

Scams to Avoid

A People's Law School Publication

Contents

Introduction	1
Charity and Sales Scams	2
Loan and Credit Scams	4
Online and Computer Scams	6
Prize and Contest Scams	9
Romance and Relationship Scams	11
Work Scams	13
Identity Theft	14
If You've Been Scammed	16
Resources	19
Where to Get Help	19
Glossary	21
About	23
About this Publication	23

Introduction

A **scam** is an illegal or dishonest scheme to trick you out of your money. This publication helps you spot scams and guard against them. It covers 15 of the most common scams that affect British Columbians, explains the growing problem of identity theft, and tells you the steps to take if you have been the victim of a scam.

At People's Law School, we believe accurate, plain English information can help people take action to work out their legal problems. This publication explains in a general way the law that applies in British Columbia. **It is not intended as legal advice.** For help with a specific legal problem, contact a legal professional. Some sources of legal help are highlighted in the "Where to Get Help" section. We have tried to use clear language throughout. See the "Glossary" section for definitions of key legal terms, which are also bolded in the text.



	Visit the People's Law School website at www.peopleslawschool.ca ^[1] for more in-depth coverage of scams and how to deal with legal problems.
--	---

People's Law School

People's Law School is a non-profit society in British Columbia, dedicated to making the law accessible to everyone. We provide free education and information to help people effectively deal with the legal problems of daily life.

Scams to Avoid © People's Law School is, except for the images, licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International Licence.

References

[1] <http://www.peopleslawschool.ca>

Charity and Sales Scams

This information applies to British Columbia, Canada. Last reviewed for legal accuracy by People's Law School in March 2017.

Some people try to trick you into donating money to a fake charity or cheat you when you buy something.

Charity scams

A **charity scam** is when someone asks you to make a donation to a fake charity or pretends to be from a real charity.

They might approach you on the street, at your door, over the phone or on the internet. If they're collecting money for a fake charity, often the name will be similar to a legitimate and respected charity. Some will say their charity helps police, firefighters, children with cancer, or some other worthy cause. Some try to take advantage of a recent natural disaster such as an earthquake or flood.



You can check whether a charity that has approached you is genuine by searching over the Canada Revenue Agency's Registered Charities Listing ^[1].

Fake charities will typically try to pressure you to give a donation on the spot. If you do not want to donate any money, you don't have to. Simply ignore the email or letter, hang up the phone, or say "No thanks, I'm not interested" to the person at your door.

Free trial scams



"I saw an ad online for a diet pill called BurnFast. If I paid the \$1.95 shipping & handling charges, I could get a free trial. I decided to try it, and received a sample shipment of pills. A month later another shipment of pills arrived and my credit card was billed \$90 for my 'monthly supplies'. When I complained, BurnFast said I had agreed to a monthly subscription."

- Barney, Revelstoke

Ads for **free trial scams** promote any number of things - a miracle vitamin, a teeth whitener, a set of kitchen knives - by inviting you to try out the product for free or for a very low cost (such as if you cover the shipping and handling charges).

What they don't tell you is that when you sign up for the free trial, you may be signing a membership, subscription or service **contract** that allows the company to charge fees to credit cards.

Some "free trials" disguise the true nature of their offer, hiding the terms and conditions in small print or using pre-checked sign-up boxes as the default setting online. Often, they automatically enrol you in a club or subscription.



Review the terms of any "free trial" offer carefully before you provide any payment information. If you don't want to buy what you've tried, you will likely need to cancel or take some other action before the trial is up. If you don't, you may be agreeing to buy more products.

Door-to-door scams

Some people rely on old-fashioned techniques to try deceiving you. In a **door-to-door scam**, someone knocks on your door and offers a product or service, but their true goal is to steal from you. They will typically do this by convincing you to pay cash up-front for a service that is never provided. The service might be roofing your home, pruning your trees, or installing a security system.

If they actually perform the work, it will typically be substandard and there will be no way to contact them later. Their bill will often include items you did not agree to, and their "money-back guarantee" will be worthless.

Under BC law, if you sign a contract at your door, it is called a **direct sales contract**. The contract must contain a detailed description of the goods and services to be provided, an itemized purchase price, a notice of your cancellation rights, and many other details. You can cancel the contract by giving notice to the company within 10 days after receiving the contract. You don't have to have any reason for cancelling.



If you are considering an offer from someone who has come to your door, insist on a written contract. Take the time to read and understand it. If you are feeling pressured, do not sign anything. Close the door.

Preventing problems

Here are ways to reduce the risk of being the victim of a charity or sales scam.

Never pay at the door

Never give money or credit card information at the door. Take the time to do some research first.

Research the company

Ask for written information to be sent to you about the charity or company. Contact the Better Business Bureau to find out what they know of the charity or company (see the "Where to Get Help" section for contact details). See what other people are saying about them by searching online for the name of the organization and the word "reviews" or "complaints".



Image via www.istockphoto.com

Make sure you understand the offer


Take the time to understand all the terms and conditions and costs involved before making a purchase or donation.

Protect your personal information

Don't give out your credit or debit card information unless you are certain the company or charity is genuine.

Read your statements

Read your bank and credit card statements. That way you'll know right away if you're being charged for something you didn't authorize.

 *Scams to Avoid* © People's Law School is, except for the images, licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International Licence.

References

[1] <http://www.cra-arc.gc.ca/chrts-gvng/lstngs/menu-eng.html>

Loan and Credit Scams



This page is used in the Scams to Avoid Lesson Module, a law-related ESL lesson for newcomers to Canada.

This information applies to British Columbia, Canada. Last reviewed for legal accuracy by People's Law School in March 2017.

To trick you out of your money, some scams involve offers to loan you money or help you borrow money.

Loan scams

In a **loan scam**, a company tells you they can "guarantee" you a loan even if you have bad **credit** or no credit (that is, a poor history of paying back loans and paying bills). All you need to do is pay an upfront fee to "process the loan" or cover "insurance costs".

You send this "advance fee", but they don't send the promised loan. Instead, they keep your money and send you a letter saying that your loan application has been denied.

This is illegal in BC. It is against the law for a company to charge an advance fee to obtain a loan, even if that fee is described as the first or last month's payment.



Legitimate lenders never "guarantee" that you will qualify for a loan before a credit check is done. In a credit check, they look at your history of paying bills and repaying loans, which are detailed in a **credit report**. A legitimate lender would want to review your credit report before approving any loan.

Credit repair scams

The pitch goes something like this:

"Credit problems? You can now wipe your credit report clean of bankruptcies, judgments, foreclosures and lien payments. AND IT'S 100% LEGAL!"

This is a **credit repair scam**. It promises to help you improve your credit report. The detail in your credit report helps businesses, banks and others decide if you are likely to pay your bills on time. The scam typically urges you to dispute the negative information in your credit report or to set up a new credit identity for yourself.

In fact, there's no legal way to erase accurate negative information from within the last 5 years from your credit report. After 6 years, negative information can be purged from your credit report.

When accurate negative information is challenged, if the credit reporting agency cannot verify the information within a reasonable period of time, the information is removed. But it may be only temporarily. If the information is later verified, it will be placed back in your report.

Preventing problems

Here are ways to reduce the risk of being the victim of a loan or credit scam.

Know who you're dealing with


If you are seeking to borrow money, apply for loans through local banks and credit unions.

Research the company

See what other people are saying about the company. Search online for their name together with the word "reviews" or "complaints". Contact the Better Business Bureau to find out what they know of the company (see the "Where to Get Help" section for contact details).

Seek out help to improve your credit report

If you've got a poor credit history, get advice on how to improve your **credit score**. You can improve your score by improving your track record on managing credit. The Credit Counselling Society helps people learn how to manage their money and debt better. See the "Where to Get Help" section for contact details.

 *Scams to Avoid* © People's Law School is, except for the images, licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International Licence.

Online and Computer Scams



This page is used in the Scams to Avoid Lesson Module, a law-related ESL lesson for newcomers to Canada.

This information applies to British Columbia, Canada. Last reviewed for legal accuracy by People's Law School in March 2017.

Technology has opened up new opportunities for people with bad intentions to try to trick you out of your money.

Malware or spyware

You're browsing the internet. An online ad features an item you've been thinking of buying. You click on the ad to learn more. A window pops up on your computer saying "Your personal files are encrypted!" The only way to "release" them is by paying a steep fee. If you don't pay the fee in the next 72 hours, "you will never be able to recover your files".

This is an example of **malware**, which is software used to disrupt use of a device or gain access to sensitive information. Some malware is called **spyware** because it is installed on your device without you realizing it.

Scammers try to install this software on your device so they can fool you into paying them money or gain access to information stored on your device such as bank account details and passwords.

The installation of the software can be triggered in many ways - when you click on a link in an email, download a file from a website, or install free software.

In fact, it is illegal to install software programs on someone's device without the consent of the device owner or an authorized user (for example, a family member or employee).

Phishing emails

You get an email message that appears to be from your bank. The sender's name, the layout of the email, the logo - it's all the same as your bank's, at least on first look. The email says that your account has been compromised, and you need to visit a website to "verify" your account information. As you look more closely at the email, you see there are some typos, the logo is slightly off, and the address of the website is slightly different from your bank's website.

This email is fake. It has been sent by scammers pretending to be from your bank, trying to trick you into handing over personal and financial information. This is known as **phishing**. The email is being used as bait to "fish" for victims.

Once the scammers have your information such as bank account details, credit card numbers, and passwords, they use it to take your money and commit more **fraud**.



If an email asks you to visit a website to "update" or "confirm" your account information, be extremely cautious. Institutions like a bank or government agency will never expect you to submit your personal information online or by email.

Money transfer scams



"I got an email from a lawyer overseas. A person sharing my family name had died and left behind a large sum of money. The lawyer hadn't been able to locate any of the dead person's relatives. He suggested that, because I had the same family name, he could pay the inheritance to me. We could then split the money, rather than handing it over to the government. I just had to pay some taxes and legal fees, and to provide my bank details so they could deposit the money."
- Harry, Surrey

An email from overseas claims that an important event - such as an inheritance or a change of government - has resulted in a person having a large sum of money which needs to be transferred out of the country. The sender claims that if you help with the transfer, you can keep a portion of the money. If you reply to the email, the sender says you will receive your "reward" once you pay various "taxes and fees".

This is a **money transfer scam**. It is sometimes called a **Nigerian scam** or **419 fraud**, after the section of the Nigerian criminal code dealing with fraud.

There are many variations of the scam, but all aim to steal your money.

You will never be sent any of the money, and you will lose any amounts you pay in "taxes and fees".

Antivirus software scams



"I received a call from someone saying they were from Windows. The caller said my computer had been reported as having a virus that was infecting others. They told me to go to a website so they could fix it. Once I did, they took over the controls of my computer. They then told me that I would have to pay \$300 for the "repair". I pulled the power on my computer and brought it to a local company to fix it."
- Kathy, Nanaimo

One of the most reported scams targeting Canadians is the **antivirus software scam**. You get an email or phone call from a company that says your computer has a virus. They say they can "repair" your computer. This can involve installing software or "taking over" your computer to fix it.

The software they install turns out to be **malware** or **spyware** that enables the scammer to gain access to your personal information. Or the scammer insists on a payment for their "repair" before they turn the controls of your computer back over to you.



Never give control of your computer to a third party unless you can confirm they are a real representative of a company you trust. If you receive an unsolicited call from someone claiming to be from "Microsoft Support", "Windows" or "Apple", hang up. Technology companies do not make these kinds of calls.

Mobile phone scams

Many of the tricks scammers try with email and computers are also used on mobile phone users.

For example, scammers hide malware in games or apps that you can download on a smartphone. When you download the game or app, the malicious software is installed on your phone. It can then be used by the scammers to steal your personal and financial information.

Other scammers use the **missed call scam**. They call your phone and hang up so quickly that you can't answer the call in time. 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.

Preventing problems

Here are ways to reduce the risk of being the victim of an online or computer scam.

Protect your devices

Password protect your devices. On your cellphone, lock the keypad when you're not using it. Have software installed on your devices to prevent **spam**, **viruses**, and **spyware**. Keep that software up-to-date.

Be cautious using email

When using email, never click on a link in an email, even to log in to well-known sites such as Facebook or Twitter. Go to the site directly and log in there. Don't open an attachment in an email sent by someone you don't know.

Be cautious online


Don't click on links unless you trust the site you're on. Don't download files or applications unless you can verify the source. When you're using social media services such as Facebook or Twitter, be alert for scammers posing as a friend and trying to trick you into clicking on a link to a malicious site.

Erase information

Make sure your information is completely erased before you sell, recycle or discard your computer or cellphone. This involves more than deleting everything. To make sure that your private information is gone forever, you need to "wipe the hard drive" using special software. You can buy this software or have a professional do this for you.



Image via www.istockphoto.com

 *Scams to Avoid* © People's Law School is, except for the images, licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International Licence.

Prize and Contest Scams



This page is used in the Scams to Avoid Lesson Module, a law-related ESL lesson for newcomers to Canada.

This information applies to British Columbia, Canada. Last reviewed for legal accuracy by People's Law School in March 2017.

"Congratulations! You have just won a free holiday in sunny Mexico!" Tempting, no doubt. But all too often, offers of a "free" prize turn out to be scams.

Fake lottery scams

You get a letter in the mail. "You have won a car!" In order to secure your prize, all you have to do is send a fee to claim the prize. The organizers sound legitimate, a hospital foundation, but you've never heard of them. You pay the fee. But you never hear from them again.

This is a **fake lottery scam**.

Often, there is no prize at all. Even if you do receive a prize, it may not be what was promised to you.

In fact, legitimate lotteries do not require you to pay a fee or tax to collect winnings.

As well, 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 haven't entered the lottery.

Text message trivia scams



"I got a text recently: 'Tell us who won the Stanley Cup in 1915 — and you could win BIG!!' I thought, 'I know the answer! It's the Vancouver Millionaires, the only time a Vancouver team has won.' So I texted back. They kept sending hockey questions. I couldn't resist answering. When I got my next bill, I had \$150 in unexpected texting charges."
- Bruce, North Vancouver

A text message from a number you don't recognize encourages you to take part in a trivia contest for a great prize. All you need to do is text back correct answers to a few questions. The first questions are easy. You're encouraged to keep playing. To claim your "prize", you're asked a question that is virtually impossible to answer correctly.

In these **trivia scams**, the scammers make money by charging extremely high rates for the messages you send and any further messages they send to you.

Preventing problems

Here are ways to reduce the risk of being the victim of a prize or contest scam.

Examine any offer carefully

Read the terms and conditions of any offer very carefully. Claims of "free" or very cheap offers often have hidden costs.

Don't pay to participate


Don't pay to enter a contest. Buying things won't increase your chances of winning. Don't call or text phone numbers beginning with 1-900 unless you are aware of the costs involved.



Image via www.istockphoto.com

Protect your personal information

Never give your credit card number to someone who claims they will "deposit winnings" in your account.

 *Scams to Avoid* © People's Law School is, except for the images, licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International Licence.

Romance and Relationship Scams

This information applies to British Columbia, Canada. Last reviewed for legal accuracy by People's Law School in March 2017.

Would someone you have never met really declare their love for you after only a few letters or emails?

Romance scams



"I was in an 'internet-only' romantic relationship with a man for two years. Like me, he had lost his spouse. We messaged each other every day. When his daughter became very ill, he said he needed money to pay her medical bills. I sent him \$20,000 by wire transfer. A month later, he stopped answering my messages. I contacted the police, but they couldn't find him. He had vanished."
- Rita, Vancouver

In a typical **romance scam**, someone assumes a fake identity to lure you into an emotional or romantic relationship with them, so they can trick you out of your money. This is also called **catphishing**.

It might start on a dating website. They share phony details of their lives and intentions. They send alluring (and usually fake) photos of themselves. They might send you flowers or other small gifts. Once they've gained your trust, they tell you they have a sick family member or are in a deep depression. They ask you to send them money to help their situation. And then they disappear.

Someone who lies to try to get you to part with your money commits **fraud**, which is a criminal offence.



Do not send money by wire transfer service to someone you've never met. If someone you have been in contact with says they can't meet in person, walk away.

Relative scams

There are scams that target grandparents and other older relatives. In what's often called a **relative scam** or an **emergency scam**, a grandparent receives a phone call from a scammer claiming to be one of his or her grandchildren. The caller says they are in some kind of trouble and need money. They may say they're in hospital, stuck in another country, or have gotten into trouble with the law. They ask for money to be sent immediately through a wire transfer service.

Their aim is to pressure you to send them money as soon as possible without checking the story. To do this, they often act very emotional on the call, or ask you not to tell anyone in the family about the call.

If you get a call like this, ask the caller questions that only your loved one would be able to answer. Alternatively, hang up and call your relative directly or another family member, to find out if there is a real emergency.

Preventing problems

Here are ways to reduce the risk of being the victim of a relationship scam.

Know who you're dealing with

Do your research before engaging with someone online. Check their name and their background by searching on the internet and social media sites like Facebook and LinkedIn.

Be alert for suspicious behaviour


Be wary of a romantic interest who avoids talking on the phone, is constantly making excuses about why they can't meet in person, or tries to isolate you from family and friends.

Protect your personal information

Don't give out any personal information over the phone unless you initiated the call. Don't give out any personal information in an email or when you are chatting online.

Protect your money

Never wire money unless you're absolutely certain that you're sending it to someone you know and trust. Wiring money is like sending someone cash - once it's sent, it's gone.

 *Scams to Avoid* © People's Law School is, except for the images, licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International Licence.

Work Scams



This page is used in the Scams to Avoid Lesson Module, a law-related ESL lesson for newcomers to Canada.

This information applies to British Columbia, Canada. Last reviewed for legal accuracy by People's Law School in March 2017.

"Make \$50,000 in less than 90 days working from home!" If you see a job offer that looks too good to be true, it probably is.

Work at home, make huge profits

Most of us love the idea of earning extra income or quitting our full-time jobs altogether and working from home. But unfortunately the vast majority of these offers are **work-at-home scams**.

These offers typically promise huge demand, big profits, and big earnings for part-time work. They often demand that you buy a "start-up kit" of supplies you'll need to use for the work (for example, special software or tools). Or they insist you have to enrol in a costly training or certification program.

Once you buy the supplies or complete the training, you never hear from them again.

Under BC law, an employer cannot ask a person looking for work to pay a fee to find a job. An employer can't charge you for giving you a job or for providing you with information about possible work opportunities.



Work-at-home scams generally have one thing in common. They require you to **buy** something before you can begin work. If you respond to a work-at-home offer, you will probably wind up **spending** money instead of earning it.

Preventing problems

Here are ways to reduce the risk of being the victim of a work scam.

Research the company


Learn as much as you can about the company and what it does. Check with the Better Business Bureau to see what they know about the company (see the "Where to Get Help" section for contact details).

Get everything in writing

Get a complete description of the work involved. You should never have to pay for a job description.

Make sure you understand the offer

Before you sign anything, make sure you read it and understand it.

 Scams to Avoid © People's Law School is, except for the images, licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International Licence.

Identity Theft



This page is used in the Scams to Avoid Lesson Module, a law-related ESL lesson for newcomers to Canada.

This information applies to British Columbia, Canada. Last reviewed for legal accuracy by People's Law School in March 2017.

Someone has taken your name, your credit card information, and your Social Insurance Number (SIN), and they are pretending to be you. They're running up steep bills, even committing crimes - and as far as your bank and the authorities are concerned, they **are** you. This is **identity theft**, and it is one of the fastest growing crimes in Canada.

What is identity theft?

Identity theft happens when someone takes your personal information - such as your name, address, date of birth, SIN, your bank account numbers, credit card information, or online passwords - and uses it to access your finances, make purchases in your name, or commit other crimes. For example, they might:

- take money out of your bank account
- make purchases using your credit card information
- apply for a credit card or a loan in your name
- sign up for a cellphone service in your name

It is a criminal offence to possess someone else's identification for criminal purposes, or to use it to commit a crime (such as impersonating someone or misusing a credit card).

How do they get the information?



"I got a call from my credit card company asking if I had just bought something in New York. I've never been to New York. It turns out someone had been using my credit card for weeks, and run up \$10,000 in charges. The police think she got my credit card information by pulling an old bill out of my garbage, and then she contacted the credit card company to change my address. I had wondered why I hadn't received a bill for almost two months."

- Hazel, Williams Lake

Identity thieves can obtain your personal information in many ways. Some might find a wallet or phone you lost, and take information from it.

Some go through garbage or recycling bins for discarded bills or other mail with personal information on it.

Some use technology to steal your information. For example, they pretend to be a reputable company and send fake emails or texts to trick you into providing personal and financial information.

Warning signs

There are many signs that could indicate your personal information is being used by someone else.

- On your bills or bank statements, you don't recognize some purchases or withdrawals.
- Bills or bank statements arrive late or not at all (they may have been redirected).
- You're alerted by your bank or credit card company about suspicious transactions.
- You start getting bills from companies you know nothing about.
- A company or collection agency contacts you about a **debt** that isn't yours.

Consequences of identity theft

Being the victim of identity theft can be a complicated and frustrating experience.

There is the immediate inconvenience of having to cancel cards and accounts and get replacements.

There can be charges for purchases you didn't make and services you didn't order. If these purchases were made with a lost or stolen credit card, you shouldn't be liable for any losses as long as you report the lost or stolen card immediately.

As well, identity theft can result in a bad **credit report**, which could make it difficult for you to find employment, rent a place to live, or borrow money. See the section "If You've Been Scammed" for steps you can take to protect or repair your credit report.

Preventing problems

Here are ways to minimize the risk of someone stealing your identity.

Protect your personal information

Never give personal or financial information to anyone who contacts you by phone or online unless you know who they are or can confirm they are legitimate. Be extra careful about giving out your Social Insurance Number (SIN). It's virtually a key to your identity.

Handle your documents carefully

Carry only the identification you need. Don't carry your SIN card, birth certificate, or passport on a regular basis. Store them in a safe place and only carry them when you know you need them. Tear or shred receipts and copies of papers you no longer need, such as old tax returns, insurance forms, and credit offers you get in the mail.



Be cautious using email


Be extremely wary of emails that seem to come from financial institutions or authorities asking you to provide personal information. If in doubt, look up their contact information, call them, and ask them to verify the request before providing any information.

Be cautious online

On social networking sites, don't post more personal information than necessary. Set your privacy settings as high as possible. Don't accept friend requests from people you don't know.

Read your statements

Read your bank and credit card statements. That way you'll know right away if you're being charged for something you didn't authorize. Report any missing mail or statements right away.

 *Scams to Avoid* © People's Law School is, except for the images, licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International Licence.

If You've Been Scammed

This information applies to British Columbia, Canada. Last reviewed for legal accuracy by People's Law School in March 2017.

If you think you've been the victim of a scam or identity theft, here are steps to take to prevent further problems.

Step 1. Stop communicating with the scammer

Immediately stop all communication with the person or company involved in the scam.

Step 2. Gather any information you have

Gather any records you have relating to the scam - any emails or other communication with the scammer, banking statements, contracts, and marketing materials used for the scam (such as brochures or online ads).

Make a list of any money or information that may be lost or stolen.

Leave room on your list for steps you take going forward. As you contact authorities, financial institutions, and other agencies, keep track of their contact details and any information you learn. This will help clear your name and re-establish your credit.

Step 3. If a credit card or bank account is involved, notify your financial institutions

If you think someone has used your credit card or accessed your bank account, immediately notify your financial institutions. Cancel any credit cards that are affected. Close or put a hold on any affected accounts.

Step 4. If any identification is missing, cancel it

If any government-issued identification was lost or stolen, such as a driver's licence or passport, contact the agency issuing the document. Explain what happened, and find out how to get replacement documents.

Step 5. If any mail is missing, contact Canada Post

If you think your mail is being stolen or redirected, contact Canada Post's customer service department at 1-866-607-6301 or www.canadapost.ca^[1].

Step 6. Protect your devices

If you used your computer or cellphone to communicate with a scam operator, or your device was infected by a scam, take your device to a professional to have it checked. Make sure you have up-to-date software to prevent **spam**, **viruses**, and **spyware**.

Step 7. Report the incident to the police

If you suffered a loss because of a scam, report the incident to your local police department. Ask the police for a report number and record it. Include the police report number in all correspondence you have relating to the incident.

Step 8. Contact the credit reporting agencies

Contact the credit reporting agencies Equifax and TransUnion to let them know of the scam or identity theft. These are the two main agencies in Canada that prepare **credit reports**.

- **Equifax:** 1-800-465-7166 (toll-free) or www.equifax.ca^[2]
- **TransUnion:** 1-800-663-9980 (toll-free) or www.transunion.ca^[3]

Discuss with the credit reporting agencies whether to have a "fraud alert" placed on your file. A fraud alert means that businesses or banks will call you before opening any new accounts or changing your existing accounts.

Ask each credit reporting agency to send you a copy of your credit report. The report may reveal **debts** charged in your name.

Step 9. Report the incident to consumer agencies

Report the incident to the agencies that help protect consumers. See the "Where to Get Help" section for contact details.

- If you are the victim of a scam or identity theft, report it to the Canadian Anti-Fraud Centre ^[4]. This federal agency doesn't conduct investigations but it does collect information about fraud and identity theft, which can help protect others from being scammed.
- Report a scam to the Better Business Bureau's Scam Tracker ^[5], or complain about a business or charity by filing a complaint with the BBB ^[6].
- If you've been tricked into signing a contract or buying a product or service, report the incident to Consumer Protection BC ^[7].

Step 10. Consider legal action

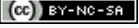
You can consider taking legal action against those involved in the scam or fraud. If you don't have a lawyer, see the options for free or low cost legal help in the "Where to Get Help" section.

Get help

If you have been the victim of a scam or identity theft, there are agencies you can contact for support and advice:

- VictimLink BC is a toll-free 24/7 information and support line for victims of crime.
- The Credit Counselling Society provides support for people struggling with debt, as well as counselling to help people manage money better.

See the "Where to Get Help" section for contact details.

 *Scams to Avoid* © People's Law School is, except for the images, licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International Licence.

References

- [1] <http://www.canadapost.ca>
- [2] <http://www.equifax.ca>
- [3] <http://www.transunion.ca>
- [4] <http://www.antifraudcentre-centreantifraude.ca/index-eng.htm>
- [5] <https://www.bbb.org/scamtracker/mbc/reportscam>
- [6] <https://www.bbb.org/consumer-complaints/file-a-complaint/get-started>
- [7] <https://www.consumerprotectionbc.ca/consumers-other-businesses-home/how-to-make-a-complaint>

Resources

Where to Get Help

This information applies to British Columbia, Canada. Last reviewed for legal accuracy by People's Law School in March 2017.

Access Pro Bono

Volunteer lawyers provide free legal advice to qualifying persons who cannot obtain legal aid or afford a lawyer.

Lower Mainland: 604-878-7400

Toll-free: 1-877-762-6664

www.accessprobono.ca ^[1]

Better Business Bureau of Mainland British Columbia

A non-profit organization that assists people in the Lower Mainland and interior BC in finding businesses and charities they can trust.

Toll-free: 1-888-803-1222

contactus@mbc.bbb.org ^[2]

www.mbc.bbb.org ^[3]

Better Business Bureau of Victoria

A non-profit organization that assists people on Vancouver Island in finding businesses and charities they can trust.

Toll-free: 1-877-826-4222

info@vi.bbb.org ^[4]

www.vi.bbb.org ^[5]

Canadian Anti-Fraud Centre

The central agency in Canada that collects information about fraud and identity theft. They don't conduct investigations but they do help law enforcement agencies by identifying connections among seemingly unrelated cases.

Toll-free: 1-888-495-8501

www.antifraudcentre.ca ^[6]

Competition Bureau

A federal agency that helps consumers make informed purchasing decisions. They help combat deceptive selling practices and scams.

Toll-free: 1-800-348-5358

Toll-free TTY: 1-800-642-3844 (for hard of hearing)

www.competitionbureau.gc.ca ^[7]

Consumer Protection BC

A non-profit organization that helps protect consumers in BC. They provide information and investigate complaints relating to consumer purchases.

Toll-free: 1-888-564-9963

info@consumerprotectionbc.ca ^[8]

www.consumerprotectionbc.ca ^[9]

Credit Counselling Society

A non-profit organization that provides support for people struggling with debt, as well as counselling to help people manage money better.

Toll-free: 1-888-527-8999

info@nomoredebts.org ^[10]

www.nomoredebts.org ^[11]

Lawyer Referral Service

The Canadian Bar Association, BC Branch offers referrals to lawyers who can provide a half-hour consultation for \$25.

Lower Mainland: 604-687-3221

Toll-free: 1-800-663-1919

lawyerreferral@cbabc.org ^[12]

www.cbabc.org ^[13]


VictimLink BC

A toll-free 24/7 information and support line for victims of crime in British Columbia.

Toll-free: 1-800-563-0808

TTY: 604-875-0885 (for hard of hearing)

VictimLinkBC@bc211.ca ^[14]

 *Scams to Avoid* © People's Law School is, except for the images, licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International Licence.

References

- [1] <http://www.accessprobono.ca>
- [2] <mailto://contactus@mbc.bbb.org>
- [3] <http://www.mbc.bbb.org>
- [4] <mailto://info@vi.bbb.org>
- [5] <http://www.vi.bbb.org>
- [6] <http://www.antifraudcentre.ca>
- [7] <http://www.competitionbureau.gc.ca>
- [8] <mailto://info@consumerprotectionbc.ca>
- [9] <http://www.consumerprotectionbc.ca>
- [10] <mailto://info@nomoredebts.org>
- [11] <http://www.nomoredebts.org>
- [12] <mailto://lawyerreferral@cbabc.org>
- [13] <http://www.cbabc.org>
- [14] <mailto://VictimLinkBC@bc211.ca>

Glossary

This information applies to British Columbia, Canada. Last reviewed for legal accuracy by People's Law School in March 2017.

Catphishing

When someone assumes a fake identity to lure another person into an emotional or romantic relationship with them, so they can trick them out of their money.

Consumer

A person who buys goods or services.

Contract

A legally recognized agreement made between two or more people.

Credit

The ability to obtain money or value based on trust that payment will be made in the future.

Credit report

A detailed list of a person's credit and bill-paying history, and other information about them.

Credit score

A number that expresses the information in a person's credit report at one point in time. The score indicates the risk the person represents for lenders, compared with other people, on a scale from 300 to 900. The higher the score, the lower the risk for lenders.

Creditor

A person or company to whom another person owes money or an obligation.

Debt

A sum of money or an obligation owed by one person to another.

Fraud

To intentionally deceive someone in order to gain an unfair or illegal advantage.

Identity theft

When someone takes personal information and uses it to access that person's finances, make purchases in their name, or commit other crimes.

Malware

Software used to disrupt use of a computer or other device or gain access to sensitive information on the device.

Phishing

When someone sends a fake email or text to trick a person into handing over personal and financial information. Their message is being used as bait to "fish" for victims.

Scam

An illegal or dishonest scheme to trick people out of their money.

Spam


Email that is not wanted.

Spyware

Malicious software installed on a device without the owner realizing it.

Virus

A harmful software program.

 *Scams to Avoid* © People's Law School is, except for the images, licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International Licence.

About

About this Publication

Scams to Avoid helps you learn how to spot and guard against scams that try to trick you out of your money. This publication covers 15 of the most common scams that affect British Columbians, explains the growing problem of identity theft, and tells you the steps to take if you have been the victim of a scam.


Acknowledgements

Contributors to this publication:

- Legal review: Drew Jackson
- Writing, editing and layout: Drew Jackson, Elena Renderos and Gayla Reid

This publication was made possible through the financial support of the Law Foundation of BC, the Notary Foundation of BC, the Department of Justice Canada, and the Province of British Columbia.

Copyright

 *Scams to Avoid* © People's Law School is, except for the images, licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 2.5 Canada Licence. This licence lets others share, reuse, remix, and build upon the work non-commercially, as long as they credit the copyright holder and license their new creations under the identical terms.

About People's Law School

People's Law School is a non-profit society in British Columbia, dedicated to making the law accessible to everyone. We provide free education and information to help people effectively deal with the legal problems of daily life.



150 - 900 Howe Street

Vancouver, BC V6Z 2M4

604-331-5400

info@peopleslawschool.ca ^[1]

www.peopleslawschool.ca ^[2]

References

- [1] <mailto:info@peopleslawschool.ca>
- [2] <http://www.peopleslawschool.ca>