online are at risk of receiving fraudulent payments. In many cases, victims will receive an overpayment with instructions to forward the difference to a third party (i.e. shipping company) to complete the transaction. Victims that comply are subsequently 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 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.

Directory Scam

Businesses receive an invoice for an unauthorized directory listing or publication. Typically, this fraud starts with a call to the business looking to confirm the company's contact information. The fraudsters may record the initial conversation and manipulate the recording to make it seems as though an order was placed.

Warning Signs – How to Protect Yourself

- Educate employees at every level to be wary of unsolicited calls.
- Compile a list of authorized service providers for your business.
- Fraudsters will use legitimate company names (ie. Yellow Pages) to make their invoices seem authentic. Inspect invoices thoroughly prior to making payment.


Canadian Anti-Fraud Centre
C A F C
Centre antifraude du Canada
FRAUD: RECOGNIZE IT. REPORT IT. STOP IT.
LA FRAUDE : IDENTIFIEZ-LA. SIGNALEZ-LA. ENRAYEZ-LA.
Competition Bureau Canada
Bureau de la concurrence Canada
Royal Canadian Mounted Police
Gendarmerie royale du Canada
Canada