



SCAM PROTECTION



# Fraud

Recognize It.

Report It.

Stop It.

## The Face of Fraud: It's not who you think.

Believe it or not, there is no typical fraud victim in Canada, but research finds that fraud victims are likely to be educated, informed, relatively affluent and involved in their communities.

Your risk of becoming a fraud victim is not linked to your age, race, income or geographic location. Scammers don't care about any of that – they just want your money.

## You wouldn't fall for it?

Thousands of Canadians are defrauded each year. Scam artists are up to date and well-organized. They use the latest trends and sophisticated techniques:

- Professional marketing materials.
- Well-crafted and researched telephone scripts, which are traded among criminals.
- Putting you at ease with their friendly tone and “generous” offer.
- Having believable answers ready for your tough questions.
- Impersonating legitimate businesses, charities, and causes.
- Expertly using your own emotions against you.
- These are professional criminals. They know what they're doing and, unfortunately for their victims, they do it well.
- The price for a product is much less than the price for the same product on the open market.
- You are offered a large payment or reward in exchange for allowing the use of your financial account – often to deposit cheques or transfer money.

# Identity theft steals your good name, your money – even your self-respect

Protect yourself. Don't give out your social insurance or driver's licence numbers on the phone or Internet. Crooks use them to steal your money and commit crimes in your name. Check your credit report every year.

## **FRAUD**

**RECOGNIZE IT • REPORT IT • STOP IT**

## Don't fall for a winning prize scam

A call says you won a big lottery prize but you must send money before you can collect. It is a fraud and you will lose your money! Hang up and call PhoneBusters™, The Canadian Anti-fraud Call Centre at 1-888-495-8501.

Legitimate lottery and sweepstakes administrators never charge fees to deliver your prize. This is one of the most common scams – if you send money you will never get it back.

### **FRAUD**

**RECOGNIZE IT • REPORT IT • STOP IT**

## You can protect yourself

Identity theft is the fastest-growing type of fraud. Crooks can do bad things with your good name. Protect your precious personal information. Ask all marketing, research or charity callers for:

- Detailed, written information that you can check yourself.
- Time to think about the offer. Scam artists pressure you for an answer, saying the offer will expire or go to the next person if you don't act now.
- Valid references and the means to contact them.
- A call-back number. But beware – a crook can give you a number where a colleague is standing by to finish taking your money.
- Shred unwanted personal documents such as transaction records, credit applications, insurance forms, cheques, financial statements and tax returns.

## “Phishing” – What is phishing?

Phishing attacks use ‘spoofed’ (look alike) email messages and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social insurance numbers (SIN), etc. By hijacking the trusted brands of well-known financial institutions, online retailers and credit card companies, phishers are able to convince up to 5% of recipients to respond to them.

## What should Internet users do about phishing schemes?

Internet users should follow three simple rules when they see email messages or websites that may be part of a phishing scheme: **Stop, Look, and Call.**

1. **Stop.** Phishers typically include upsetting or exciting (but false) statements in their email messages with one purpose in mind. They want people to react immediately to that false information, by clicking on the link and inputting the requested data before they take time to think through what they are doing. Internet users however, need to resist that impulse to click immediately. No matter how upsetting or exciting the statements in the email may be, there is always enough time to check out the information more closely.
2. **Look.** Internet users should look more closely at the claims made in the email, think about whether those claims make sense, and be highly suspicious if the email asks for numerous items of personal information such as account numbers, usernames, or passwords.

For example:

- If the email indicates that it comes from a financial institution where you have a debit or credit-card account, but tells you that you have to enter your account information again, that makes no sense. Legitimate financial institutions already have their customer's account numbers in their records. Even if the email says a customer's account is being terminated, the real financial institution will still have that customer's account number and identifying information.
  - If the email says that you have won a prize or are entitled to receive some special "deal", but asks for financial or personal data, there is good reason to be highly suspicious. Legitimate companies that want to give you a real prize don't ask you for extensive amounts of personal and financial information before you're entitled to receive it.
3. **Call.** If the email or website purports to be from a legitimate company or financial institution, Internet users should call or email that company directly and ask whether the email or website is really from that company. To be sure that they are contacting the real company or institution where they have accounts, credit-card account holders can call the toll-free customer numbers on the backs of their cards, and financial institution customers can call the telephone numbers on their financial statements. Never call the number given in the email to confirm the contents validity as it will lead to the criminals who sent the email and they will verify whatever was said.

## FRAUD

RECOGNIZE IT • REPORT IT • STOP IT

# The Pitch Versus the Facts

## Is Your Credit Really Protected?

**The Pitch:** They say, “We’ll protect you from scammers who could run up huge debts on your credit cards without you knowing. Just send us your card numbers and our fee.”

**The Facts:** Offers of credit protection or “insurance” against fraud are just attempts to get your credit card numbers and your money. Call your credit card companies or your credit union first. If someone fraudulently uses your cards, most companies hold you responsible only for the first \$50, and many waive all losses.

## Do You Absolutely Need That Money?

**The Pitch:** A call, a letter or an email from a “highly-placed” official of a foreign government requests your assistance to transfer a large amount of money. If you can help, you’ll earn a huge fee!

**The Facts:** Beware of anyone asking you to deposit a cheque and return some of the money or send some of the money to someone else. Such cheques are often counterfeit. The deposit will look legitimate until the cheque bounces in a few days. Your financial institution will then ask you how you intend to cover the money you transferred to the scammers. It takes up to 21 days for a cheque to clear, so it’s essential that you ask your financial institution whether the cheque has cleared – not just whether the money is available. Businesses or anyone selling goods on the Internet or through the paper should be especially suspicious of cheques received for payment of goods that exceed the agreed upon amount of purchase and the request for return of the overpayment to the purchaser. Always wait for the cheque to clear prior to returning any overpayment as it is likely the cheque is either stolen or counterfeit.

## Nigerian Scam

**The Pitch:** A person will receive a call, letter or email stating that someone has money stuck in a foreign country and they are looking for outside assistance to get their money out. The person will be offered a large portion of the money if they help, sometimes in the millions of dollars. This person will then be told that they just need to provide their financial account information so that the money can be transferred to it, or they will be asked for an address to send a cheque to cover the costs of getting through the red tape for the release of funds. If the person provides the requested funds they will eventually be asked for more and more money to assist in getting the funds released or their account will be hacked and money transferred out. Sometimes a cheque is sent to a person and they are requested to cash it, keep their portion and wire the rest back to the criminal or a third party. In all cases the cheque they receive will be a counterfeit cheque and the member will lose the funds wired to the criminal. Letters or email messages for these types of scams are typically badly written with many spelling mistakes.

**The Facts:** Be skeptical of individuals representing themselves as Nigerian business people or foreign government officials asking for your help in placing large sums of money in overseas bank accounts. Do not believe the promise of large sums of money for your cooperation. Guard your account information carefully.

## You Pay to Play, But You Can't Win

**The Pitch:** A caller says you were automatically entered into a foreign lottery and you won a big prize! But you must act now and send fees to cover taxes and handling.

**The Facts:** Most legitimate lotteries do not call winners. If a caller requires you to pay an up-front fee to claim a prize, it's a scam. The only winner is the crook.

## Pre-qualified Never Means Prepay

**The Pitch:** You're told you've been "pre-qualified" for a low-interest loan or credit card, or to repair your bad credit even though financial institutions turn you down. They ask for your social insurance, driver's licence and financial account numbers – and a processing fee of several hundred dollars.

**The Facts:** Beware of advertisements or phone calls offering credit, especially if you have been turned down by financial institutions. Legitimate lenders never "guarantee" a card or loan before you apply. A legitimate pre-qualified offer means you've been selected to apply – you must still complete an application and you can still be turned down.

## Not So Special Delivery

**The Pitch:** Your business receives a "last chance" invoice for a listing in a "business directory". Or an invoice says an urgent delivery of photocopier or fax supplies is awaiting confirmation of your address. It appears that someone in your office ordered services or supplies but the bill hasn't been paid.

**The Facts:** Scam operators dupe many businesses into paying for goods and services they haven't ordered. They bet that many small business owners and their staff are just too busy to check that every invoice is legitimate. Carefully examine all invoices, even those under \$50.

## Con Job

**The Pitch:** An employment advertisement offers a work-at-home opportunity, multi-level marketing plan or other means to “be your own boss” and earn significantly higher income. Beware also of Internet job sites. Some of the job postings are made by organized crime and are meant only to set up phone interviews with individuals to gather personal information.

**The Facts:** Sending fees for job information or to be listed for jobs in Canada or abroad is risky. In many cases, scammers advertise all kinds of job opportunities from envelope stuffing to filling out forms, but all too often these ads make promises they don't keep. You lose more money instead of making more money. For a phone interview, if the interviewer asks too many personal questions you should be suspicious. A prospective employer does not need to know your social insurance number or your driver's licence number. Beware of odd questions that reveal too much personal information that could later be used to assume your identity. Full addresses should not be provided on an online posting, city and province should be sufficient. Never include your social insurance number on the resume.

### It's a rip-off! Here's the tipoff:

- The caller is more excited than you are.
- The caller demands an immediate answer but refuses to send you anything in writing.
- You must pay fees or buy a product before you can collect your prize or obtain credit.
- You are asked for credit card or financial account numbers, or copies of personal documents – but you get nothing in writing.
- You can only send payment by wire service or by courier. (This gets around the laws concerning mail fraud.)
- You receive an unexpectedly large cheque.
- Your business is invoiced for supplies or directory listings you did not order.

# FRAUD

RECOGNIZE IT • REPORT IT • STOP IT

## Deceptive telemarketers call you?

The right information can help you avoid falling for fraud. When a caller asks you to send money in order to claim a big prize, it's fraud! You'll lose your money. When a caller or Internet contact asks for your social insurance or driver's licence number, don't provide it! You could lose your identity and your money.

## Identity theft statement form available online

PhoneBusters, the Canadian Anti-Fraud Call Centre now offers a downloadable form for reporting identity theft on its website. It makes reporting easier and ensures the police have all the information they need.

Visit [www.phonebusters.com](http://www.phonebusters.com) and follow the link under the "Identity Theft" section.

## Your report is important

Talk to your credit union. Your credit union is often aware of the scams that are in circulation and can assist you in understanding whether the offer you have received is legitimate or not. However, your credit union is not a law enforcement agency so it is important to report any suspicions you may have or fraudulent losses you have experienced to them as well.

**If a scam artist contacts you or if you've been defrauded, call PhoneBusters at 1-888-495-8501.**

PhoneBusters will gather evidence; identify new trends and alert law enforcement in Canada and abroad. By reporting, you can prevent others from becoming victims and help put an end to fraud.