



# Crime Prevention Week

November 1-7, 2011

**Prepare – Prevent – Protect**

## Top 10 Scams

Day 6: November 6, 2011

The following Top Ten Scams list, themed "How to Spot Them and How to Stop Them", is developed jointly by BBB, Consumer Protection BC, and Competition Bureau of Canada. In no specific order, here are the Top Ten Scams to be on the lookout for in 2011

### 1. Door-to-Door Scams

Every new season seems to attract a new door-to-door scammer offering unbelievable deals: roofing contractors in the spring, paving contractors in the summer, and heating contractors in the fall. These fraudulent contractors use high pressure sales tactics to frighten people into expensive yet substandard—and often unnecessary—work, with no way to contact them when the product fails.

### 2. Not-so-Free Trial Offers

Online ads may tempt you to try out a diet product, acne cream, or teeth whitener, but be careful about signing up for so-called 'free' trial offers. Many websites that offer a free trial for products do not disclose the billing terms and conditions on their website. Before giving the company any credit or debit card information, review the website fully and be aware that free trials may result in repeated billing.

### 3. 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 Tweets and Facebook messages, deceptive "free" trials are advertised, and "clickjacking" on Facebook convinces users to post malicious links on their status updates..

### 4. 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.

### 5. Phishing, Vishing, and Smishing

Identity thieves are always looking for new ways to strike, and taking advantage of new technologies is a boon for scamming unsuspecting users. "Phishing" scams send emails that look legitimate, requesting that your "account information needs to be updated." Recipients are sent to a phony, but legitimate looking website and prompted to enter their information details. "Vishing" attacks come via telephone, usually through a recorded message that tells users to call a toll-free number. The caller is then typically asked to punch in a credit card number or other personal information. "Smishing" scams target mobile device users, sending text messages that might ask a recipient to register for a service that downloads a virus or warn that the consumer will be charged unless he cancels his supposed order by going to a website that then extracts such credit card numbers and other private data. These are all tactics to get you to reveal personal or financial information.

### 6. Relative Scam

This phone scam targets grandparents who think they are aiding their grandchildren by sending money for an emergency situation, but are in fact giving thousands of dollars to con artists. The victim receives a distressed phone call from someone he believes is his grandchild, who typically explains that he has been arrested or involved in an auto accident and need the grandparent to wire money to post bail or pay for damages—usually amounting to a few thousand dollars.



# Crime Prevention Week

November 1-7, 2011

**Prepare – Prevent – Protect**

## Top 10 Scams

Day 6: November 6, 2011

### 7. Job Scams

In tough economic times, scammers target the unemployed and others through work-at-home, online, and mystery shopper job scams. Online job-hunters are told they will be paid to work from home once payment is sent for a start-up kit that never arrives. Mystery shoppers are hired to secret shop a wire-transfer service; they're 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 you encounter. The so-called business address often turns out to be fake, with the money wire-transferred to another unknown location. In the end, the cheque received is a counterfeit or bogus, which the victim finds out only days later when it's returned by their bank and they are out the money transferred.

### 8. Business Opportunities

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

### 9. Business Directory Scams

Small business owners are often targets of scammers. Unauthorized invoices, unordered packages, and phony business directories are all common tactics used to bilk businesses out of money. Many businesses have received lookalike, or phony, invoices for advertising space in the familiar, locally distributed yellow page directories. These invoices are actually solicitations for listings in alternative business directories that differ from the well-known yellow pages. In fact, the different directory may not be that widely distributed, can be of little or no value to advertisers, or may never be published at all.

### 10. Overpayment Scams

Online buyers and sellers, particularly those that use websites like Craigslist and Kijiji, are potential targets for overpayment scams. A person selling merchandise is contacted by someone claiming to be interested in buying the product. The purchaser arranges to make the payment by cheque and even offers more than the value of the product, asking for the extra money to be sent back to them by cheque or wired to an account. The cheque turns out to be fraudulent, leaving the shipper out of both funds and product.