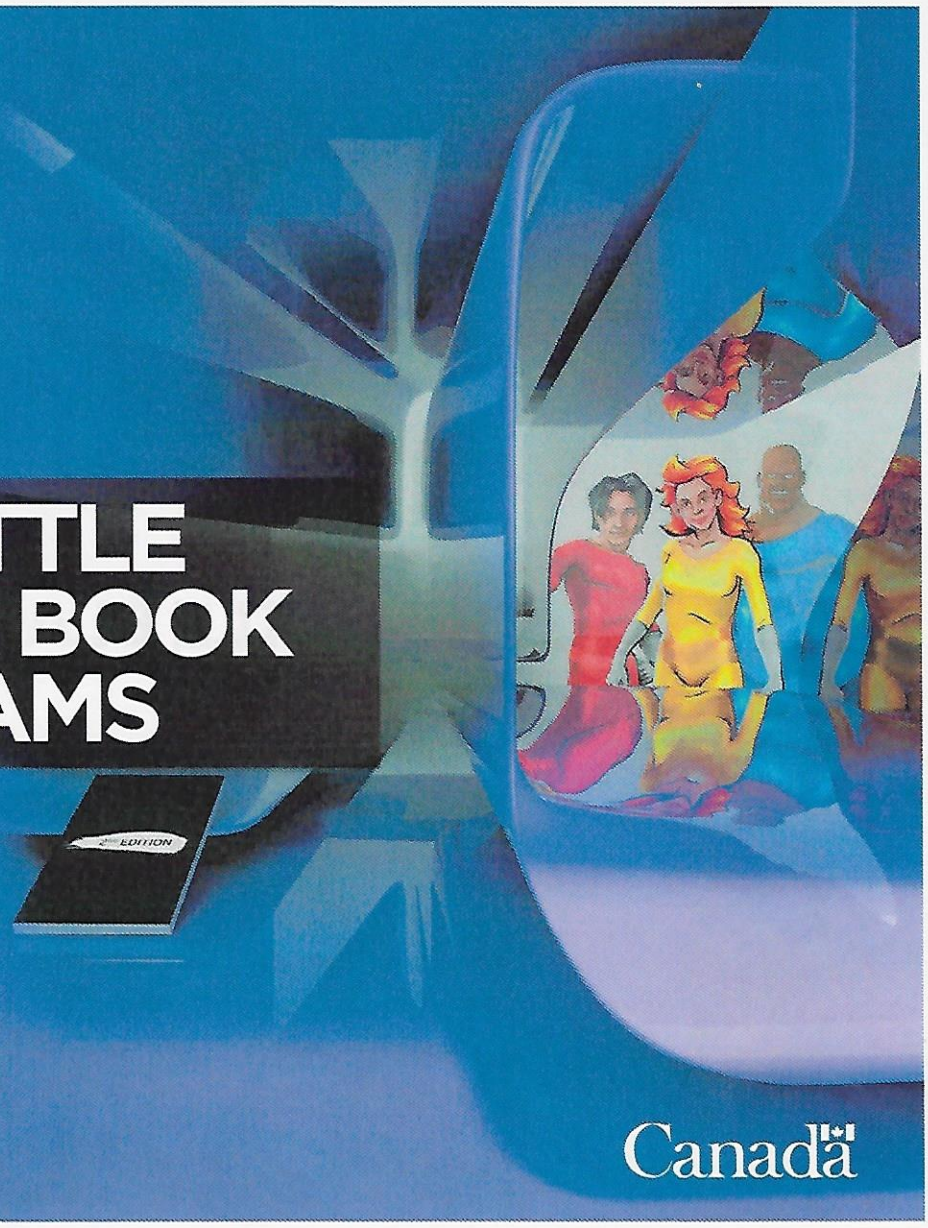
Competition Bureau Canada | Bureau de la concurrence Canada

THE LITTLE BLACK BOOK OF SCAMS



Canada

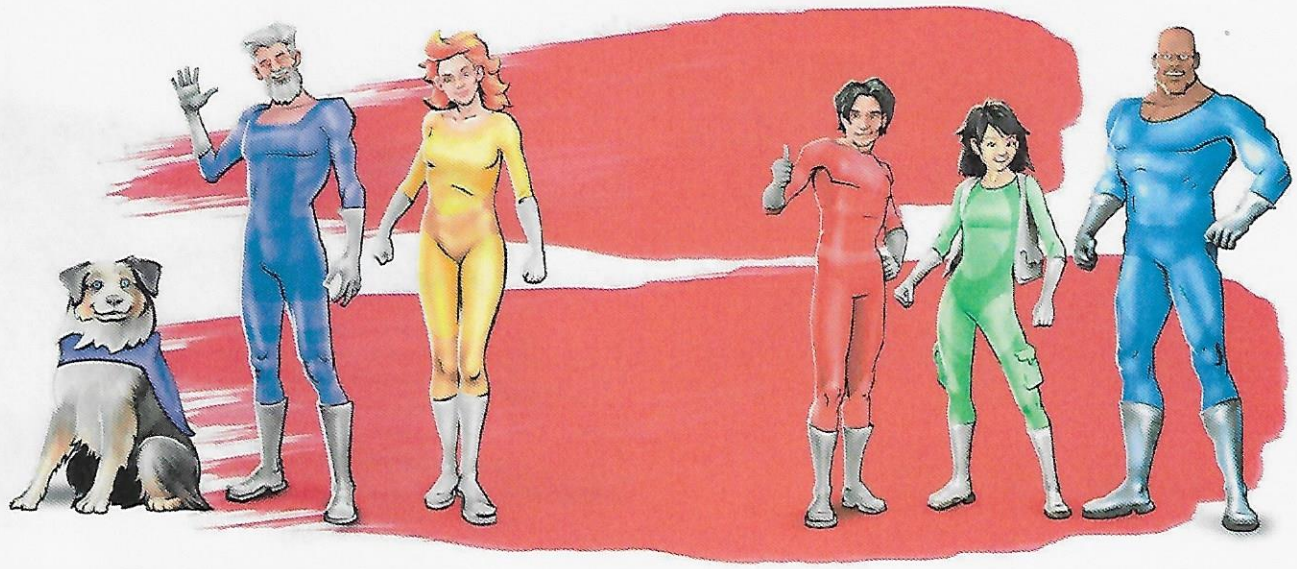
PREFACE

Scammers are sneaky and sly. They can target anyone, from youngsters to retirees. They can also target businesses. No one is immune to fraud.

Our group of superheroes has found a way to see through the scams. Their secret is simple: knowledge is power!

Read on to find out how you can also become a fraud-fighting superhero. Share this booklet with family and friends and start powering up!

TABLE OF CONTENTS



FRAUD FIGHTING 101

Become a real-life superhero by arming yourself with the information you need to fight fraud and keep yourself, your family and your money safe.

You work hard for your money. You want to spend it on things that matter to you—whether it's your children's education, an exciting trip or a new smartphone.

Fraudsters are real. They are out there every day looking for victims. They will target you online, over the phone, by mail or in person.

You're a target. Thousands of Canadians lose millions of dollars to fraudsters every year. The impact of fraud on families and businesses can be devastating.

Learn to fight fraud. This booklet includes 12 of the most common scams currently targeting Canadians. It is filled with tips and tricks on how to protect yourself and what to do if you get scammed.

Report it! Anyone can be targeted, from teenagers, to grandparents, to senior corporate officers. The best thing you can do is to report the fraud, whatever the amount, to the appropriate authorities. Don't be embarrassed as it will help others from falling for it.

Knowledge is your power. Protect yourself by seeking out more information. In addition to this booklet, you can also consult numerous trusted websites for more information.

The Canadian Anti-Fraud Centre, managed by the RCMP, the Competition Bureau and the Ontario Provincial Police, has plenty of information on fraud. Power up today by visiting www.antifraudcentre.ca!

SUBSCRIPTION TRAPS

Good deals can bait you into falling for expensive traps!

A subscription trap can trick you by offering "free" or "low-cost" trials of products and services. Products commonly offered are weight loss pills, health foods, pharmaceuticals and anti-ageing products.

Once you provide your credit card information to cover shipping costs, you are unknowingly locked into a monthly subscription. Delivery and billing can then be difficult, if not almost impossible, to stop.

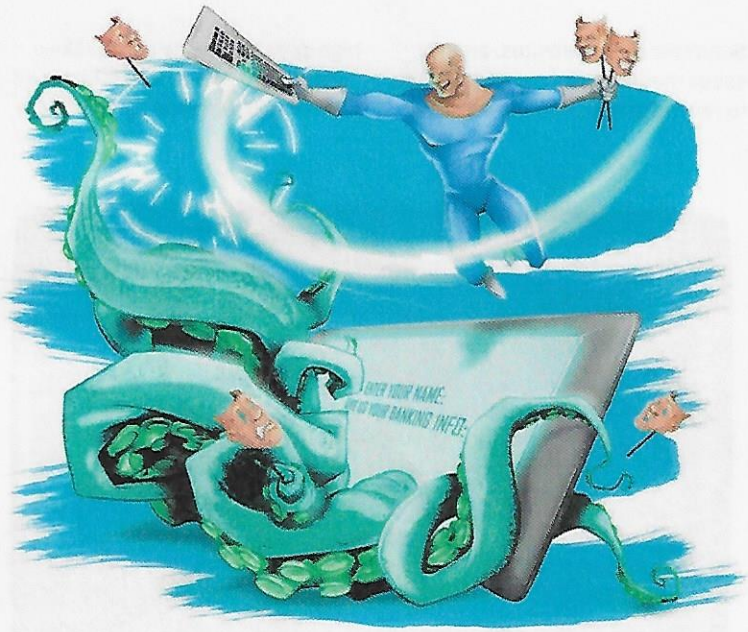
Scammers use websites, emails, social media platforms and phones to reel people in. Remember, high-pressure sales tactics like a "limited time offer" are often used to rush you into making a decision.

Tips to protect yourself:

- Trust your instincts. If it's too good to be true, don't sign up.
- Before you sign up for a free trial, research the company and read reviews, especially the negative ones. The Better Business Bureau is a great source of information.
- Don't sign up if you can't find or understand the terms and conditions. Pay special attention to pre-checked boxes, cancellation clauses, return policies, and any vague charges.
- If you go ahead with a free trial, keep all documents, receipts, emails, and text messages.
- Regularly check your credit card statements for frequent or unknown charges.
- If you have trouble cancelling your subscription, contact your credit card provider, your local consumer protection organization, or law enforcement agencies.

If you suspect a scam, always report it.

Go to pages 19 and 20 for more information.



IDENTITY THEFT

Help ensure your identity remains yours alone!

Scammers are always on the lookout to collect or reproduce your personal information to commit fraud. Thieves can make purchases using your accounts, obtain passports, receive government benefits, apply for loans, and more. This could turn your life upside down.

Fraudsters use techniques that range from unsophisticated to elaborate. Offline, they can go through trash bins or steal mail. Online, they can use spyware and viruses, as well as hacking and phishing (see page 13).

They look for credit card information, bank account details, full name and signature, date of birth, social insurance number, full address, mother's maiden name, online usernames and passwords, driver's licence number, and passport number.

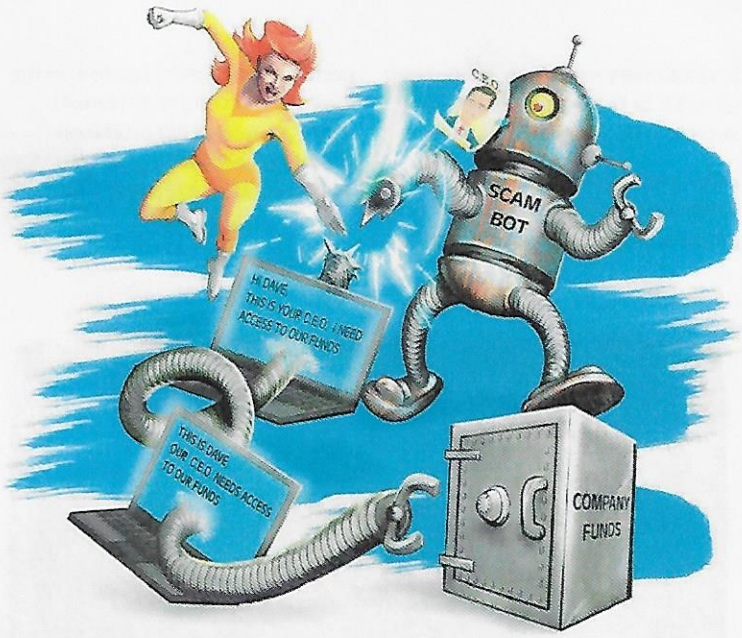
Identity theft is a serious crime!

Tips to protect yourself:

- Never provide your personal information over the phone, via text message, email or the internet.
- Avoid public computers or Wi-Fi hotspots, such as in coffee shops, to access or provide personal information; they put you at risk.
- Create strong and unique passwords for each of your online accounts. Password-protect your devices and home Wi-Fi network.
- Use a secure and reputable payment service when buying online—look for a URL starting with "https" and a closed padlock symbol.
- Avoid giving out personal information on social media. It can be used along with your pictures to commit fraud.
- Always shield your PIN when using your card. If you hand it over to a cashier, never lose sight of it.
- Shred and destroy documents with personal information.

If you suspect a scam, always report it.

Go to pages 19 and 20 for more information.



CEO SCAMS

Your CEO is asking for money urgently; make sure the email is legitimate!

Do you work in accounting or finance? Do you have the authority to move money at work? Do you report to a chief executive officer (CEO)? If yes, be on the lookout; this scam specifically targets you!

In a typical "CEO scam," fraudsters will impersonate a senior company executive, either by gaining access to their email address or by imitating one. They will send realistic-looking emails that try to trick you into wiring money to a third party.

The emails will make the request sound urgent and confidential. For example, they may say the money is needed to secure an important contract, complete a confidential transaction, or update a supplier's payment information.

Fraudsters are usually strategic about the timing of these emails. They send them when executives are away or hard to reach. This lucrative scam can cost businesses tens of thousands to millions of dollars.

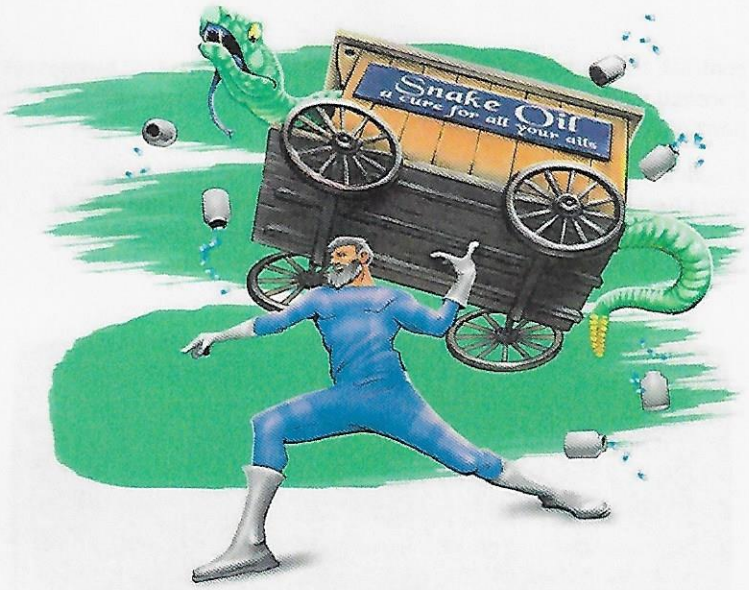
CEO scams are a growing global threat that targets small local businesses and large corporations alike.

Tips to protect yourself:

- Keep your computer systems secure with an up-to-date, reputable antivirus software and strong passwords.
- Validate all transfer requests either on the phone or in person. Never use the contact information provided in emails.
- Verify the sender's email address—scammers will often create addresses that are very similar to legitimate ones, with just one or two different letters.
- Encourage your company to create a standard process for money transfers that requires multiple levels of approvals.
- Limit the details you share publicly. Fraudsters use information that's available online and on social media to find potential victims and to time their fraud.

If you suspect a scam, always report it.

Go to pages 19 and 20 for more information.



HEALTH AND MEDICAL SCAMS

Watch out for magical cures that offer quick and easy fixes.

There are fraudsters out there who hope to take advantage of people's suffering. The three most common types of health scams are **miracle cures, weight loss programs** and **fake online pharmacies.** In all cases, they often appear as sponsored posts on social media or website pop-ups.

Scammers offer products and services that **seem to be legitimate alternative medicines and treatments** that quickly and easily treat serious conditions. Some of these may seem to be endorsed by celebrities or promoted by testimonials of people claiming to have been cured.

Weight loss scams promise **dramatic results with little to no effort.** The scammers might promote unusual diets; revolutionary exercises; fat-busting devices; or breakthrough products, such as pills, patches or creams.

Fake online pharmacies offer **drugs and medications at very cheap prices or without a doctor's prescription.** They advertise on the internet and send spam emails. If you do receive the promised products, there is no guarantee they are the real thing or safe to take.

Tips to protect yourself:

- **Remember that there are no magic pills or miracle cures for achieving quick weight loss or treating medical conditions.**
- **Don't trust claims about medicines, supplements or other treatments. Get the facts straight from your healthcare professional.**
- **Never commit to anything under pressure, especially if a large advance payment or long-term contract is required.**
- **Know that if an online pharmacy is legitimate, it will require valid prescriptions.**
- **Be skeptical of celebrity endorsements or testimonials.**

If you suspect a scam, always report it.

Go to pages 19 and 20 for more information.

ROMANCE SCAMS

Who is really behind the keyboard?

Keep your guard up and look out for potential scammers who will try to lower your defences by appealing to your romantic and compassionate side. They can prey on you on popular, legitimate dating sites as well as on fake ones.

On a real dating site, a scammer might send you a few messages and a good-looking photo of themselves, or of someone they claim to be. Once you are charmed, they will **start asking you to send money.** They may claim to have a very sick family member or a desperate situation with which they need your help. Once you **give them money, they often disappear.**

A fraudster can also create a fake dating site where you **pay for each message you send and receive.** To keep you writing back and paying, the scammer may hook you in with vague emails about their love and desire for you.

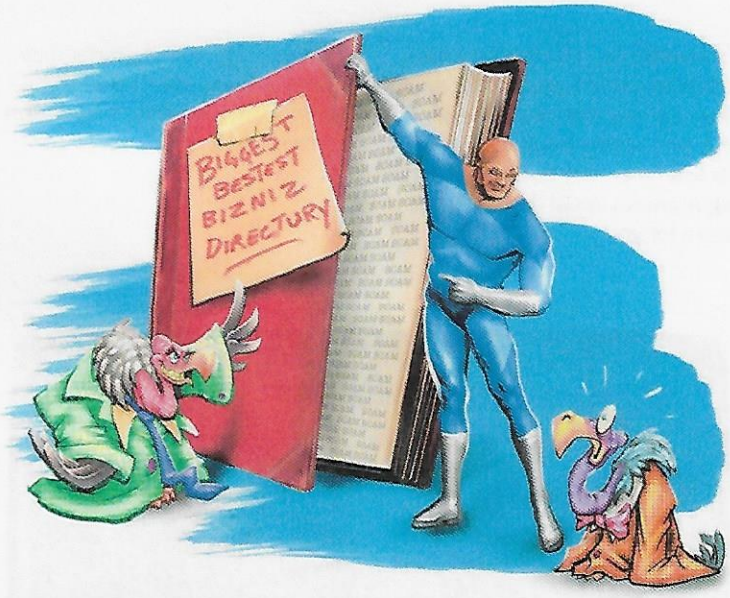
In many cases, the scammer may even arrange to meet up with you in person to make their **fraud seem more credible.**

Tips to protect yourself:

- Never send money or give financial details on a dating site.
- Trust your instincts, ask questions and carefully read the terms and conditions before signing up.
- Know which services are free, which ones cost money and what it takes to cancel your account.
- Make sure you only use legitimate and reputable dating sites. Always check website addresses carefully, as scammers often mimic real web addresses.
- Remember that it's very unlikely that someone will declare their undying love to anyone after only a few letters, emails, phone calls or pictures.

If you suspect a scam, always report it.

Go to pages 19 and 20 for more information.



BUSINESS SCAMS

Stay up to date on the schemes targeting businesses!

Organizations of any size can still be duped by clever frauds, so make sure you know about them.

A typical one is the directory scam. A fraudster sends your company a proposal for a listing or advertisement in a magazine, journal or business directory, or for an online directory. They'll call to confirm the address and other details. Then the accounting department will receive and pay the bill, unaware that your company never actually ordered or authorized the service.

Another common fraud is the health and safety products scam. You might receive a phone call from someone claiming to be from the provincial government, telling you that your first-aid kits need to be replaced or you have to update your company's health and safety training. In both cases, you may be told to act quickly.

One other possible scam is the office supply scam, which involves you receiving and being charged for items you didn't order.

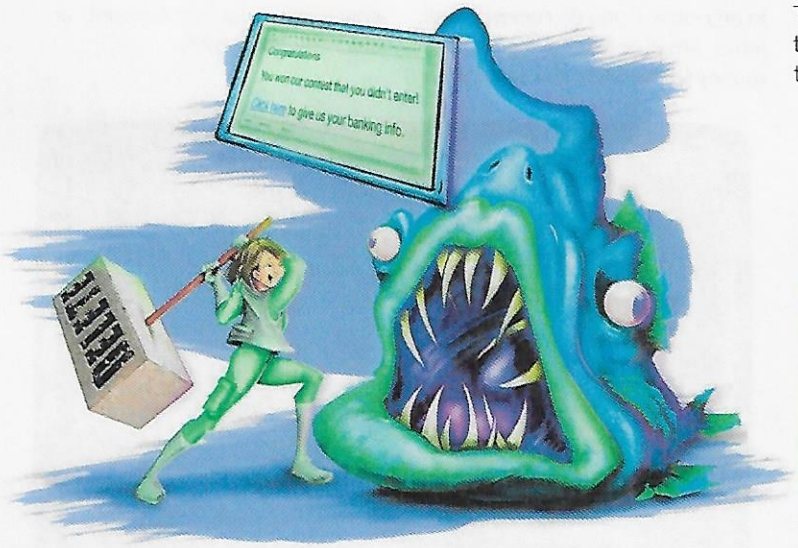
In many cases, scammers will hound you to pay the amount they claim you owe. They will even trick you into believing that they will report you to a collection agency.

Tips to protect yourself:

- Educate yourself, your employees and your co-workers to be cautious of unsolicited calls.
- Create a list of companies that are typically used by your business.
- Limit the number of staff who can approve purchases and pay bills.
- Clearly define procedures for verification, payment and management of accounts and invoices.
- Contact your province's regulator to know your legal obligations.
- Fraudsters will use company names or logos similar to those of known businesses to make their invoices seem real. Inspect invoices carefully before making any payments.

If you suspect a scam, always report it.

Go to pages 19 and 20 for more information.



PHISHING AND SMISHING SCAMS

Be on the lookout. Messages are easily fabricated!

As we spend more time online, fraudsters are getting more creative with scams in the digital space.

Phishing is when you get an unsolicited email that claims to be from a legitimate organization, such as financial institutions, businesses or government agencies. Scammers ask you to provide or verify, either via email or by clicking on a web link, personal or financial information, like your credit card number, passwords and social insurance number.

Smishing is the same thing, except it occurs via text messages.

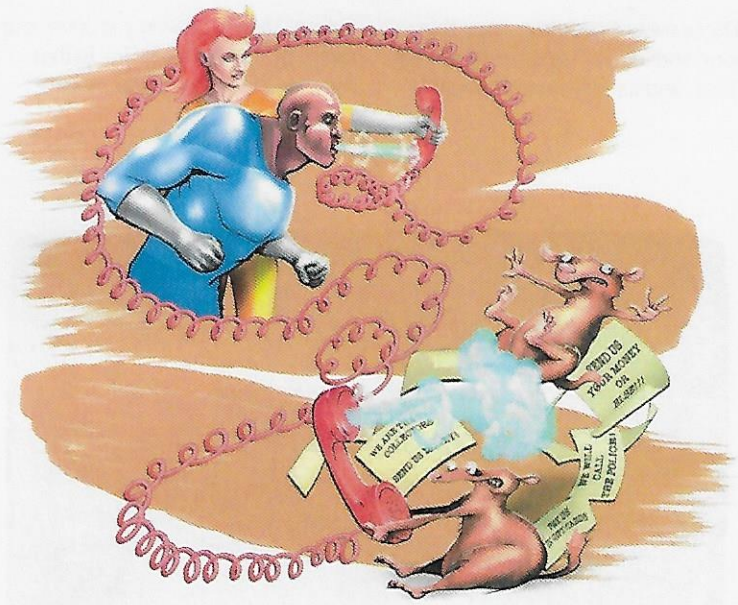
These messages often copy the tone and logo of organizations you trust, and usually include a call to action. They take many shapes and forms but the bottom line is that they seek your personal details.

Tips to protect yourself:

- Know that reputable organizations will never ask for your personal information through email or text.
- Ignore communications from unknown contacts.
- Delete suspicious messages as they can carry viruses.
- Don't reply to spam messages, even to unsubscribe, and don't open any attachments or follow any links.
- To verify a hyperlink without clicking, hover your mouse over it. Carefully check if it is accurate.
- Update your antivirus software on all devices.
- Never use the phone number or email address provided in the suspicious message—use contact information listed on verified websites.

If you suspect a scam, always report it.

Go to pages 19 and 20 for more information.



TAX SCAMS

Got a call or email from the CRA? Make sure it's real!

You get a text message or an email from the Canada Revenue Agency (CRA) claiming you're entitled to an extra refund and all you need to do is provide your banking details. Watch out—this wonderful-if-true situation is exactly what a tax scam looks like.

Another variation is that they call you to say that you owe the CRA money and that you need to pay right away, or else they will report you to the police.

In any case, if you do receive a call, letter, email or text saying you owe money to the CRA, you can double check online via "My Account" or call 1-800-959-8281.

Tips to protect yourself:

The CRA will never:

- use aggressive or threatening language.
- threaten you with arrest or send police.
- ask for payments via prepaid credit cards or gift cards, such as ITunes, Home Depot, etc.
- collect or distribute payments through Interac e-transfer.
- use text messages to communicate under any circumstances.

Emails from the CRA:

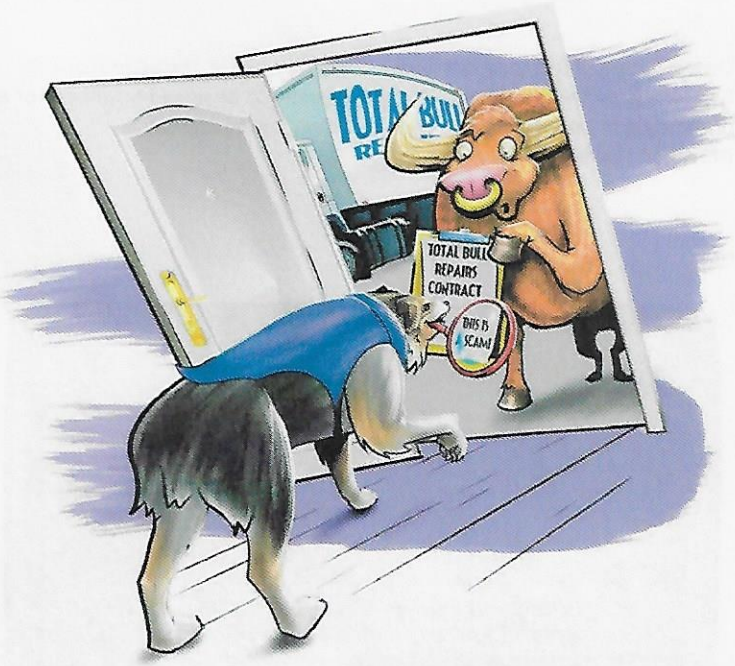
- never ask for financial information.
- never provide financial information.

The CRA's accepted payment methods are:

- online banking.
- debit card.
- pre-authorized debit.

If you suspect a scam, always report it.

Go to pages 19 and 20 for more information.



DOOR-TO-DOOR SCAMS

Knock, knock! Who's there? A scammer!

Despite living in the digital age, there are still some old fashioned scams that come right to your door, posing a threat to you and to businesses. With this trick, door-to-door salespeople use high-pressure tactics to convince you to buy a product or sign up for a service you don't want or need.

These aggressive pitches are often for charitable donations, investment opportunities or home services and maintenance of various appliances, like water heaters, furnaces and air conditioners.

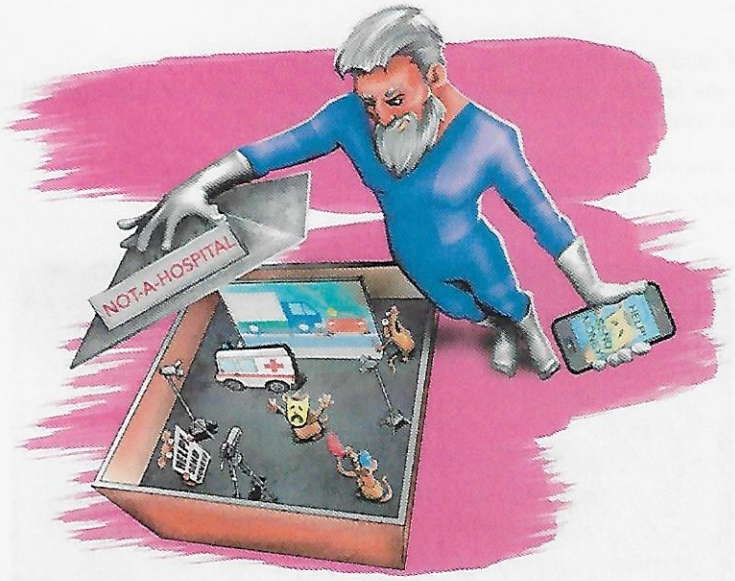
In many cases, you'll never receive the product or service promised. In others, the products or services are of poor quality or not as represented.

Tips to protect yourself:

- Don't feel pressured to make a quick decision—take time to do some research on the seller and the products first.
- Ask for photo ID, get the name of the person and of the company or charity they represent.
- Ask for the charity's breakdown of where funds are allocated. Be sure to get this in writing.
- Never share any personal information or copies of any bills or financial statements.
- Only allow access to your property to people you trust.
- Research before you invest. Don't sign anything and always read the fine print.
- Know your rights. Contact your local consumer affairs office—most provinces and territories have guidelines under their consumer protection act.

If you suspect a scam, always report it.

Go to pages 19 and 20 for more information.



EMERGENCY SCAMS

Caring grandparents, don't act too quickly!

Emergency frauds usually target loving grandparents, taking advantage of their emotions to rob them of their money.

The typical scam starts with a grandparent receiving a phone call from someone claiming to be their grandchild. The "grandchild" goes on to say they're in trouble—common misfortunes include having been in a car accident, getting locked up in jail, or trouble returning home from a foreign country—and they need money immediately.

The caller will ask you questions, getting you to reveal personal information. They'll also swear you to secrecy, saying they are embarrassed and don't want other family members to find out what's happened.

One variation of this ploy features two people on the phone, one pretending to be a grandchild and the other a police officer or lawyer.

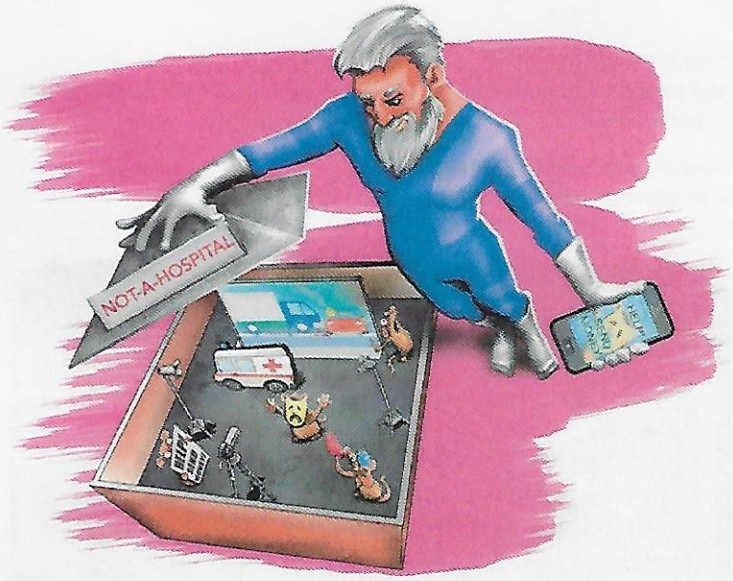
In other cases, the scammer will pretend to be an old neighbour or a family friend in trouble.

Tips to protect yourself:

- Take time to verify the story. Scammers are counting on you wanting to quickly help your loved one in an emergency.
- Call the child's parents or friends to find out about their whereabouts.
- Ask the person on the phone questions that only your loved one would be able to answer and verify their identity before taking steps to help.
- Never send money to anyone you don't know and trust.
- Never give out any personal information to the caller.

If you suspect a scam, always report it.

Go to pages 19 and 20 for more information.



EMERGENCY SCAMS

Caring grandparents, don't act too quickly!

Emergency frauds usually target loving grandparents, taking advantage of their emotions to rob them of their money.

The typical scam starts with a grandparent receiving a phone call from someone claiming to be their grandchild. The "grandchild" goes on to say they're in trouble—common misfortunes include having been in a car accident, getting locked up in jail, or trouble returning home from a foreign country—and they need money immediately.

The caller will ask you questions, getting you to reveal personal information. They'll also swear you to secrecy, saying they are embarrassed and don't want other family members to find out what's happened.

One variation of this ploy features two people on the phone, one pretending to be a grandchild and the other a police officer or lawyer.

In other cases, the scammer will pretend to be an old neighbour or a family friend in trouble.

Tips to protect yourself:

- Take time to verify the story. Scammers are counting on you wanting to quickly help your loved one in an emergency.
- Call the child's parents or friends to find out about their whereabouts.
- Ask the person on the phone questions that only your loved one would be able to answer and verify their identity before taking steps to help.
- Never send money to anyone you don't know and trust.
- Never give out any personal information to the caller.

If you suspect a scam, always report it.

Go to pages 19 and 20 for more information.

PURCHASE OF MERCHANDISE SCAMS

Not all online vendors are reputable!

Online shopping is a favourite pastime for many consumers. But many deals you see online—from inexpensive designer purses to significantly discounted electronic goods—are too good to be true.

Fraudsters can create accounts on legitimate auction sites, such as eBay, or on an online marketplace, like Kijiji or Craigslist. They will advertise their products at very low prices, enticing you to buy them.

At the end of the day, if you do get something, it might be of poor quality or a bad imitation of what you expected.

In other instances, fraudsters will lure you into clicking on sponsored links that will direct you to a seemingly genuine website. If you decide to buy from there, you won't benefit from any protection or services that legitimate websites offer.

If a site or offer stands out dramatically from the rest, there's likely something off.

Tips to protect yourself:

- Buy from companies or individuals you know by reputation or from past experience.
- Never make a deal outside the auction site.
- Beware of sellers from far away or that have limited or no reviews.
- Use a credit card when shopping online; many offer protection and may give you a refund.
- Be wary of websites that contain spelling mistakes and grammatical errors.
- Read the refund and return policies carefully, including the fine print.
- Ask the supplier questions and confirm service delivery timelines and the total cost.

If you suspect a scam, always report it.

Go to pages 19 and 20 for more information.

SALE OF MERCHANDISE SCAMS

Scammers can pose as buyers.

If you sell items online, either personally or as part of a business, you need to be careful who you sell to as there is a risk of being targeted by tricksters who want to take your merchandise, money, or both.

In one version, the fraudster will agree to buy your item without seeing it. You'll get a PayPal or email money notification that claims the payment is pending.

The catch is, the notification will say the payment will only be released when you provide a tracking number for the goods. By the time you enter the tracking number, you'll have already shipped the merchandise only to learn that the payment notification was a fake.

In other cases, you might get paid with a fake money transfer, a fraudulent cheque or a stolen credit card.

In another version, the scammer may send you a message that says the payment can't be sent due to a problem with your PayPal or bank account. You'll be asked to pay a fee to obtain a business account to complete the transaction. The scammer offers to pay the fee if you reimburse them using a transfer or wire service. If you agree, the "fee" money will go to the con artist.

Tips to protect yourself:

- Always meet in a local, public and safe place to complete an exchange.
- Beware of generic emails with bad grammar.
- Beware of far away buyers who want to buy products or other items without seeing them.
- Verify the sender's email address—scammers will often create addresses that are very similar to legitimate ones, with just one or two different letters.
- Never send money to get money.

If you suspect a scam, always report it.

Go to pages 19 and 20 for more information.

RED FLAGS: THINGS TO WATCH FOR

Learn to recognize the signs that something is amiss.

Wire transfer. Many scams involve a request to wire money electronically using a money transfer service, like MoneyGram and Western Union, or using cryptocurrency, such as Bitcoin. Remember that sending a transfer through these services is like sending cash—once the amount is picked up, it's almost impossible to get your money back.

Overpayment. When you're selling something—especially online—be wary of how you get paid. A fraudster may send you a counterfeit cashier's, personal or corporate cheque in an amount in excess of what they owe. You'll be asked to deposit the cheque and wire the excess funds immediately back to them. Once your bank realizes the cheque is a fake, you'll be on the hook for the money withdrawn.

Spelling mistakes. Be skeptical of emails, messages or websites that contain misspelled common words; grammar errors that make it difficult to read or expressions that are used incorrectly. Email and web addresses should also be examined closely to see if there are subtle mistakes or differences.

Personal information request. Fraudsters may ask potential victims to provide more personal or financial information than is required for the transaction or discussion. Be suspicious if someone asks for copies of your passport, driver's licence and social insurance number, or birth date, especially if you don't know the requestor.

Unsolicited calls. You might get a call from someone claiming that you have a virus on your computer, you owe taxes or there has been fraudulent activity in your bank accounts. Know that legitimate organizations will not call you directly. Hang up and call the organization yourself using the number from a trustworthy source, such as the phone book, their website, or even invoices and account statements.

Unsolicited friend requests on social media. Don't accept friend requests from people you don't know until you review their profile or ask your real-life friends if they know them. Does their profile look fairly empty or have posts that are very generic? Do they seem to be promising more than friendship? These are some red flags that point to a scam. Delete that request and block future ones.

Astounding mail offers. You received a game card in the mail. It guarantees you will or have already won. Prizes might range from cars to trips. If you have not entered a contest, throw that card away. It's probably a scam!

It's just too good to be true. Everybody loves a great deal. But shocking offers, unbelievable discounts and unreal rates may signal that the offer isn't quite what it seems. Cheap prices usually equal cheap products, or counterfeit goods. Free offers may require providing your credit card for shipping. Small tactics like these can lead to big profits for scammers.

REPORTING A SCAM

Who to contact depends on where you live and what type of scam is involved.

Whether you've been scammed or targeted by a fraudster, you should always report it. Canadian authorities may not always be able to take action against scams, but there are ways you can help. By reporting the scam, authorities may be able to warn other people and alert the media to minimize the chances of the scam spreading further. You should also warn your friends and family of any scams you come across.

Here is some advice on where to report, depending on the type of scam:

Canadian Anti-Fraud Centre
www.antifraudcentre.ca
1 888 495 8501

Competition Bureau
www.competitionbureau.gc.ca
1 800 348 5358

Local scams

Contact your local consumer affairs office

Your local consumer affairs office is the best resource for investigating scams that appear to come from within your own province or territory. A list of provincial and territorial consumer affairs offices can be found in the Canadian Consumer Handbook.

www.consumerhandbook.ca

Financial and investment scams

Contact Canadian Securities Administrators

Financial scams involve sales offers or promotions about financial products and services, such as superannuation, managed funds, financial advice, insurance, or credit or deposit accounts.

Investment scams involve share buying, foreign currency trading, offshore investments, Ponzi schemes, or prime bank investment schemes.

You can report financial and investment scams to the Canadian Securities Administrators or your local securities regulator.

www.securities-administrators.ca

Banking and credit card scams

Contact your bank or financial institution

In addition to reporting these scams to the Canadian Anti Fraud Centre, you should alert your bank or financial institution about any suspicious correspondence that you receive regarding your account. They can advise you on what to do next.

When contacting your bank or financial institution, make sure to use the telephone number found in the phone book, on your account statement or on the back of your card.

Spam emails and text messages

Contact the Spam Reporting Centre

Many scams arrive by email and text message. Visit www.fightspam.gc.ca for information on Canada's anti spam legislation and how to report spam.

Fraudulent, phishing or smishing messages requesting personal details can also be reported to the bank, financial institution or other concerned organization. Again, be sure to use a phone number or email address that is listed in an official reputable source, and not the one that appears in the email.

Fraud, theft and other crimes

Contact the police

Many scams that may breach consumer protection laws (those enforced by the Competition Bureau and other government and law enforcement agencies) may also breach the fraud provisions of the *Criminal Code*.

If you are the victim of fraud—meaning you have suffered a loss because of someone's dishonesty or deception—consider contacting your local police, especially if the amount involved is significant. You should definitely contact the police if your property has been stolen or you've been threatened or assaulted by a scammer.

Identity theft

Contact the police

Identity theft refers to the acquisition and collection of someone else's personal information for criminal purposes.

If you suspect or know that you are a victim of identity theft or fraud, or if you unwittingly provided personal or financial information, you should:

- Contact your local police force and file a report.
- Contact your bank or financial institution and credit card company
- Contact the two national credit bureaus and place a fraud alert on your credit reports.
- Always report identity theft and fraud. Contact the Canadian Anti-Fraud Centre

Additional organizations to contact depending on the situation:

- Your provincial Better Business Bureau
- Canada Revenue Agency—Charities Inquiries Line

  www.cra-arc.gc.ca
  1 800 267 2384
- Your provincial records office
- Credit bureaus can put a fraud alert on your account, which will alert lenders and creditors of potential fraud:

  Equifax Canada
  1-800-465-7166

  TransUnion Canada
  1-866-525-0262

The Little Black Book of Scams is available online at www.competitionbureau.gc.ca