



FOR IMMEDIATE RELEASE
January 4, 2011

Better Business Bureau announces Top Ten Scams for 2012

VANCOUVER— This year's Top Ten Scams list focuses on how scammers can use misrepresentation to gain consumers' trust.

"We are seeing trends towards spoofing well-known brands and 'scams of the moment' which capture people's attention because the topic is in the public consciousness," says Lynda Pasacreta, BBB President and CEO. "Scammers are capitalizing by using false pretences to get our attention and steal our trust."

The following Top Ten Scams list, themed "Pay Attention to the Message," is developed jointly by BBB, Consumer Protection BC, and BC Crime Prevention Association. In no specific order, here are the Top Ten Scams to be on the lookout for in 2012.

1. Brand Spoofing

Brand spoofing (aka phishing) is a general term for e-mail, text messages and websites fabricated and sent by criminals and designed to look like they come from well-known and trusted businesses, financial institutions and government agencies in an attempt to collect personal, financial and sensitive information. If the recipient follows the link provided and connects with the fraudulent website, any information entered into the data fields (account #, PIN, contact information, social insurance number etc.) could be recorded, collected and used for fraudulent purposes. Additionally, some variants of phishing scams make use of Trojan horses to infect recipient computers with malware.

QUICK TIP: If you receive these messages just delete them and do not click on any links, and hang up on callers you aren't familiar with. Never give credit information online or over the phone unless you are sure of the identity of the caller. If you are a victim of ID theft, call your financial institutions to have them cancel your cards and re-issue new ones. Contact your local police and Canada's main credit reporting agencies: TransUnion Canada at tuc.ca (1-800-663-9980) and Equifax Canada at equifax.ca (1-800-465-7166).

2. Advance Fee Loans

Consumers have reported losing substantial sums of money responding to advertisements that "guarantee" loans to people, often online. Consumers complete credit applications and are told the loan (from \$5,000 to \$100,000) has been approved and the promised funds will be received once a fee is paid. After payment, the loan is never received as promised.

QUICK TIP: It is illegal for a company to charge a fee in advance to obtain a loan, even if that fee is disguised as the first or last month's payment. Watch for claims of "guaranteed" loans even if you have bad credit, no credit, or a bankruptcy, and demands that you wire or send money before you can have a loan offer confirmed in writing. Report any suspected fraudulent schemes to your local police and the Canadian Anti-Fraud Centre (CAFC) at 1 (888) 495-8501 or antifraudcentre-centreantifraude.ca

3. Gold Buying Schemes

When the BBB was created in 1912, the average price of gold was \$18.93 per ounce (and it had been so for about 100 years before). In 2011, the price of gold soared, rapidly fluctuating and averaging over \$1735 per ounce. Similar to gold rushes of the past, a strained economy



and high demand for gold resulted in many consumers selling, trading and receiving unfair returns when cashing in their gold and jewellery.

QUICK TIP: Before cashing in on the gold rush it is important to do your research. When choosing an appraiser, find someone locally whom you know and trust. Know that the true price of gold may not be what you will be paid for every ounce of gold you own. Get multiple appraisals and compare prices before selling. Be sure that jewellery of differing karats is weighed and priced separately. Have jewels such as diamonds priced separately from the gold they are contained in.

4. Financial Elder Abuse

Financial elder abuse occurs when seniors' pocketbooks are exploited by scammers who take advantage of a person's vulnerabilities associated with age - like hearing loss, loneliness, physical limitations and impaired mental capacity. Common financial elder abuse frauds include tricking seniors into giving out private banking information; encouraging unnecessary home repair work, telemarketing and mail fraud; and swindles by family or friends that result in seniors giving up money, property, personal information and decision making capacity.

QUICK TIP: Most elder abuse happens to a senior by someone they know, such as a family member, friend or caregiver. Many victims do not even realize they have been taken advantage of. Signs a senior is being financially abused include: missing belongings, unusual activity in bank accounts, suspicious stories, sudden changes in Power of Attorney or Wills, bounced cheques and numerous unpaid bills. Report all incidents of financial elder abuse to your local police.

5. Power Saving Claims

The switch to Smart Meters in B.C. fostered a rise in false claims and deceptive ads by some scammers selling energy conservation devices. Consumers reported purchasing a number of power saving devices they claim did not work and that did not meet electrical safety standards.

QUICK TIP: BBB was created 100 years ago to put a stop to unethical, deceptive claims and advertising. The BBB Ad Review program seeks to help consumers and businesses identify untrue, deceptive, fraudulent and insincere statements. Protect yourself from deceptive advertising by doing your research before making a purchase. Always check out a company's BBB Business Review (bbb.org) first and report deceptive advertising and business claims to your local BBB. If it sounds too good to be true, remember that it probably is.

6. Door-to-Door Sales

Each year a variety of unscrupulous door-to-door salespeople use high pressure sales tactics to frighten people into purchasing expensive, substandard - often unneeded products and services. Be wary of overly aggressive sales people selling everything from alarm systems to vacuums and air purifiers, as well as roofing, paving, window washing, painting, plumbing, heating, repair and landscaping services.

QUICK TIP: Don't give in to high pressure sales tactics. If you feel threatened by an aggressive salesperson, ask them to leave your property. If they refuse, call the police. Before making any purchase, take the time to do your due diligence, getting the name and location of the company and ensuring all details and verbal promises are included in a contract. Door-to-door contracts are regulated by Consumer Protection BC. Complaints or questions? 1 (888) 564-9963 or www.consumerprotectionbc.ca

7. Virus Fixing Scheme



In the case of the alleged caller from Microsoft, he/she claim to be phoning about a serious problem with the person's computer. The caller warns that if the problem is not solved, the computer will become unusable. In order to "fix" it, the computer owner is directed to a website and told to download a program, plus pay a fee for a subscription to this preventative service. The catch: there was never anything wrong with the computer, the caller is not working for Microsoft, and the owner has downloaded to their computer damaging malware and spyware.

QUICK TIP: Treat all unsolicited phone calls with skepticism. Check with the organization directly that the caller is claiming to be from, using the contact numbers found on their website. Do not provide any personal information to avoid identity theft. Never provide credit or debit card information for payment. Report any fraudulent activity to the Canadian Anti-Fraud Centre at 1 (888) 495-8501 or www.antifraudcentre.ca.

8. Fraudulent Locksmiths

Consumers reported "local locksmiths" advertising online using a local telephone number and local address, but when contacted, consumers are connected to a call centre in another city and there is no locksmith at the address listed in your area. Consumers who have hired these companies allege that they have been overcharged for products and services, received bad advice or poor workmanship, or have had difficulty contacting the business to correct problems.

QUICK TIP: Don't just pick the first "local" company you find online. Confirm the company address and ask for the legal name of the business. When the locksmith arrives, ask for identification, a business card and their license. In BC, locksmiths are licensed through the Ministry of Public Safety & Solicitor General. Also make sure that they are insured, so you know costs will be covered should any damage be done to your personal property. Expect a legitimate locksmith to ask you for identification to confirm your identity as the homeowner. Check out their BBB Business Review (bbb.org).

9. Penny Auctions

Online ads, often designed to look like news reports, are cropping up on popular websites claiming that you can get great deals on iPads and other electronics with online penny auctions. Most commonly with a penny auction, users must set up an account and purchase bids with a credit or debit card; each individual bid may cost less than a dollar and are often sold in bundles of 100 or more. Every item has a countdown clock and as people bid, the cost of the item goes up incrementally and more time is added to the clock. Even if you don't win the item, you still have to pay for the bids you placed which can add up over time.

QUICK TIP: Before providing any personal information or signing up for any "free" trial with a penny auction, read all of the fine print carefully on the website. Pay close attention to details on signup and annual fees, minimum bidding requirements, maximum prize amounts and how to get a refund. Know what you're buying. Before bidding on an item, research how much it costs elsewhere and keep track of how much you're spending on bids overall to see if you really are getting a good deal. Keep a close eye on your credit card for unexpected charges.

10. Anti-Social Network

Social networks like Facebook and Twitter are becoming more and more popular. Users are often subject to targeted advertising and direct messages, and scams of all colours use social networks to operate. Fraudulent work-at-home job offers are sent through Twitter "tweets" and Facebook messages, deceptive "free" trials are advertised, and "clickjacking" on Facebook convinces users to unknowingly post malicious links on their status updates.



QUICK TIP: Your computer should always have the most recent updates installed for spam filters, anti-virus and anti-spyware software, and a secure firewall. Use the most up-to-date versions of your web browser to offer further protection. Be wary of messages from friends and especially strangers that direct you to another website via a hyperlink. To learn more about how to protect yourself from false or misleading advertising, contact the Competition Bureau at competitionbureau.gc.ca or 1 (800) 642-3844.

-30-

For more information, please contact:

Lynda Pasacreta, President and CEO
Better Business Bureau serving Mainland BC
For interviews with Lynda Pasacreta contact:
Mark Fernandes, Strategic Communications and Public Relations Officer
Tel: 604-488-8701
Email: Mark@mbc.bbb.org

Tatiana Chabeaux-Smith, Manager of Public Relations
Consumer Protection BC
Tel: 604-296-2856
Email: tatiana.chabeaux-smith@consumerprotectionbc.ca

Carolyn Sinclair, Executive Director
BC Crime Prevention Association
Office phone: 604-501-9222 Cell: 604-961-6418
c.sinclair@bccpa.org