



# CANADIAN ANTI-FRAUD CENTRE BULLETIN

The 12 Scams of the Holidays

2021-11-30

FRAUD: RECOGNIZE, REJECT, REPORT

The spirit of the holidays is a time of giving for most but, for scammers, it is a time of taking. The Canadian Anti-Fraud Centre highlights the most popular holiday scams so that you can recognize, reject, report and be merry.

- 1) Counterfeit Merchandise** – Look out for huge and flashy discount ads that direct you to websites that look like the legitimate manufacturer's. If you do receive any inferior product, they could pose significant health risks.
- 2) Selling Goods & Services Online** – Be suspicious of payment offers that are more than the asking price and confirm that you have received a legitimate payment before you send the product.
- 3) Crypto Investments** - Fraudsters are using social media and fraudulent websites. Prior to investing, ask for information on the investment. Research the team behind the offering and analyze the feasibility of the project. Verify if the company is registered by using the National Registration Tool ([www.aretheyregistered.ca](http://www.aretheyregistered.ca)).
- 4) Romance Scams** – An attractive fake identity lures you into their web of lies spun with loving messages and sweet promises. The fraudsters play on your emotions to maximize their payday over time.
- 5) Online Shopping** – Fraudsters pose as genuine sellers and post fake ads for items that do not exist. The listing price for almost any item (e.g. event ticket, rental, vehicle, puppy) is usually too good to be true. Research before you buy. Whenever possible, exchange goods in person or use your credit card for payment.
- 6) Phishing Emails and Texts** – You may receive messages claiming to be from a recognizable source (e.g. financial institution, telecommunications company, service provider, shipping company) asking you to submit or confirm your information. They may even include a malicious link.



Royal Canadian Mounted Police  
Gendarmerie royale du Canada



Competition Bureau  
Canada

Bureau de la concurrence  
Canada



Ontario Provincial Police

Canada

- 7) Secret Santa** – You may have noticed multiple gift exchange posts on your social media feeds. This may seem like a fun activity where you only have to send one gift and receive multiples in return. Unfortunately, this exchange collects some of your personal information and also hides a pyramid scheme where only those on top profit. Pyramid schemes are illegal in Canada.
- 8) Prize Notifications** – You may receive a letter or a call with the good news; you’ve won millions and a fancy car too! First, you just need to confirm your personal information and then cover a few fees before your winnings can be delivered. Remember: If you didn’t enter, you can’t win. You can’t enter another country’s lottery without purchasing a ticket from within that country. In Canada, if there are fees associated to a prize, they are removed from the total winnings; you would never be required to pay fees in advance.
- 9) Emergency** – Is a supposed loved one reaching out to you because they need money now and you’re the only one they trust to keep it a secret? Resist the urge to act immediately and verify the person’s identity by asking them questions a stranger wouldn’t know.
- 10) Gift Cards** – Gift cards are a popular and convenient way to give a gift. They should also be considered like cash; once they are exchanged, it is unlikely that you are getting your money back. Gift cards are not meant for payments and no legitimate business or organization will request these; especially under pressure.
- 11) Identity Theft** – In all the hustle and bustle of the season,  
**DO:** keep your wallet on your person and cover your PIN;  
**DON’T:** share passwords or provide your personal information on impulse.
- 12) Identity Fraud** – Fraudsters love a good shopping spree; especially when they’re using someone else’s name and money. Contact your financial institutions and the credit bureaus, Equifax Canada and TransUnion Canada, as soon as you notice:
- a. Suspicious activity on your financial statement/s.
  - b. Unauthorized activity on your credit report.
  - c. Letters approving or declining credit applications you did not authorize.
  - d. Re-routed mail.
  - e. Bills from service providers you do not use.
  - f. Your information was compromised as part of a database breach.

Anyone who suspects they have been the victim of cybercrime or fraud should report it to their local police and to the Canadian Anti-Fraud Centre’s [online reporting system](#) or by phone at 1-888-495-8501. If not a victim, report it to the Canadian Anti-Fraud Centre anyways.