

Better Business Bureau of Mainland BC Top Ten Scams:

The tough economic times have made a strong impact on this year's list of the Top Ten Scams. Consumers are feeling the pinch and are looking for investment opportunities, new sources of credit, or thinking of renovating their homes to enhance their market value. During an economic downturn scammers are out in full force looking to catch people at their most vulnerable.

Schemes and scams take on various forms but they all share common traits. The best defense is knowledge; knowing the danger signs and how to protect yourself can save you time and money. The following list is developed jointly by the BBB, Business Practices and Consumer Protection Authority of BC, Competition Bureau of Canada, BC Crime Prevention Association and BC Securities Commission. In no specific order, here are the Top Ten Scams for 2008.

- 1) Economic Downturn & Loan Scams
- 2) Home Repair Rip-Offs
- 3) Too Good to Be True Business Opportunities
- 4) Bogus Online Ads
- 5) Cure-All Health Products
- 6) Guaranteed Vehicle Brokers
- 7) Prize Offers
- 8) Bogus Cheques & Overpayment Schemes
- 9) Greenwashing Scams
- 10) Spoofing Attacks

Better Business Bureau of Mainland BC Top Ten Scams:

1. Economic Downturn & Loan Scams

Tough economic times often bring out the bad guys. During a credit crunch, you may turn to new sources to help with your finances. While it may not be called a "loan" in the marketing, there are small business cash advances which offer thousands of dollars for business ventures despite your credit rating. These types of opportunities often come with up-front fees, and excessive interest charges. In some cases, it may even be attempts to gain information for identity theft. Before you jump up and send in that processing fee or security deposit, be warned that this is likely a scam. You should never have to pay cash in advance for a loan.

QUICK TIP: Never pay money to get money. If it is a legitimate loan or lender, the fee will be added to the total amount owed on the loan as required by BC consumer protection laws. For information about disclosure requirements when you are applying for a personal loan in BC, contact Business Practices and Consumer Protection Authority (BPCPA) of BC toll free at 1.888.564.9963 or visit www.bpcpa.ca

EXAMPLES: Recent examples cited include e-commerce banking solicitations, [Ponzi and pyramid schemes](#), and the release of the new Britney Spears CD.

What is a Ponzi scheme

It is the name given to pyramid selling in the US. A Ponzi scheme uses cash from new customers or investors to pay returns to existing investors. It does little legitimate business, but just recycles money. The scheme depends on a constant stream of new investors to fund the payouts.

How did Madoff's alleged fraud work?

His firm was known for stockbroking with a twist. Madoff was running a huge investment business for wealthy clients and investors on the side of his stockbroking firm. It was on a separate floor from the rest of the business. He was offering attractive returns to new investors and was falsifying his trading statements. He made it look as if he was investing in blue-chip stocks and options, but there was very little capital at the heart of the operation.

How did he attract new investors?

He was paying clients a 10% to 12% annual return. He managed to produce consistent returns over a 10-year period, which is extremely unusual for the fund management business. His broking, hedge funds and fund management businesses all recorded the same "success".

How did it go wrong?

New clients began to dry up once the credit crunch took hold. This year Madoff was forced to pay redemptions when clients needed to withdraw their cash. Some analysts had also pointed out that his investment prowess was virtually impossible to achieve given the ups and downs of the stockmarket.

Why did the regulators miss it?

The Securities Exchange Commission (SEC) argues that Madoff kept few records and was clever at hiding the alleged fraud. While he was a pioneer of electronic trading and rose to become chairman of the Nasdaq technology exchange, he refused to provide his clients online access to their accounts. According to the Washington Post he sent out accounting statements by mail, whereas most hedge funds emailed statements and allowed them to be downloaded via computer for easier analysis by investors.

Can it happen here?

Steven Philipsohn, chairman of the Commercial Fraud Lawyers Association, said London is just as big as New York as an international financial centre and just as likely to harbour Madoff-style characters. "As the credit crunch bites, more and more problems will come to light," he said.

2. Home Repair Rip-Offs

Home improvements may be on your agenda, but finding a contractor with reasonable costs and availability may be a challenge. During the spring thaw, unscrupulous and unqualified people often show up to homes with offers to do everything from landscaping to roofing. Some may offer to pave your driveway with leftover materials, or even remodel your home for a low price. These fly-by-night operators come into communities for a short time and do shoddy work that often results in having the work to be redone.

QUICK TIP: Get the name and address of the company the vendor claims to represent and check it with the Better Business Bureau and the city-licensing office. Get all the details of the work put in writing and make sure that you understand everything in the document. Verify the individual is licensed, bonded, insured and has registered with WorkSafeBC (Workers' Compensation Board). If you are entering into a contract with a contractor who came to your door to sell their services, find out about your cancellation rights. Contact the Business Practices and Consumer Protection Authority (BPCPA) toll free at 1.888.564.9963 or visit www.bpcpa.ca to find out more about consumer contracts. Remember, price is not everything because in the end it may cost you more than you planned.

EXAMPLES:

Each year hundreds of thousands of consumers complain to their state attorneys general about home-repair rip-offs. The National Association of Consumer Agency Administrators, in fact, says home repairs are second only to car repairs on the nation's pet-peeve list. To get the inside story on how tradesmen take advantage of their customers, Smart Money interviewed dozens of general contractors, home inspectors and tradesmen themselves. We culled the results and assembled this section, which tells you what to watch out for when signing up for a repair. e.g. as below,

Roofers:

State attorneys general have files stuffed with stories of roofers who have skipped town with a client's shingles -- and his check. Some roofers don't even bother using shingles, claiming that a coat of latex paint prevents leaks just as effectively.

If you've got a leaky roof, the likely cause is flashing, which is the material -- usually copper, galvanized steel or aluminum -- that joins your roof to the chimney and vents. Flashing can be fixed cheaply with a black gooey substance called asphalt cement (which lasts around three years) or with new flashing (which lasts more than a decade). Plan on paying \$30 to \$50 an hour to have flashing fixed correctly.

Beware the roofer who gazes up at your house and announces, "Your roof is 15 years old. It will leak soon unless you replace the shingles." The only way to determine if you need a new roof is by walking around on it. Worn-out shingles, which have lost their oil and thus their water repellency, look brittle, curl up at the edges and often crumble into powder when broken.

A new asphalt shingle roof (with one layer of shingles) costs \$30 to \$50 per "square" (a roofer's square is 100 square feet), depending on the quality of the shingles and the slope of your roof, and lasts 15 to 20 years. A second layer will last about 10 years. If you plan to move within that time, adding a second coat without stripping the first will save you around 20% in labor (as well as \$500 to \$700 for a dumpster to haul away the old shingles).

3. Business Opportunities

Your good friend or family member may have invited you to attend a presentation involving an investment opportunity. You don't know anything about the company, and are desperate to hear that it is legit. These investments appear lucrative, but often are more hype than substance. The promoter convinces investors that they can be part owners of investment portfolios if they enlist new recruits, maybe promising commissions in cash and bullion.

QUICK TIP: In reality, this is most likely a pyramid scheme. The new capital brought on by new investors is keeping this imaginary investment afloat. Get the facts. If you do go to an information session, collect business cards, promotional materials, and ask questions such as, who are the principals of the company? When did the company get started? How much is the start-up cost? Gather as much information as possible before agreeing to anything. To report misleading advertising and deceptive marketing practices contact the Competition Bureau at: www.competitionbureau.gc.ca or 1.800.642.3844. Go to the BC Securities Commission's Investright.org website for information on how to select an advisor and what to look out for when choosing to invest.

EXAMPLES:

Lured by deceptive promises of independence and easy income, many would-be entrepreneurs are jumping into the arms of con artists who claim: "we are not just selling you a business, we put you IN business." The following Project Telesweep cases illustrate the nature and extent of the business opportunity fraud epidemic in America: **Major financial losses.** A Pennsylvania woman responded to an advertisement for a pizza vending machine business opportunity. The promoter promised huge earnings and the best locations in the area. The woman ended up losing her entire investment of \$72,000.

In order to make up the loss, she and her husband had to mortgage their home and sell off a dairy cow herd. They are now working multiple jobs in a struggle to avoid losing their family farm.

Promises of instant riches. One trademark of a business opportunity scam is an overblown promise of easy money. In one ad for a pay telephone scheme, a promoter promises: "Get 96 sites for \$7,795. Then Retire! Call 1-800/XXX-XXXX." A brochure for a Utah snack vending machine company reads: "Many People Earn \$36,000/year in Income, But . . . Very Few Earn \$30,000/year working only five-six hours per week." In another case, a promoter for a gumball machine business opportunity claimed that one operator had earned \$14,000 from four machines . . . in just seven days!

4. Bogus Online Ads

Online classifieds can be an effective way to hunt for shopping bargains and find those hard-to-get concert tickets. While those classified websites offer free access to hundreds of ads, beware that those listings are rarely vetted prior to posting. The seller may not be legitimate, and there may not be concert tickets coming to you in the end.

QUICK TIP: DO NOT wire money to complete an order you have purchased from a stranger. This money will be impossible to recover if the product you purchased does not arrive. If you are meeting the person, try to meet in a neutral location. Avoid purchasing things like gift certificates and gift cards from online classifieds. If the person offers the gift card for less than the value, the card may be either stolen or fake.

EXAMPLES:

The dark side of online advertising

Martin Fleischmann put his faith in online advertising. He used it to build his Atlanta company, MostChoice.com, which offers consumers rate quotes and other information on insurance and mortgages. Last year he paid Yahoo! Inc. (YHOO) and Google Inc. (GOOG) a total of \$2 million in advertising fees. The 40-year-old entrepreneur believed the celebrated promise of Internet marketing: You pay only when prospective customers click on your ads.

Now, Fleischmann's faith has been shaken. Over the past three years, he has noticed a growing number of puzzling clicks coming from such places as Botswana, Mongolia, and Syria. This seemed strange, since MostChoice steers customers to insurance and mortgage brokers only in the U.S. Fleischmann, who has an economics degree from Yale University and an MBA from Wharton, has used specially designed software to discover that the MostChoice ads being clicked from distant shores had appeared not on pages of Google or Yahoo but on curious Web sites with names like insurance1472.com and insurance060.com. He smelled a swindle, and he calculates it has cost his business more than \$100,000 since 2003.

5. Cure-All Health Products

Fraudulent “cure-all” health products promise quick cures and easy solutions to a variety of problems, from obesity to diabetes and cancer. Any product that claims to be a miracle cure may be a fraud that could cheat you of time, money and most importantly, your health.

QUICK TIP: Beware of ads that promise too much. Think twice before buying a product that claims it can do it all. Steer clear of a product that claims to be a “scientific breakthrough.” If the first or only place you learn about a new treatment is through an advertisement on the Internet, be suspicious. Consult your health care practitioner before trying any new treatment. For further information on health fraud, go to the Competition Bureau’s website: www.competitionbureau.gc.ca/healthfraud

EXAMPLES:

"Operation Cure.All" Wages New Battle in Ongoing War Against Internet Health Fraud

FTC, FDA and other law enforcement agencies move to stop Internet scams for supplements and other products that purport to cure cancer, HIV/AIDS and countless other life-threatening diseases. FTC also warns of risks associated with some supplements, including drug interactions.

As part of an ongoing and comprehensive law enforcement and consumer education campaign begun in 1997, the Federal Trade Commission today announced a new round of enforcement actions against the fraudulent marketing of supplements and other health products on the Internet. The FTC's action is part of a coordinated effort with the U.S. Food and Drug Administration (FDA), Health Canada, and various state Attorneys General to crack down on unscrupulous marketers who use the Internet to prey on the sickest and most vulnerable consumers. The six new FTC enforcement actions target companies marketing a variety of devices, herbal products, and other dietary supplements to treat or cure cancer, HIV/AIDS, arthritis, hepatitis, Alzheimer's, diabetes and many other diseases. Among the many products for which unfounded claims were being made were a DHEA hormonal supplement, St. John's Wort, various multi-herbal supplements, colloidal silver and a variety of electrical therapy devices. The FTC's cases were also prompted by representations by some marketers that their products are safe when, in fact, there may be potentially dangerous interactions with other medications.

Among the many false and unsubstantiated claims challenged in today's cases were promises that:

- People could cancel their surgery, radiation or chemotherapy in favor of herbal cures that cost hundreds of dollars;
- A device that delivered mild electric current would kill the parasites that cause such serious diseases as cancer and Alzheimer's; and
- Those with HIV or AIDS could use St. John's Wort as a safe treatment for the disease. In fact, the FTC alleged, there is inadequate evidence to support the use of the herb to treat AIDS. Indeed, St. John's Wort is known to interfere with proven HIV/AIDS medications.
- "Many of the Web sites targeted today are jeopardizing the health and safety of consumers with outlandish promises and false hope," said FTC Chairman Timothy J. Muris. "Unfortunately, examples of questionable products being peddled on the Web abound, and the Federal Trade Commission, with its partners, will step up its efforts to protect consumers from these compelling, but deceptive health claims."

6. Guaranteed Vehicle Brokers

After listing your used vehicle for sale in the classifieds, you receive a phone call from a company advising you that they have a purchaser for your vehicle. The caller asks for a fee guaranteeing that the purchaser will pay more than the vehicle is advertised for. They promise that if you list your vehicle on their classified site and the vehicle is not sold within 90 days, you will get your money back. Unfortunately, your vehicle is not sold, the guarantee is not honored, you can't reach the company and you are out of pocket the funds you have given this company.

QUICK TIP: The BBB advises consumers to be wary of brokers who “guarantee” auto sales with prearranged buyers. Ask detailed questions such as: is the buyer specifically interested in your vehicle, rather than a range of similar vehicles? Always understand telemarketing offers and ask for additional documentation. Certain telemarketers must be licensed in BC. You can check to see if the telemarketing company is licensed through Business Practices and Consumer Protection Authority of BC at www.bcpca.ca or 1.888.564.9963.

EXAMPLES:

Tip: Invoice Price applies to new cars only, not to used cars.

For used car pricing, you should use Kelly Blue Book Values or eBay completed auction prices as your guide

The Best Way You Can Save Cash On A New Car Is With Competing Quotes

We'll review car buying sites like [InvoiceDealers](#), [Cars.com](#), [Yahoo!Autos](#), [Autos.com](#), [Edmunds.com](#), [MyRide.com](#) and [CarsDirect](#) to lookup how much dealers pay for cars, and get free car purchase quotes. Get quotes now from all of them and compare. You can use these sites if you're leasing too, they also list new car prices, used car prices, and dealer invoice prices for new cars. Now you'll know what dealers pay for new cars. Don't drive all over town wasting time at dealers. Do your car pricing online and get quotes emailed to you from dealers. You should **never** enter a dealership without "[The Folder](#)" with your price quotes to compare. You must check all sites, you never know who has the best price on your car. You would feel foolish if you bought a car and found out it was \$1500 less at [InvoiceDealers](#). A few minutes of research now saves you thousands off your new car, leaving you more money for your family vacation. In [Chapter 4](#) we'll cover exactly how you calculate the dealer's cost of the car and how to calculate a fair offer for your new car using our [Buyers Offer Spreadsheet](#).

7. Prize Offers: You Don't Have to Pay To Play

You may have attended a trade show and entered a draw for a free trip, and several days later you get a call you have won. Or, you received a letter that states that you have won an international lottery or fabulous prize. The common trait to both these 'winnings' is that thing is that you must send them money, be available for a home delivery or a special presentation, or provide them with some very personal information such as your bank account or credit card number.

QUICK TIP: If there's a catch or condition, you haven't won. If it sounds too good to be true, or you're not sure, check the offer out further. Contact your BBB at 604.682.2711 or 1.888.803.1222. If you think it's fraud, call the Canadian Anti-Fraud Call Centre, Phone Busters, at 1.888.495.8501. To be removed from telemarketing calling lists contact the Canadian Do Not Call List: 1.866.580.DNCL or go to: www.lnnte-dncl.gc.ca.

EXAMPLES:

PRIZE SCAMS

THE SETUP: You receive a postcard stating you've won a new car, an entertainment center, a dream vacation, or some other fabulous prize. In order to collect the prize, you need to pre-pay some taxes, pay a transfer fee, or purchase a few products to the tune of several hundred dollars.

THE ZINGER: Your prize, if it arrives at all, will be practically worthless. For instance, the entertainment center may in reality be a cheap plastic cassette recorder.

AVOID THIS SCAM: No legitimate contest will charge you money to collect a prize.

8. Bogus Cheques & Overpayment Schemes

In this scam, fraudsters typically target people selling a product through classified ads, online bulletin boards or people looking for work on employment postings. The scammer sends a cheque for the listed product or service that is more than the negotiated price. The original cheque is usually stolen or is a fake, and by the time the victim has cashed and returned the excess funds, the scammer has disappeared with the money and the product.

Another cheque overpayment scheme can be under the guise of working as a mystery shopper. The victim believes that they will be paid to mystery shop a wire transfer service. They are sent a cheque, told to deposit it, keep a small percentage of the money as their wage, wire the rest, and then complete the survey on the service they encounter. The address turns out to be bogus, the money wire transferred to another unknown location and the victim is out the money transferred.

QUICK TIP: Never accept payment for more than your selling price. Never agree to refund the excess to a buyer or wire-transfer money to another location. A legitimate buyer or employer would never ask you to do so. Consider using an independent online payment service. Speak to your credit card service provider to determine what avenues it has to guarantee payment processing.

EXAMPLES:

Scammers prey on all consumers, regardless of age, education or income, targeting them through telephone, mail solicitation and email. Although the offers are often personally addressed to potential victims, they are posted using bulk mail, with thousands of consumers receiving the exact same offer. In 2006, the Competition Bureau received over 8,400 complaints from consumers who had received one of these phoney cheques or prize notices.

Here are some examples of fraudulent cheque scams:

- A scammer purchases a \$2,000 laptop on eBay and sends the vendor a bogus cheque for \$3,000. The scammer will then contact the vendor and ask that they send a cheque to cover the overpayment of \$1,000.
- As part of a phoney employment opportunity, victims will answer classified ads in the newspaper where they are asked to evaluate a particular wire transfer service, which allows people to send and receive money worldwide. They will receive a bogus cheque for \$4,000 and will then wire \$3,000 from their own bank account to validate the service. The other \$1,000 is supposed to be payment for their work.
- If you receive a letter from a lottery corporation, which states that you are required to cash an enclosed cheque to pay the tax and clearance fees in order to receive your prize, chances are it's a scam. Legitimate lottery and sweepstakes administrators never charge fees to deliver your prize. Furthermore, how can you win if you've never entered a contest?

New scams are being invented daily. Scam artists are up-to-date and well-organized. They use the latest trends and sophisticated techniques; they have limitless imagination.

If deals like these sound too good to be true, they probably are. Hang up the phone, do not respond to questionable contests by mail, shred unwanted personal documents and call PhoneBusters, the Canadian Anti-Fraud Call Centre, at 1-888-495-8501. PhoneBusters gathers evidence, identifies new trends and alerts law enforcement in Canada and abroad. By reporting, you can prevent others from becoming victims and help put an end to fraud.

It is illegal under the *Competition Act* to send out mail solicitations that contain false or misleading representations. If you feel that you have been misled by a mail solicitation or would like more information on the application of the *Competition Act*, contact the Competition Bureau at 1-800-348-5358, or visit the Web site at www.competitionbureau.gc.ca

The Competition Bureau chairs the Fraud Prevention Forum, which is a concerned group of private sector firms, consumer and volunteer groups, government agencies and law enforcement organizations committed to fighting fraud aimed at consumers and businesses. Through its partners, the Forum works to prevent Canadians from becoming victims of fraud by educating them on how to recognize it, report it and stop it. For more information on the Forum or Fraud Prevention Month, visit: www.competitionbureau.gc.ca/fraud

9. Eco Cons – Are you buying it?

There are a number of products on supermarket shelves that are “green”, “eco-friendly”, “all natural” or “environmentally safe.” A study by TerraChoice Environmental Marketing, found evidence of Green washing -- making false or misleading green marketing claims – in 99% of products checked.

Quick TIP: Look for EcoLogo or Green Seal symbols that show third party testing of products. Be skeptical of marketing promotions that offer to support environmental processes without proof the processes are subscribed to and are effective. Canada has guidelines for green advertising that can be visited at the Competition Bureau website: www.competitionbureau.gc.ca

EXAMPLES:

Improved Scamfinder site helps you avoid latest cons and scams

Sunday, December 07, 2008

Sheryl Harris/Plain Dealer Consumer Affairs Reporter

For folks like Alice Stringer, an encounter with a scam began with a good intention. She answered an online ad for puppies for sale. The sellers, who were overseas, said they wanted to find a home for the pups because their young daughter had just died and the dogs reminded them of her.

She was suspicious of the story and the incredibly low price tag on the dogs. "What do you think? Is it a scam?" she wanted to know.

Another reader discovered a fake check scam too late to help her job-hunting son. He thought he'd found a legitimate job when a company sent him instructions for mystery shopping, along with a check to cover his salary and expenses. Following instructions, he wired money overseas and wrote his report about the money-wiring service's customer service.

Not only was his employer bogus, the check he received was counterfeit. The bank held him responsible for paying back thousands of dollars he spent against the funds - and it shut down the mother and son's joint bank account. Scamfinder explains scams against individuals and businesses. Here are some of the common ones.

Job scams

- You receive a check and are then asked to wire money abroad.
 - You're asked to process checks through a bank account you set up for your employer or through your own bank account.
 - You're asked to collect checks and then send them to other locations in the United States -- even without processing them.
- Puppy scams
- The seller is from overseas. He may claim to be a missionary or an American working abroad.

10. Spoofing Attacks

You may receive an email that looks like it is from an organization you know, or visit a webpage that looks like it is from your bank. When a one person or program successfully masquerades as another by falsifying data, this is spoofing. Spoofing attacks have grown and become more sophisticated and have illegally used organizations like the Better Business Bureau and the Canada Revenue Agency to trick consumers into sharing their information. The key common tactic is to get you to either fill in personal information or download malicious software on to your computer to compromise your security and put your identity and money at risk.

QUICK TIP: If you receive an email from a person or organization that instructs you to complete an online form, or download a program, stop. Organizations do not usually correspond only by email, especially without prior contact. Call to check the legitimacy of the email. Do not click the link or respond to the email to play along, because you may expose your computer and your identity at risk. Delete the email. If you fear your computer has been compromised, contact a computer technician to examine your system. Make sure to check your credit report annually with Equifax (1.800.465.7166 or www.equifax.ca) and Trans Union Canada (1.866.525.0262 or www.tuc.ca.) For more information about identity theft, go to the BC Crime Prevention Association website: www.bccpa.org.

EXAMPLES:

'Spoofing' or Spoof Sites

As part of a 'phishing' scam, Internet fraudsters create authentic-looking web sites to look like other sites. Financial institutions are the most targeted groups to be 'spoofed' (or have their sites copied). Through e-mail, the 'spoofed' or forged sites attempt to persuade readers to input personal and banking details by creating a sense of urgency around the request. Unfortunately, some readers react and respond quickly with the requested information trusting the request to be legitimate. They may not realize until it's too late that they had just been 'phished.' Many spoofed sites look very legitimate and are sometimes difficult to detect as fraud. The scammers use company logos, impressive graphics, text and credible-looking links. But don't be fooled by the e-mail or the links, and don't provide any information without checking directly with the bank or company first. Visit the [Alerts!](#) section to learn about examples of current fraud reported against HSBC. Also, visit the [Anti-Phishing Working Group](#) site to read examples of spoofed e-mails and phishing scams.

[back to top](#)

How to Spot Online Fraud

HSBC's Security Site includes an [Alerts!](#) section designed to raise your awareness and keep you informed of phishing attacks against HSBC and other companies.

It will also provide links to the [Anti-Phishing Working Group](#) site so you can review other phishing and spoofing attacks reported. Review the site regularly so you'll know who is being targeted and the steps to take if you receive fraudulent e-mail or fall victim to an online scam. The following are examples of typical phishing attacks using spoofed sites to lure readers into the scam: