



Competition Bureau  
Canada

Bureau de la concurrence  
Canada



The Canadian Edition

# THE LITTLE BLACK BOOK OF **SCAMS**

YOUR GUIDE TO PROTECTION AGAINST FRAUD

Canada

First published by the Competition Bureau Canada 2012  
Reproduced with permission from the Australian Competition and Consumer Commission



Illustrations by Pat Campbell

This publication is also available online in HTML at: [www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/03074.html](http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/03074.html).

For information on the Competition Bureau's activities or to obtain alternate formats, such as regular print, Braille or another appropriate format please contact:

Information Centre – Competition Bureau  
50 Victoria Street, Gatineau, QC K1A 0C9  
Tel.: 819-997-4282  
Toll free: 1-800-348-5358  
TTY (for hearing impaired): 1-800-642-3844  
Fax: 819-997-0324  
Website: [www.competitionbureau.gc.ca](http://www.competitionbureau.gc.ca)

#### Permission to reproduce

Except as otherwise specifically noted, the information in this publication may be reproduced, in part or in whole and by any means, without charge or further permission from the Competition Bureau provided due diligence is exercised in ensuring the accuracy of the information reproduced; that the Competition Bureau is identified as the source institution; and that the reproduction is not represented as an official version of the information reproduced, nor as having been made in affiliation with, or with the endorsement of the Competition Bureau. For permission to reproduce the information in this publication for commercial purposes, please contact the:

#### Web Services Centre

Innovation, Science and Economic Development Canada  
C.D. Howe Building  
235 Queen Street  
Ottawa, ON Canada  
K1A 0H5  
Email: [info@ic.gc.ca](mailto:info@ic.gc.ca)

© Her Majesty the Queen in Right of Canada, represented by the Minister of Industry.

Cat. No. Iu54-42/2015E  
ISBN 978-0-660-03847-6

2015-11-20

Aussi offert en français sous le titre *Le petit livre noir de la fraude*.





The Canadian Edition

# THE LITTLE BLACK BOOK OF **SCAMS**

YOUR GUIDE TO PROTECTION AGAINST FRAUD

# FOREWORD



## COMMISSIONER OF COMPETITION

The Competition Bureau, under the provisions of the *Competition Act* and other laws, pursues businesses and individuals who carry out deceptive marketing practices, such as false representations via telemarketing, fake lotteries, or Internet or mobile phone scams.

The Canadian edition of *The Little Black Book of Scams* aims to increase your awareness of the many types of fraud that target Canadians and offers some easy steps you can take to protect yourself and avoid falling victim to fraud.

Since it was first published in March 2012, the booklet has been very popular from the start, being offered in print and online. As of July 2013, the Bureau had distributed over

14,000 printed copies and the document had been downloaded over 30,000 times. The online version now has better accessibility and had been visited over 80,000 times.

This booklet debunks common myths about scams, provides helpful tips, questions to ask yourself, and many contact information for reporting a scam to the correct authority,

I am grateful to the Australian Competition and Consumer Commission, who originally developed *The Little Black Book of Scams* and granted the Bureau permission to produce a Canadian edition.

John Pecman  
*Commissioner of Competition*



## CONTENTS

 Introduction	1
 Lotteries, sweepstakes and contests	2
 Pyramid schemes	4
 Money transfer requests	6
 Internet scams	8
 Mobile phone scams	10
 Health and medical scams	12
 Emergency scams	14
 Dating and romance scams	16
 Charity scams	18
 Job and employment scams	20
 Small business scams	22
 Service scams	24
 Handy hints to protect yourself	26
 Scams and you: What to do if you get scammed!	28
 Getting help and reporting a scam	29

# MYTH BUSTERS

Busting these common myths will minimize your chances of being scammed.

- All companies, businesses and organizations are legitimate because they are licensed and monitored by the government: This is not always true. While there are rules about setting up and running a business or a company in Canada, scammers can easily pretend to have approval when they don't. Even businesses that are licensed could still try to scam you by acting dishonestly.
- All Internet websites are legitimate: This is not always true. Websites are quite easy and cheap to set up. The scammers can easily copy a genuine website and trick you into believing it is legitimate.
- There are short cuts to wealth that only a few people know: This is not always true. Ask yourself the question: if someone knew a secret to instant wealth, why would they be telling their secret to others?
- Scams involve large amounts of money: This is not always true. Sometimes scammers target a large number of people and try to get a small amount of money from each person.
- Scams are always about money: This is not always true. Some scams are aimed at stealing personal information from you.

## GOLDEN RULES

Remember these golden rules to help you beat the scammers.

- Always get independent advice if an offer involves money, personal information, time or commitment.
- There are no guaranteed get-rich-quick schemes—sometimes the only people who make money are the scammers.
- Do not agree to offers or deals right away. If you think you have spotted a great opportunity, insist on time to get independent advice before making a decision.
- Do not hand over money or personal information, or sign anything until you have done your homework and checked the credentials of the company that you are dealing with.
- Do not rely on glowing testimonials: find solid evidence of a company's success.
- Log directly on to a website that you are interested in rather than clicking on links provided in an email.
- Never send money, or give credit card or online account details to anyone you do not know and trust.
- If you spot a scam or have been scammed, get help. Contact the Canadian Anti-Fraud Centre, the Competition Bureau or your local police for assistance. See page 29 for contact information.

Scammers are imaginative and manipulative. They know how to push your buttons to produce the response they want.



# INTRODUCTION

Every year, Canadians lose millions of dollars to the activities of scammers who bombard us with online, mail, door-to-door and telephone scams.

We are pleased to bring you the first Canadian edition of *The Little Black Book of Scams*. We hope this book will increase your awareness of the vast array of scams that target Canadians and share with you some easy steps you can take to protect yourself.

## SCAMMERS DO NOT DISCRIMINATE

Scammers target people of all backgrounds, ages and income levels. Fake lotteries, Internet frauds, get-rich-quick schemes and miracle health cures are some of the favoured means of separating the unwary from their money. New varieties of these scams appear all the time.

The Competition Bureau has seen the devastating effects scams can have on people and their families. One of the best ways to

combat this kind of fraud is to take measures to prevent yourself from being caught in the first place.

## PROTECT YOURSELF

If you want to stay on top of scams, inform yourself on how to recognize the various types of scams and protect your personal information by visiting law enforcement organizations' websites, the Canadian Anti-Fraud Centre ([www.antifraudcentre.ca](http://www.antifraudcentre.ca)) or other reputable organizations.

# LOTTERIES, SWEEPSTAKES AND CONTESTS

Many Canadians are lured by the excitement of a surprise win and find themselves sending huge amounts of money to claim fake prizes.

## WHAT TO LOOK FOR

You cannot win money or a **prize in a lottery** unless you have entered it yourself, or someone else has entered it on your behalf. You cannot be chosen as a random winner if you don't have an entry.

Many lottery scams try to trick you into providing your banking and personal details to claim your prize. You should not have to pay any fee or tax to claim a legitimate prize.

Don't be fooled by claims that the offer is legal or has government approval—many scammers will tell you this. Instead of receiving a grand prize or fortune, you will lose every cent that you send to a scammer. And if you have provided other personal details, your identity could be misused too.

A fake prize scam will tell you that you have won a prize or a contest. You may receive a phone call, an email, a text message or see a pop-up screen on your computer. There are often costs involved with claiming your prize, and even if you do receive a prize, it may not be what was promised to you.

The scammers make their money by making you pay fees or taxes, call their premium rate phone numbers or send premium text messages to claim your prize. These premium rate calls can be very expensive, and the scammers will try to keep you on the line for a long time or ask you to call a different premium rate number.



## PROTECT YOURSELF

### REMEMBER

Legitimate lotteries do not require you to pay a fee or tax to collect winnings.

### CAUTION

Never send money to anybody you don't know and trust.

### THINK

Don't provide personal banking details to anyone that you do not know and trust.

### INVESTIGATE

Examine all of the terms and conditions of any offer very carefully—claims of free or very cheap offers often have hidden costs. Calls to premium rate phone numbers or premium text messages can be very expensive.

### ASK YOURSELF

Did I enter this contest? You cannot win money or a prize in a contest unless you have entered it yourself, or someone else has entered it on your behalf.

# PYRAMID SCHEMES

Pyramid schemes promise a large financial return for a relatively small cost. Pyramid schemes are illegal and very risky—and can cost you a lot of money.

## WHAT TO LOOK FOR

In a typical **pyramid scheme**, unsuspecting investors are encouraged to pay large membership fees to participate in money-making ventures. The only way for you to ever recover any money is to convince other people to join and to part with their money as well. People are often persuaded to join by family members or friends. But there is no guarantee that you will recoup your initial investment.

Although pyramid schemes are often cleverly disguised, they make money by recruiting people rather than by selling a legitimate product or providing a service. Pyramid schemes inevitably collapse and you will lose your money. In Canada, it is a crime to promote a pyramid scheme or even to participate in one.

**Ponzi schemes** are fraudulent investment operations that work in a similar way to pyramid schemes. The Ponzi scheme usually entices new and well-to-do investors by offering higher returns than other investments in the form of short-term returns that are either abnormally high or unusually consistent. The schemer usually interacts with all the investors directly, often persuading most of the existing participants to reinvest their money, thereby minimizing the need to bring in new participants as a pyramid scheme will do.

Be cautious, but do not be discouraged from carefully researching business opportunities based on commissions. There are many legitimate multi-level marketing opportunities where you can legally earn an income from selling genuine products or services.



!	<b>PROTECT YOURSELF</b>
<b>REMEMBER</b>	Pyramid and Ponzi schemes may be sent to you from family members and people you trust—they might not know that they could be illegal or that they are involved in a scam.
<b>CAUTION</b>	Never commit to anything at high-pressure meetings or seminars.
<b>THINK</b>	Don't make any decisions without doing your homework—research the offer being made and seek independent advice before making a decision.
<b>INVESTIGATE</b>	Do some research on all business opportunities that interest you.
<b>ASK YOURSELF</b>	If I am not selling a genuine product or service, is participation in this activity legal?

# MONEY TRANSFER REQUESTS

Money transfer scams are on the rise. Be very careful when someone offers you money to help transfer their funds. Once you send money to someone, it can be very difficult, if not impossible, to get it back.

## WHAT TO LOOK FOR

The **Nigerian** scam (also called the 419 fraud) has been on the rise since the early-to-mid 1990s in Canada. Although many of these sorts of scams originated in Nigeria, similar scams have been started all over the world (particularly in other parts of West Africa and in Asia). These scams are increasingly referred to as “**advance fee fraud**”.

In the classic Nigerian scam, you receive an email or letter from a scammer asking your help to transfer a large amount of money overseas. You are then offered a share of the money if you agree to give them your bank account details to help with the transfer. They will then ask you to pay all kinds of taxes and fees before you can receive your “reward”. You will never be sent any of the money, and will lose the fees you paid.

Then there is the scam email that claims to be from a lawyer or bank representative advising that a long-lost relative of yours has died and left you a huge **inheritance**. Scammers can tell such genuine sounding stories that you could be tricked into providing personal documents and bank account details so that you can confirm their identity and claim your inheritance. The “inheritance” is likely to be non-existent and, as well as losing any money you might have paid to the scammer in fees and taxes, you could also risk having your identity stolen.

If you or your business is selling products or services online or through newspaper classifieds, you may be targeted by an **overpayment** scam. In response to your advertisement, you might receive a generous





offer from a potential buyer and accept it. You receive payment by cheque or money order, but the amount you receive is more than the agreed price. The buyer may tell you that the overpayment was simply a mistake or they may invent an excuse, such as extra money to cover delivery charges. If you are asked to refund the excess amount by money transfer, be suspicious. The scammer is hoping that you will transfer the refund before you discover that their cheque or money order was counterfeit. You will lose the transferred money as well as the item if you have already sent it.

!	PROTECT YOURSELF
REMEMBER	If you have been approached by someone asking you to transfer money for them, it is probably a scam.
CAUTION	Never send money, or give credit card or online account details to anyone you do not know and trust.
THINK	Don't accept a cheque or money order for payment for goods that is more than what you agreed upon. Send it back and ask the buyer to send you payment for the agreed amount before you deliver the goods or services.
INVESTIGATE	Examine the information on the Canadian Anti-Fraud Centre website for information on how to protect yourself against money transfer scams.
ASK YOURSELF	Is it really safe to transfer money for someone I do not know?

# INTERNET SCAMS

A lot of Internet scams take place without the victim even noticing. You can greatly reduce the chances of being scammed on the Internet if you follow some simple precautions.

## WHAT TO LOOK FOR

Scammers can use the Internet to promote fraud through unsolicited or junk emails, known as **spam**. Even if they only get a handful of replies from the millions of emails they send out, it is still worth their while. Be wary of replying, even just to “unsubscribe”, because that will give a scammer confirmation that they have reached a real email address.

Any email you receive that comes from a sender you do not know, is not specifically addressed to you, and promises you some benefit is likely to be spam.


**Malicious software**—also referred to as malware, spyware, key loggers, trojan horses, or trojans—poses online security threats. Scammers try to install this software on your

computer so that they can gain access to files stored on your computer and other personal details and passwords.

Scammers use a wide range of tricks to get their software onto your computer. They may trick you into clicking on a link or pop-up message in a spam email, or by getting you to visit a fake website set up solely to infect people’s computers.

**Phishing** scams are all about tricking you into handing over your personal and banking details to scammers. The emails you receive might look and sound legitimate but in reality genuine organizations like a bank or a government authority will never expect you to send your personal information by an email or online.





Scammers can easily copy the logo or even the entire website of a genuine organization. So don't just assume an email you receive is legitimate. If the email is asking you to visit a website to "update", "validate" or "confirm" your account information, be sceptical.

Delete phishing emails. They can carry viruses that can infect your computer. Do not open any attachments or follow any links in phishing emails.

**Online auctions** and **Internet shopping** can be a lot of fun and can also help you find good deals. Unfortunately, they also attract scammers.

Scammers will often try to get you to deal outside of online auction sites. They may claim the winner of an auction that you were bidding on has pulled out and offer the item to you. Once you have paid, you will never hear from them again and the auction site will not be able to help you.



## PROTECT YOURSELF

### REMEMBER

If you choose to shop online or participate in online auctions, make sure you know about refund policies and dispute-handling processes, and be careful that you are not overcharged. Also, you may want to use an escrow service, such as PayPal. This service will hold your payment and only release it to the seller once you have confirmed that you received what you paid for. There is usually a small fee for this service. A legitimate bank or financial institution will never ask you to click on a link in an email or send your account details through an email or website.

### CAUTION

Never buy from bidders with poor ratings on auction sites, and do your best to ensure that you are only making purchases from genuine shopping sites. Never provide your personal, credit card or account information unless you are certain the site is genuine.

### THINK

Don't reply to spam emails, even to unsubscribe, and do not click on any links or call any telephone number listed in a spam email. Make sure you have current protective software or get advice from a computer specialist.

### INVESTIGATE

If an email or pop-up offers you a product or service that genuinely interests you and it seems reasonable, be sure that you understand all the terms and conditions and costs involved before making a purchase or providing your details.

### ASK YOURSELF

By opening this suspect email, will I risk the security of my computer? Are the contact details provided in the email correct? Telephone your bank or financial institution to ask whether the email you received is genuine.

# MOBILE PHONE SCAMS

Mobile phone scams can be difficult to recognize. Be wary of somebody who talks as if they know you or of redialling a missed call from an unknown number—there may be hidden charges.

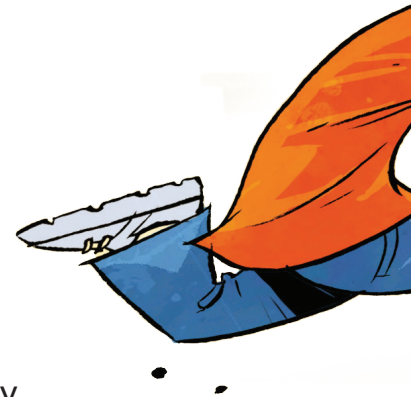
## WHAT TO LOOK FOR

**Ringtone** scams might attract you with an offer of a free or low-cost ringtone. What you may not realize is that by accepting the offer, you may actually be subscribing to a service that will keep sending you ringtones—and charging you a premium rate for them. There are many legitimate companies selling ringtones, but there are also scammers who will try to hide the true cost of taking up the offer.

Scammers either don't tell you that your request for the first ringtone is actually a subscription to a ringtone service, or it may be obscured in fine print related to the offer. They also make it difficult for you to stop the service. You have to actively "opt out" of the service to stop the ringtones and the associated charges.

**Missed call** scams start by scammers calling your phone and hanging up so quickly that you can't answer the call in time. Your phone registers a missed call and you probably won't recognize the number. You may be tempted to call the number to find out who called you. If it is a scam, you will be paying premium rates for the call without knowing.

**Text message** scams work in a similar way, but through a Short Message Service (SMS). Scammers send you a text message from a number you may not recognize, but it sounds like it is from a friend—for instance: "Hi, it's John. I'm back! When are you free to catch up?" If you reply out of curiosity, you might be charged at premium rate for SMS messages (sometimes as much as \$4 for each message sent and/or received).





An **SMS contest** or **SMS trivia scam** usually arrives as a text message or in an advertisement and encourages you to take part in a trivia contest for a great prize. All you need to do is answer a certain number of questions correctly. The scammers make money by charging extremely high rates for the messages you send and any further messages they send to you. With trivia scams, the first set of questions will be very easy. This is meant to encourage you to keep playing. However, the last one or two questions that you need to answer to claim your “prize” could be very difficult or impossible to answer correctly.

!	PROTECT YOURSELF
REMEMBER	Text “STOP” to end unwanted text messages or to end unwanted subscriptions.
CAUTION	Never reply to text messages offering you free ringtones or missed calls from numbers that you do not recognize.
THINK	Don’t call or text phone numbers beginning with 1-900 unless you are aware of the cost involved, and carefully read any terms and conditions when texting short codes.
INVESTIGATE	Read all the terms and conditions of an offer very carefully. Services offering free or very cheap products often have hidden costs.
ASK YOURSELF	Do I know how to stop any subscription service I want to sign up to?

# HEALTH AND MEDICAL SCAMS

Medical scams prey on human suffering. They offer solutions where none exist or promise to simplify complex health treatments.

## WHAT TO LOOK FOR

**Miracle cure** scams offer a range of products and services that can appear to be legitimate alternative medicines, usually promising quick and effective remedies for serious medical conditions. The treatments claim to be effective against a very wide range of ailments and are often promoted using testimonials from people who have used the product or service and have been “cured”.

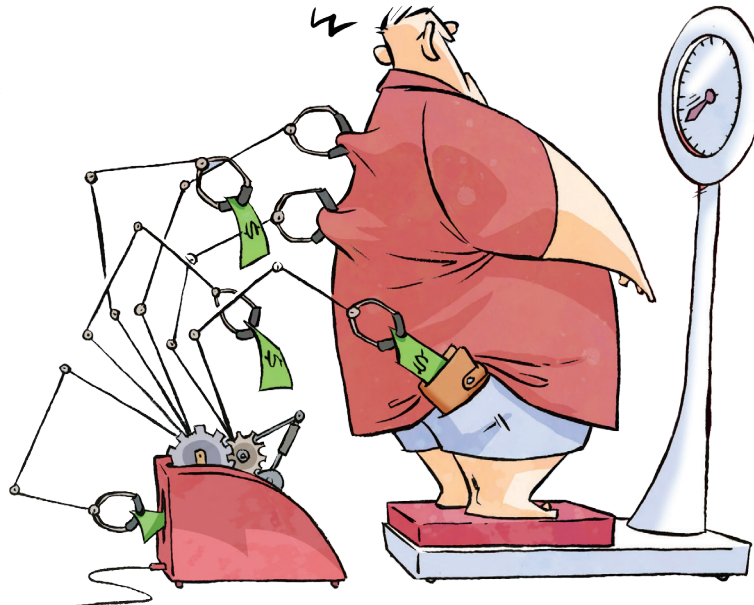
**Weight loss** scams promise dramatic weight loss with little or no effort. This type of scam may involve an unusual or restrictive diet, revolutionary exercise or “fat-busting” devices, or breakthrough products such as pills, patches or creams. The products are promoted with the use of false claims such as “lose 10 kilos in

10 days” or “lose weight while you sleep”, and often require large advance payments or that you enter into a long-term contract to participate in the program.

**Fake online pharmacies** use the Internet and spam emails to offer drugs and medicine at very cheap prices and/or without the need for a prescription from a doctor. If you use such a service and you actually do receive the products in response to your order, there is no guarantee that they are the real thing.

There are legitimate online pharmacies. These businesses will have their full contact details listed on their website and will also require a valid prescription before they send out any medicine that requires one.

HEY SHIRL! I CAN  
ACTUALLY SEE MYSELF  
LOSING WEIGHT!



## PROTECT YOURSELF

### REMEMBER

There are no magic pills, miracle cures or safe options for serious medical conditions or rapid weight loss.

### CAUTION

Never commit to anything under pressure.

### THINK

Don't trust an unsubstantiated claim about medicines, supplements or other treatments. Consult your healthcare professional.

### INVESTIGATE

Check for published medical and research papers to verify the accuracy of the claims made by the promoters.

### ASK YOURSELF

If this really is a miracle cure, wouldn't my healthcare professional have told me about it?

# EMERGENCY SCAMS

Emergency scams target grandparents and play upon their emotions to rob them of their money.

## WHAT TO LOOK FOR

In the typical scenario of an **emergency** scam, a grandparent receives a phone call from a scammer claiming to be one of his or her grandchildren. Callers go on to say that they are in some kind of trouble and need money immediately. They claim to have been in a car accident, are having trouble returning from a foreign country or they need bail money.

You may get a call from two people, one pretending to be your grandchild and the other pretending to be either a police officer or a lawyer. Your “grandchild” asks you questions during the call, getting you to volunteer personal information.

Callers say that they don’t want other family members to find out what has happened. You will be asked to wire some money through a money transfer company. Often, victims don’t verify the story until after the money has been sent.

In some cases, scammers pretend to be your old neighbour or a friend of the family, but for the most part, the emergency scam is directed at grandparents.





## PROTECT YOURSELF

### REMEMBER

Scammers are counting on the fact that you will want to act quickly to help your loved ones in an emergency.

### CAUTION

Never send money to anyone you don't know and trust. Verify the person's identity before you take any steps to help.

### THINK

Don't give out any personal information to the caller.

### INVESTIGATE

Ask the person questions that only your loved one would be able to answer. Call the child's parents or friends to verify the story.

### ASK YOURSELF

Does the caller's story make sense?

# DATING AND ROMANCE SCAMS

Despite the many legitimate dating websites operating in Canada, there are many dating and romance scams as well. Dating and romance scams try to lower your defences by appealing to your romantic and compassionate side.

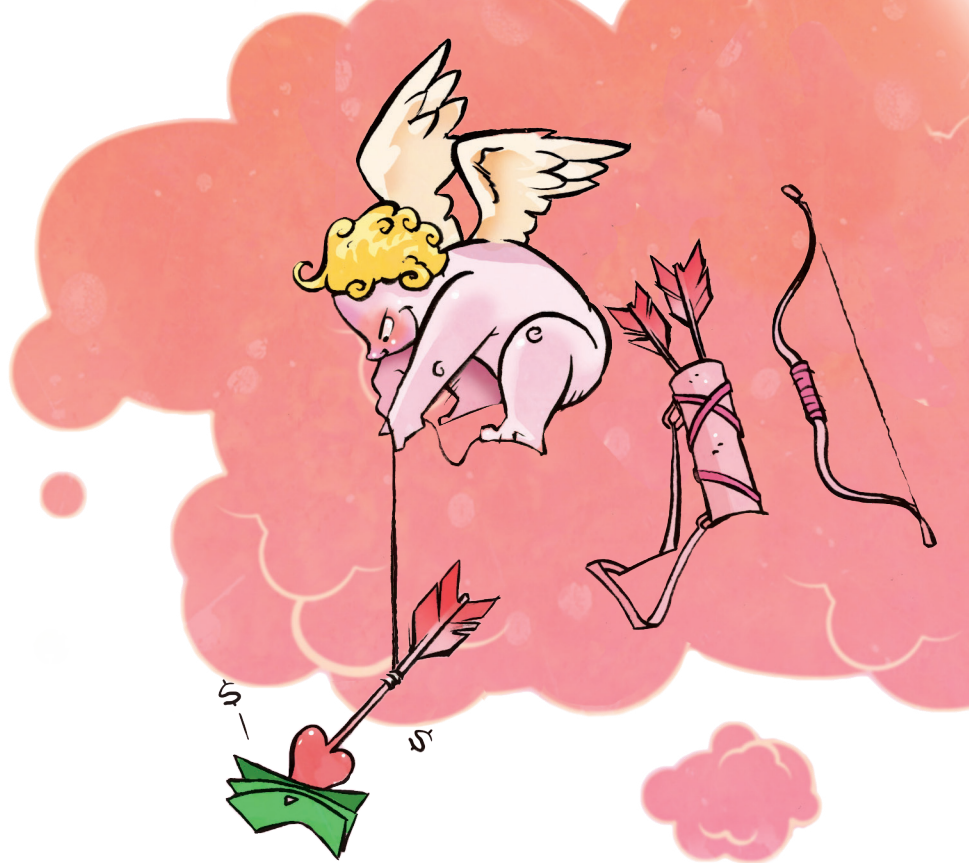
## WHAT TO LOOK FOR

Some **dating and romance** scams work by setting up a dating website where you pay for each email or message you send and receive. The scammer will try to hook you in by continuing to send you vague-sounding emails filled with talk of love or desire. The scammer might also send emails filled with details of their home country or town that do not refer to you much at all. These are attempts to keep you writing back and paying money for use of the scammer's dating website.

Even on a legitimate dating site, you might be approached by a scammer—perhaps someone who claims to have a very sick family member or who is in the depths of despair (often these scammers claim to be from Russia

or Eastern Europe). After they have sent you a few messages, and maybe even a glamorous photo, you will be asked (directly or more subtly) to send them money to help their situation. Some scammers even arrange to meet with you, in the hope that you give them presents or money—and then they disappear.

In other cases, scammers will try to build a friendship with you, perhaps even sending you flowers or other small gifts. After building a relationship, the scammer will tell you about a large amount of money they need to transfer out of their country, or that they want to share with you. They will then ask for your banking details or money for an administrative fee or tax that they claim needs to be paid to free up the money.



!	PROTECT YOURSELF
REMEMBER	Check website addresses carefully. Scammers often set up fake websites with very similar addresses to legitimate dating websites.
CAUTION	Never send money, or give credit card or online account details to anyone you do not know and trust.
THINK	Don't give out any personal information in an email or when you are chatting online.
INVESTIGATE	Make sure you only use legitimate and reputable dating websites.
ASK YOURSELF	Would someone I have never met really declare their love for me after only a few letters or emails?

# CHARITY SCAMS

Charity scams take advantage of people's generosity and kindness by asking for donations to a fake charity or by impersonating a real charity.

## WHAT TO LOOK FOR

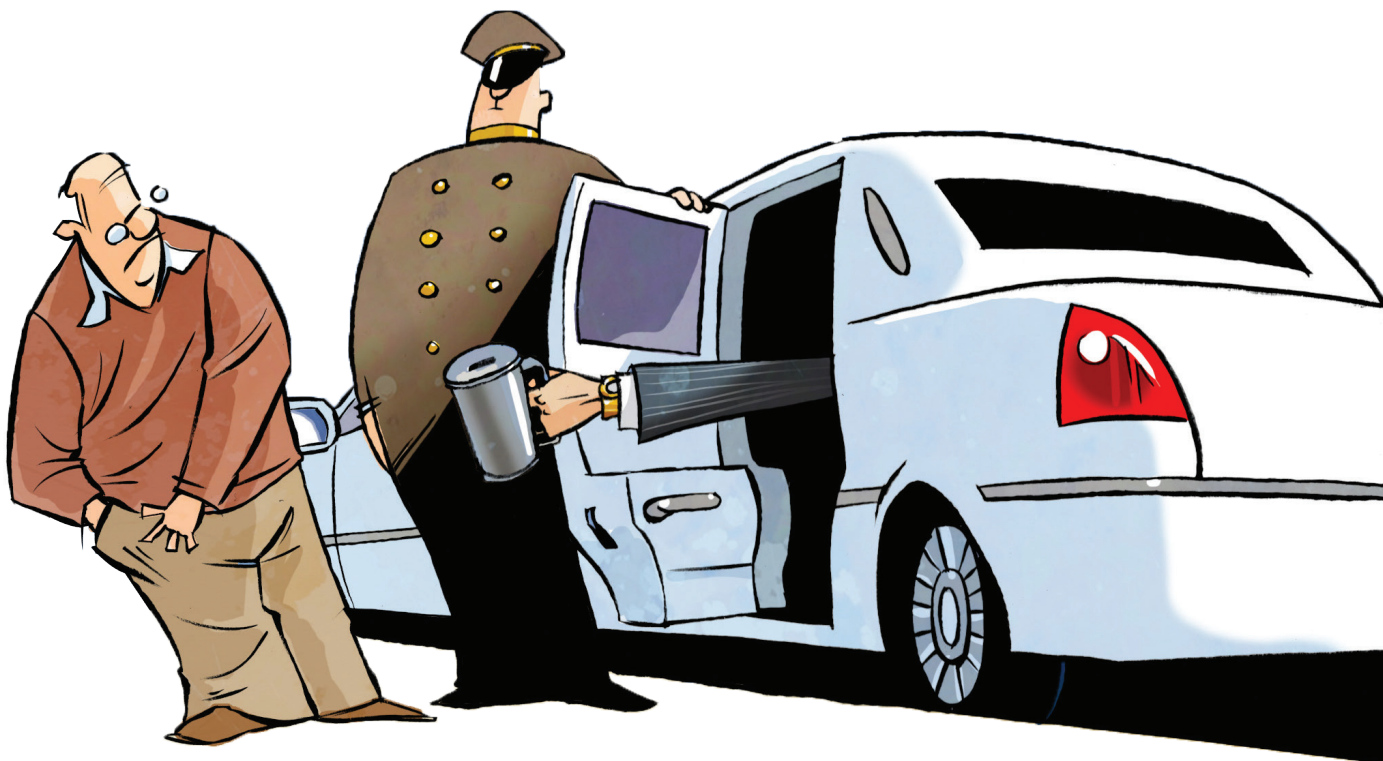
**Charity** scams involve scammers collecting money by pretending to be a real charity. The scammers can approach you in many different ways—on the street, at your home, over the phone, or on the Internet. Emails and collection boxes may even be marked with the logos of genuine charities.

Often, the scammer will exploit a recent natural disaster or famine that has been in the news. Other scammers play on your emotions by pretending to be from charities that help children who are ill.

Scammers can try to pressure you to give a donation and refuse to provide details about the charity, such as their address or their contact details. In other cases, they may simply provide false information.

Not only do these scams cost people money; they also divert much needed donations away from legitimate charities and causes. All registered charities in Canada are overseen by the Canada Revenue Agency and listed in its database. You can also contact your local Better Business Bureau to see if they have any information about the organizations that interest you. If the charity is genuine and you want to make a donation, get the charity's contact details from the phone book or a trusted website.

If you do not want to donate any money, or you are happy with how much you may have donated to charities already, simply ignore the email or letter, hang up the phone, or say no to the person at your door. You do not have to give any money at all.



## PROTECT YOURSELF

### REMEMBER

If you have any doubts at all about the person asking for money, do not give them any cash, credit card or bank account details.

### CAUTION

Never give out your personal, credit card or online account details over the phone unless you made the call and the phone number came from a trusted source.

### THINK

If in doubt, approach an aid organization directly to make a donation or offer support.

### INVESTIGATE

Search the Canada Revenue Agency database to check that the charity that has approached you is genuine.

### ASK YOURSELF

How and to whom would I like to make a contribution?

## JOB AND EMPLOYMENT SCAMS

Job and employment scams target people looking for a job. They often promise a lot of income—sometimes they even guarantee it—for little or no effort.

### WHAT TO LOOK FOR

**Work-from-home** scams are often promoted through spam emails or advertisements online or in newspaper ads. Most of these advertisements are not real job offers. Many of them are fronts for illegal money-laundering activity or pyramid schemes.

You might get an email offering a job where you use your bank account to receive and pass on payments for a foreign company. Or you might be offered a job as a “secret shopper” hired to test the services of a cheque-cashing or a money transfer company. Some “job offers” promise that you will receive a percentage commission for each payment you pass on. Sometimes, scammers are just after your bank account details so they can access your account. They might also send you a

counterfeit cheque along with instructions for you to cash the cheque and transfer a portion of the sum over a money transfer service.

A **guaranteed employment** or **income** scam claims to guarantee you either a job or a certain level of income. The scammers usually contact you by spam email and the offers often involve the payment of an up-front fee for a “business plan”, certain start-up materials or software.

There is a range of scams promoted as **business opportunities**. You may be required to make an upfront payment (for something that does not work or is not what you expected) or to recruit other people to the scheme (refer to pyramid schemes on page 4).



## PROTECT YOURSELF

### REMEMBER

There are no shortcuts to wealth—the only people that make money are the scammers.

### CAUTION

Never send your bank account or credit card details to anybody you do not know and trust. If you cash the cheque and it turns out to be counterfeit, you could be held accountable for the entire monetary loss by your bank.

### THINK

Don't make any decisions without carefully researching the offer. Seek independent advice before making a decision.

### INVESTIGATE

Beware of products or schemes claiming to guarantee income and job offers requiring payment of an upfront fee or sending money through a money transfer service. Make sure any franchise business opportunity is legitimate.

### ASK YOURSELF

Did I get all the details in writing before paying or signing anything?



# SMALL BUSINESS SCAMS

Scams that target small businesses can come in a variety of forms—from bills for advertising or directory listings that were never ordered to dubious office supply offers.



## WHAT TO LOOK FOR

**Small business** operators and individuals with their own Internet sites continue to be confused and caught by unsolicited letters warning them that their Internet domain name is due to expire and must be renewed, or offering them a new domain name similar to their current one.

If you have registered a domain name, be sure to carefully check any domain name renewal notices or invoices that you receive. While the notice could be genuine, it could also be from another company trying to sign you up, or it could be from a scammer.

- Check that the renewal notice matches your current domain name exactly. Look out for small differences—for example, “.com” instead of “.ca” or missing letters in the URL address.

- Check that the renewal notice comes from the company with which you originally registered your domain name.
- Check your records for the actual expiry date for your existing domain name.

A **directory listing** or **unauthorized advertising** scam tries to bill a business for a listing or advertisement in a magazine, journal or business directory, or for an online directory listing.

The scam might come as a proposal for a subscription disguised as an update of an existing listing in a business directory. You might also be led to believe that you are responding to an offer for a free listing when in fact it is an order for a listing requiring later payment.



Another common approach used by scammers is to call a firm asking to confirm details of an advertisement that they claim has already been booked. The scammer might quote a genuine entry or advertisement your business has had in a different publication or directory to convince you that you really did use the scammer's product.

Be wary of **order forms** offering advertising opportunities in business directories. These order forms may look like they originate from a well-known supplier of directory advertising, when they don't.

An **office supply** scam involves you receiving and being charged for goods that you did not order. These scams often involve goods or services that you regularly order—for example, paper, printing supplies, maintenance supplies or advertising.

You might receive a phone call from someone falsely claiming to be your "regular supplier", telling you that the offer is a "special" or "available for a limited time", or pretending to only confirm your address or existing order. If you agree to buy any of the supplies offered to you, they will often be overpriced and of bad quality.

!	PROTECT YOURSELF
REMEMBER	Make sure that the people processing the invoices or answering telephone calls are aware of these scams. They will most often be the point of contact for the scammers. Always check that goods or services were both ordered and delivered before paying an invoice.
CAUTION	Never give out or update any information about your business unless you know what the information will be used for.
THINK	Don't agree to a business proposal over the phone—always ask for an offer in writing. Limit the number of people in your business that have access to funds and have the authority to approve purchases.
INVESTIGATE	Effective management procedures can go a long way towards preventing these scams from succeeding. Having clearly defined procedures for the verification, payment and management of accounts and invoices is an effective defence against these types of scams.
ASK YOURSELF	If a caller claims that I have ordered or authorized something and I do not think it sounds right, shouldn't I ask for proof?

## SERVICE SCAMS

Many Canadians are being targeted by individuals claiming to offer reduced rates or deals for various services.

### WHAT TO LOOK FOR

These scams typically involve individuals that make offers for telecommunications, Internet, finance, medical and energy services. This category of scams may also include offers such as extended warranties, insurance, and door-to-door sales.

The two most reported service scams targeting Canadians are the **antivirus software** scam and **credit card interest rate reduction** scams.

The scammers involved in the antivirus software scam promise to repair your computer over the Internet. This can involve the installation of software or permission to have remote access to your computer. Payment for the software or repair is typically made by credit card.

Downloading software from an unknown source or allowing someone to remotely access your computer is risky. Scammers could use malicious software to capture your personal information such as user names and passwords, bank account information, identity information, etc.

Everyone likes to get a deal and scammers know this. The people behind credit card interest rate reduction scams often impersonate financial institutions and claim to negotiate with credit card companies to lower your interest rates. They guarantee they can save you thousands of dollars in interest. The caller will tell you that the lower interest rates are for a limited time only and that you need to act now.



You might receive an automated call, prompting you to “press 1” and provide personal information, such as your date of birth and credit card number. You will also be asked to pay a fee up front for the service. The scammers will use this information to make purchases on your credit card or to access cash advances.

!	PROTECT YOURSELF
REMEMBER	Only your service provider can offer you a better rate or price for their services.
CAUTION	Be wary of unsolicited calls from people offering a great deal “for a limited time only”.
THINK	Don’t give out your credit card number over the phone unless you made the call and the number came from a trusted source.
INVESTIGATE	If a caller claims to represent your bank, telephone your bank to ask whether the offer you received is genuine.
ASK YOURSELF	By offering up this information, am I putting myself at risk?

# HANDY HINTS TO PROTECT YOURSELF

## PROTECT YOUR IDENTITY

- Only give out your personal details and information where it is absolutely necessary and when you trust the person you are speaking to or dealing with.
- Destroy personal information: don't just throw it out. You should cut up or shred old bills, statements or cards—for example, credit cards and ATM cards.
- Treat your personal details like you would treat money: don't leave them lying around for others to take.

## MONEY MATTERS

- Never send money to anyone that you don't know and trust.
- Do not send any money or pay any fee to claim a prize or lottery winnings.
- "Jobs" asking you to simply use your own bank account to transfer money for somebody could be a front for money-laundering activity. Money laundering is a serious criminal offence.
- Avoid transferring or wiring any refunds or overpayments back to anyone you do not know.

## THE FACE-TO-FACE APPROACH

- If someone comes to your door, ask to see some identification. You do not have to let them in, and they must leave if you ask them to.
- Before you decide to pay any money, if you are interested in what a door-to-door salesperson has to offer, take the time to find out about their business and their offer.

- Contact the Competition Bureau, provincial and territorial consumer affairs offices or the Better Business Bureau of your province or territory if you are unsure about a seller that comes to your door. See pages 29 and 30 for contact information.

## TELEPHONE BUSINESS

- If you receive a phone call from someone you do not know, always ask for the name of the person you are speaking to and who they represent. Verify this information by calling the company yourself.
- Do not give out your personal, credit card or online account details over the phone unless you made the call and the phone number came from a trusted source.
- It is best not to respond to text messages or missed calls that come from numbers you do not recognize. Be especially wary of phone numbers beginning with 1-900. These may be charged at a higher rate than other numbers and can be very expensive.

## EMAIL OFFERS

- Never reply to a spam email, even to unsubscribe—often, this just serves to "verify" your address to scammers. The best course of action is to delete any suspicious emails without opening them.
- Turn off the "viewing pane" as just viewing the email may send a verification notice to the sender that yours is a valid email address.
- Legitimate banks and financial institutions will never ask you for your account details in an email or ask you to click on a link in an email to access your account.

- Never call a telephone number or trust other contact details that you see in a spam email.

## INTERNET BUSINESS

- Install software that protects your computer from viruses and unwanted programs and make sure it is kept current. If you are unsure, seek the help of a computer professional.
- If you want to access a website, use a bookmarked link to the website or type the address of the website into the browser yourself. Never follow a link in an email.
- Check website addresses carefully. Scammers often set up fake websites with addresses very similar to legitimate websites.
- Beware of websites offering “free” downloads (such as music, adult content, games and movies). Downloading these products may install harmful programs onto your computer without you knowing.
- Avoid clicking on pop-up ads—this could lead to harmful programs being installed on your computer.
- Never enter your personal, credit card or online account information on a website that you are not sure is genuine.
- Never send your personal, credit card or online banking details through an email.
- Avoid using public computers (at libraries or Internet cafes) to do your Internet banking or online shopping.
- When using public computers, clear the history and cache of the computer when you finish your session.
- Be careful when using software on your computer that auto-completes online forms. This can give Internet scammers easy access to your personal and credit card details.
- Choose passwords that would be difficult for anyone else to guess—for example, passwords that include letters and numbers. You should also regularly change passwords.
- When buying anything online, print out copies of all transactions and only pay via a secure site. If using an Internet auction site, note the ID numbers involved and read all the security advice on the site first.

# SCAMS AND YOU: WHAT TO DO IF YOU GET SCAMMED!

Canadian authorities may not always be able to take action against scams, even if it seems like a scammer might have broken the law.

## REDUCING THE DAMAGE

Although it may be hard to recover any money that you have lost to a scam, there are steps you can take to **reduce the damage** and avoid becoming a target for a follow-up scam. The more quickly you act, the greater your chance of reducing your losses.

**Report a scam.** By reporting the scam to authorities, they may be able to warn other people about the scam and minimize the chances of the scam spreading further. You should also warn your friends and family of any scams that you come across. Details on how to report a scam are on pages 29 and 30 of this publication.

## IF YOU HAVE BEEN TRICKED INTO SIGNING A CONTRACT OR BUYING A PRODUCT OR SERVICE

Contact your provincial or territorial consumer affairs office and consider getting independent advice to examine your options: there may be a cooling-off period or you may be able to negotiate a refund.

## IF YOU THINK SOMEONE HAS GAINED ACCESS TO YOUR ONLINE ACCOUNT, TELEPHONE BANKING ACCOUNT OR CREDIT CARD DETAILS

Call your financial institution immediately so they can suspend your account and limit the amount of money you lose. Credit card companies may also be able to perform a “charge back” (reverse the transaction) if they believe that your credit card was billed fraudulently.

Do not use contact details that appear in emails or on websites that you are suspicious of—they will probably be

fake and lead you to a scammer. You can find legitimate contact details in the phone book, an account statement or on the back of your ATM card.

## IF THE SCAM RELATES TO YOUR HEALTH

Stop taking any pills or substances that you are not sure about. See a doctor or other qualified medical professional as soon as you can. Be sure to tell them about the treatment that the scammer sold (take along any substances, including their packaging). Also tell them if you have stopped any treatment that you were taking before the scam.

## IF YOU HAVE SENT MONEY TO SOMEONE THAT YOU THINK MAY BE A SCAMMER

If you sent your credit card details, follow the instructions in the section opposite.

If you sent money through an electronic funds transfer (over the Internet), contact your financial institution immediately. If they have not already processed the transfer, they may be able to cancel it.

If you sent a cheque, contact your financial institution immediately. If the scammer hasn’t already cashed your cheque, they may be able to cancel it.

If you sent money through a wire service (such as Western Union or Money Gram), contact the wire service immediately. If you are very quick, they may be able to stop the transfer.

### IF YOU HAVE BEEN TRICKED BY A DOOR-TO-DOOR SELLER

You may be protected by laws that provide you with a “cooling-off” period, during which you can cancel an agreement or contract that you signed. Contact your provincial or territorial consumer affairs office for advice about door-to-door sales laws.

### IF YOU HAVE BEEN SCAMMED USING YOUR COMPUTER

If you were using your computer when you got scammed, it is possible that a virus or other malicious software is still on your computer. Run a full system check using reliable security software.

If you do not have security software (such as virus scanners and a firewall) installed on your computer, a computer professional can help you choose what you need.

Scammers may have also gained access to your online passwords. Change these using a secure computer.

### IF THE SCAM INVOLVES YOUR MOBILE PHONE

Call your telephone provider and let them know what has happened.

## GETTING HELP AND REPORTING A SCAM

The best agency to contact depends on where you live and what type of scam is involved.

**If you think you have spotted a scam or have been targeted by a scam, there are a number of government and law enforcement agencies in Canada that you can contact for advice or to make a report. This may help you and prevent others from being ripped off by scam operators.**

Canadian Anti-Fraud Centre  
[www.antifraudcentre.ca](http://www.antifraudcentre.ca)  
1-888-495-8501

The Competition Bureau's Information Centre  
[www.competitionbureau.gc.ca](http://www.competitionbureau.gc.ca)  
1-800-348-5358

### LOCAL SCAMS

#### Contact your local consumer affairs office

Your local consumer affairs office is best placed to investigate 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* on the Office of Consumer Affairs website.

[www.consumerhandbook.ca](http://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, credit or deposit accounts.

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



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

[www.securities-administrators.ca](http://www.securities-administrators.ca)

## REPORTING BANKING AND CREDIT CARD SCAMS

### Contact your bank or financial institution

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

Make sure that the telephone number you use is from the phone book, your account statement or the back of your credit or ATM card.

## REPORTING SPAM EMAILS AND SMS

Many scams arrive by email and SMS. Visit [www.fightspam.gc.ca](http://www.fightspam.gc.ca) for information on Canada's anti-spam legislation.

Fraudulent (or "phishing") emails requesting personal details can also be reported to the bank, financial institution or other organization concerned (be sure to use a phone number or email address that did not appear in the email to make your report).

## REPORTING FRAUD, THEFT AND OTHER CRIMES

### Contact the police

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

If you are the victim of fraud—you have suffered a loss because of someone's dishonesty or deception—you should consider contacting your local police (particularly if the amount involved is significant).

You should definitively contact the police if you have had your property stolen or have been threatened or assaulted by a scammer.

You may also contact one of the following organizations:

Canadian Council of Better Business Bureaus  
[www.ccbbb.ca](http://www.ccbbb.ca)

Canada Revenue Agency—Charities Directorate  
[www.cra-arc.gc.ca](http://www.cra-arc.gc.ca)  
1-800-267-2384

Your local police, credit card companies, banks, and provincial records offices.

Credit bureaus can put a fraud alert on your account, which will alert lenders and creditors of potential fraud:

Equifax: 1-800-465-7166  
TransUnion: 1-866-525-0262



