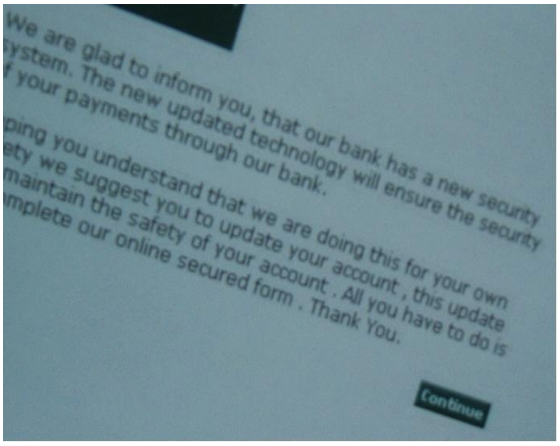
RCMP
ROYAL CANADIAN MOUNTED POLICE

Fraud

Recognize it.
Report it.
Stop it.

Personal Information and Scams Protection

A Canadian Practical Guide



Royal Canadian Mounted Police | Gendarmerie royale du Canada

Canada

Version1.4

Presented to:
Director, Commercial Crime Branch
Royal Canadian Mounted Police

By:
Mélanie Waite, Biomedical Science and Criminology Student
in collaboration with RCMP, Commercial Crime Branch

March 1st, 2007
Ottawa, Ontario

Foreword

An ounce of prevention is worth a pound of cure. This is particularly true in the case of crime prevention through education and awareness. This guide, the Canadian Practical Guide, is a prevention tool. It builds on its successful predecessor, the Student Practical Guide.

Whether online, in person, or by any other means, the criminal activities described in this guide will almost certainly have affected you or someone you know. All Canadians should be aware of the need to protect their personal information and ensure their identity and finances are not compromised. The wealth of information in the following guide will assist Canadians to protect themselves and their personal information.

Superintendent Stephen R. Foster
Director Commercial Crime Branch
Royal Canadian Mounted Police
Ottawa, Ontario

Table of Contents

"I'd read lots of stories, but I never thought it could happen to me. ... Wow, this really can happen. Anybody could pretend to be you." Ottawa Citizen Oct 2005, ID Fraud Victim.

In our information based society, we can live and perform our daily activities in relative ease because of the trust we have in systems, organizations and people that safeguard our information. Each consumer is responsible for their own off and online safety as well as their own education and awareness. Most of us have the necessary information to protect ourselves and our physical property against conventional crimes. Increasingly sophisticated threats however, require that individuals regularly make efforts in self-education. In today's technological environment, it is in your best interests to do so. This document was designed to provide a holistic approach to learning about identity fraud and scams in general. This document will evolve into newer versions as time goes on. It contains basic information and pertinent tools that Canadians may use to further their knowledge on most scams.

"If knowledge can create problems, it is not through ignorance that we can solve them."
Isaac Asimov (1920 - 1992)

Personal information has become a very valuable commodity to criminals. Much like commodities are sold on stock markets everyday, large quantities of personal information change hands on the dark side of cyberspace. Your personal information may have been compromised, sold, used or stored in a database for future use without your knowledge. Nobody is safe from this type of crime.

The RCMP defines identity fraud as the unauthorized acquisition, possession or trafficking of personal information, or, the unauthorized use of information to create a fictitious identity or to assume/takeover an existing identity in order to obtain financial gain, goods or services, or to conceal criminal activities. Your Social Insurance Number, birth certificate, passport and driver's licence are the prime information targeted by criminals. **Never carry the first three documents in your wallet, purse or car** unless you require them for a specific purpose the same day.

According to a survey conducted by Ipsos-Reid in 2006, 73% of Canadian are worried about becoming victims of identity fraud. Only 33% of Canadians feel that they are well educated on personal information and scam protection.

As new threats emerge, the RCMP will be releasing updated versions of this document. Make sure you check for updates. The RCMP knows the identity of the best subject matter expert on fraud education and awareness. It's you. Use this guide to raise your awareness level to be ready when fraud casts its net on you. Use this knowledge to educate your family, friends and acquaintances. Get informed and stay informed.

PhoneBusters, the Canadian Anti-Fraud Call Centre, is jointly operated by the Royal Canadian Mounted Police, Ontario Provincial Police and the Competition Bureau. PhoneBusters plays a key role in educating the public about specific fraudulent telemarketing pitches. The call centre also plays a vital role in the collection and dissemination of victim evidence, statistics, documentation and tape recordings which are made available to outside law enforcement agencies. You may contact PhoneBusters at 1-888-495-8501 or www.phonebusters.com.

Reporting Economic Crime Online (RECOL) is an initiative that involves an integrated partnership between International, Federal and Provincial Law Enforcement agencies, as well as with regulators that have a legitimate investigative interest in receiving a copy of complaints of economic crime. RECOL will recommend the appropriate law enforcement or regulatory agency and/or private commercial organization for potential investigation. You may file a complaint through RECOL at www.recol.ca.

1. Scams

This section will lay out a variety of scams which will be categorized in their most common way of occurrence. This section of the Canadian Guide is therefore organized in five separate environments. Although some scams cannot be prevented, in most situations the risk of victimization can be minimized. Our goal is to teach you to detect risks by raising red flags and to propose the safest course of action.

There are certain online shopping behaviours that should be mastered by consumers in order to minimize the risk of becoming an online fraud victim. Always verify an online merchant's privacy, refund and return policies as well as the legal terms before giving personal and financial information. Keep a copy of the confirmation page and of the correspondence with the online merchant or seller. The safest way to pay online is with a credit card when the customer is protected by a zero liability policy. Verify with your credit card company about this feature.

1.1 Online

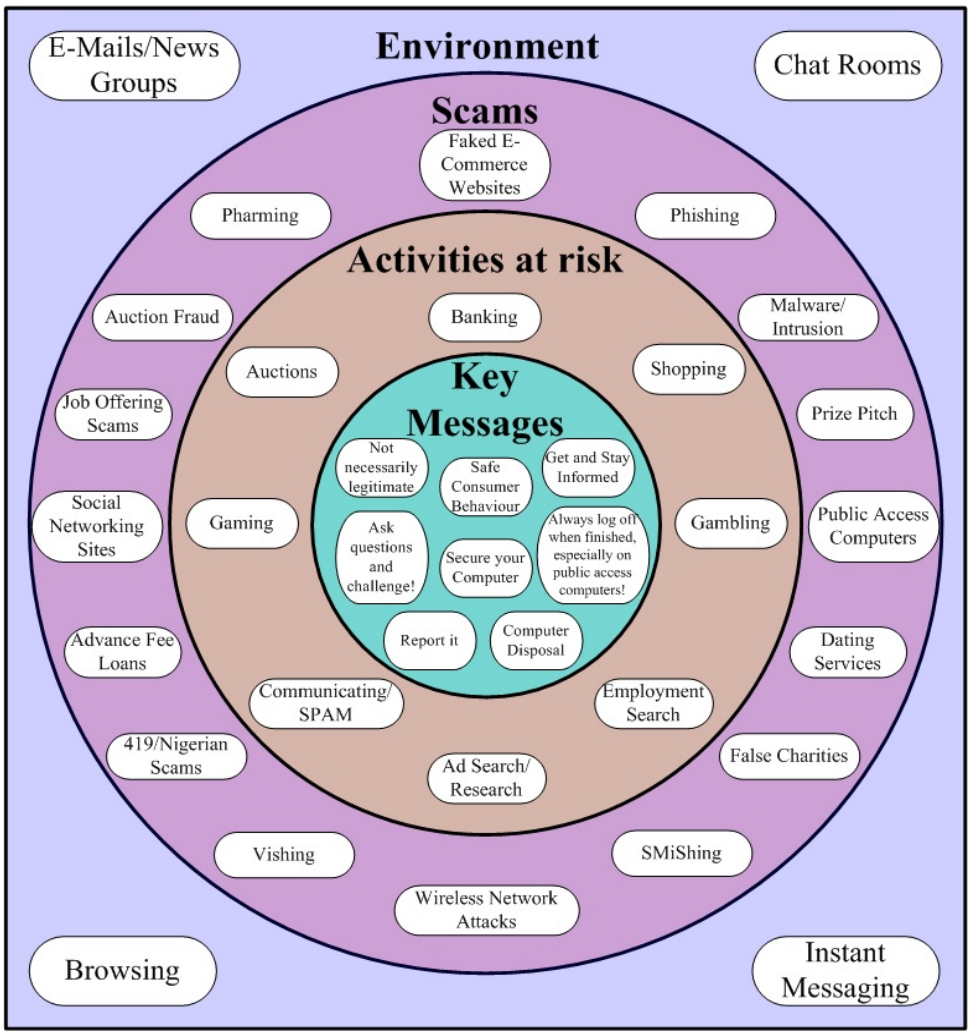


Figure 1: Key Messages to Help Avoid Online Scams Found in Different Environments

Numerous activities can be performed online such as shopping, ad searching, researching, auctioning, banking, communicating, employment searching and gaming just to name a few. As with traditional crimes, basic understanding is the key in reducing your risk of being victimized.

This section may contain unfamiliar terminology. To further expand your technological knowledge, basic descriptions and definitions can be found on web pages called "primers". The most effective method is to search with a term followed by the word "primer". For example, to learn more about "file sharing", type "file sharing primer".

1.1.1 Faked E-Commerce Websites

Be cautious of "too-good-to-be-true" offers. Some E-commerce websites are set up to capture your personal information. They will operate for a few weeks and then disappear. Successful scams always have rationalizations that potential victims want to believe. The Internet also has numerous legitimate businesses that claim to make you a good deal. Be smart, take the necessary time to research. Sometimes, it is just safer to ignore a good offer when you cannot validate it.

1.1.2 Phishing

Spam is the transmission of large quantities of unsolicited electronic messages. Just like spam, phishing messages attempt to a lure large number of individuals into providing personal information. Most often this is done by redirecting unsuspecting users to a fraudulent copy of a legitimate website. These messages use fear or urgency to trigger an impulsive reaction from the reader. Sometimes they will go as far as to tell you that you are at risk of being victim of identity fraud if you do not follow the provided link. They will use your information to gain financial advantages or to hide their criminal activities using your good name. You can outsmart them by never selecting any provided links and by immediately deleting the message. If you are still concerned, pick up the telephone directory, call the real company and get informed.

There is no guaranteed method to identify phishing E-mails and websites. Read and understand the indicators contained in Table 1.1 and 1.2. Remember, the presence of one or several indicators does not automatically mean it is a phishing attempt. It just means you should be more cautious.

Table 1.1: Comparison Between a Legitimate and Phishing E-mail

Indicator	**Legitimate**	**Phishing**
Greetings	normally personalized	may have strange greeting or not personalized
Spelling	normally does not contain spelling mistakes	may contain spelling mistakes
Urgency	give you time to think about the offer	uses upsetting or exciting statements to provoke impulsive and immediate reaction
Imbedded/Hidden Link	no deception	visible link appears legitimate but actual redirection may be fraudulent
Personal Information Request	normally information not requested	may be requested or lead to a fraudulent site that does
Sender	e-mail address is consistent with the identity/country of the sender	e-mail address may not be consistent/spoofed with the identity/country of the sender

Indicator	Legitimate	Phishing
Corporate E-mail Use	legitimate organizations avoid asking client personal information by e-mail	use of legitimate organization's name and reputation to contact a large number of consumers and may ask for personal information
Text	not likely to contain incomprehensible text	may contain disguised random text

Table 1.2: Comparison Between a Legitimate and Phishing Website

Indicator	Legitimate	Phishing
Secure Site Markers	https:// in address bar and padlock icon in the status bar	may have discrepancies or not have any security markers
Functionality	fully functional	may not be fully functional or may link to some of the legitimate site's functionality
Request for Personal Information	will not request for information that they already have	will request personal information
Domain Name	will use and display the correct domain name	address bar or status bar may be spoofed or contain a similar looking domain name or not have a status bar at all
Error in Browser Status Bar	normally will not contain error	may contain errors while loading web page
Login	will only be accessible with valid password	bogus user ID and password may work

The Internet is structured around a numeric protocol called IP for Internet Protocol. It currently uses IP version 4 which is essentially represented by four numbers from 0 to 255 separated by periods. For example 198.103.98.139 is the RCMP website's IP address. This is simply more difficult to remember than a domain name like "rcmp.ca". Criminals have become very clever in creating domains that sound and look like the real thing. These can be difficult to notice unless you know how to read them. In this section, we are going to show you how to read domain names.

Domain names are read from right to left. Consider the following the domain name in red in the following Web address:

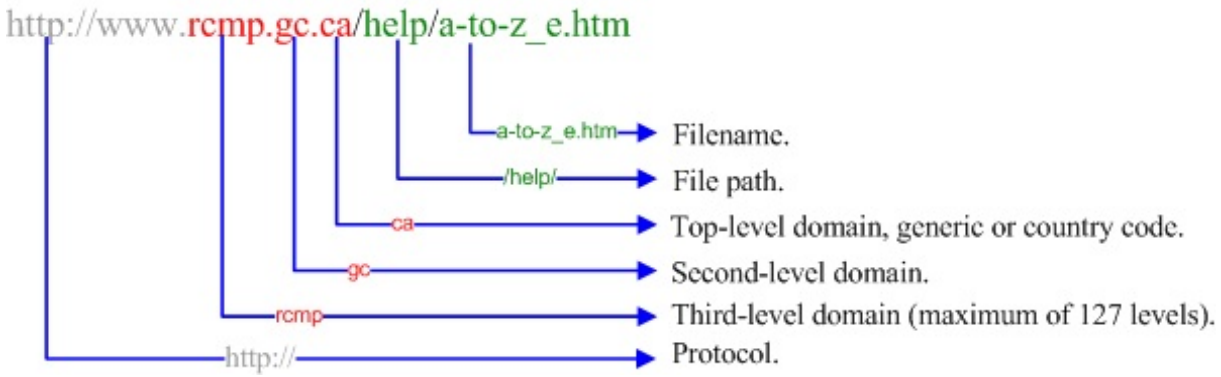


Figure 2: Complete Breakdown of a Website Address

This address will tell your browser that you are looking for the a-to-z_e.htm Web page (http://), located in rcmp.gc.ca domain, following the /help/ path. The www following the protocol identifier (http://) does not have any significance in the domain name. Your browser will send this domain name to a special server to see if such Top, Second or Third level domains exist. In this case, the matching Internet address is 198.103.98.139. Once you have identified the domain name, you may find more information about it by using a "Whois" site (See Appendix 1). This site will let you see if the domain registration is incomplete or if it is inconsistent with the corresponding organization. Your computer also has an IP address that may be recorded on sites that you visit. Therefore, your computer may be providing clues about itself and your identity. All of this information can be used by criminals to get more information on you and/or gain access to your computer. Choose a non descriptive email address. A bad choice is to use your name.

Phishing scams will often use variations of the legitimate name to fool the user. Beware of changes in the location of periods and slashes, as well as the presence of special characters and variations in the domain name. For example, if you were to replace the lowercase letter L ("l") in the following website, www.ghijklmnop.com , with the number l, you would be brought to following bogus site: www.ghijk1mnop.com . This subtle variation will go unnoticed if the internet user does not pay close attention to what is in the address bar. Another variation of a phishing scam would be the alteration of the Website address by adding a subtle domain level. This addition of a domain level would consequently change the position of all the following domain levels and therefore trick the user by bringing them to a different site than expected. Take the first example for instance, if you add a ".ca" before the real domain, you will end up with www.ghijklmnop.ca.com which becomes a totally different new domain.

There is no foolproof method to validate a website and there is always a possibility of a spyware infection on the user's computer or DNS poisoning. Always watch for unusual patterns and any discrepancies in the website's address or on it's web page. If you are suspicious about the website you are about to use, enter any bogus random username and password combination. This simple test will help you greatly minimize the risk of using a phishing website by observing whether or not the false username and password combination is accepted. Always carefully read onscreen warnings. Do not select anything without clearly reading and understanding it. One of the best ways to avoid being a victim of a phishing scam is to always delete unsolicited emails.

1.1.3 Pharming

Pharming, also known as DNS poisoning, is very similar to phishing but does not include any electronic message as bait. This type of scam is caused by a deliberate corruption of the DNS that directs the user to the requested website. This allows the hacker to redirect a website's traffic from a legitimate website to a corrupted website. Therefore, even if the user types in the correct URL (web address), the hacker can still redirect the user without his knowledge or consent to a bogus site.

1.1.4 Smishing

Smishing which is also know as SMS phishing is a new upcoming threat. This variation of the phishing scam uses the text messaging technology of mobile phones. The mobile phone owner will receive a text message with a URL address. Just like the phishing scam, do not select the URL address because you could download a Trojan horse. Be safe and immediately delete these text messages from your mobile phone message box.

1.1.5 Vishing

Now that web users are increasingly protecting themselves against phishing , scammers have adapted. Scam artists will now direct a victim to a telephone number instead of an internet address in the email that is sent in a phishing scam. It is important to know that these telephone numbers use the inexpensive technology of VoIP (Voice over Internet Protocol) which permits the scam artist to be able to recognize telephone key strokes and also allows them to be located anywhere in the world. When the person calls, a recorded message will ask the victim to enter personal numerical information on their telephone key pad in order to verify their identity. Never solely trust the caller ID information on your telephone because it can be manipulated. If you are concerned, contact the legitimate organization by using a telephone number you know to be safe. For example, use the telephone number printed on the back of your credit card to contact your credit card company.

Criminals may also target other personal or financial identification documents such as your driver's licence, passport, bank card and PIN as well as your health card.

1.1.6 Prize Pitch

A consumer may come in contact with a prize pitch scam by e-mail, telephone or mail. This scam is usually a prize notification. The consumer is led to believe that, to be able to receive or collect the prize, they must pay a series of bogus taxes and fees. A variation of this scheme would be when the consumer is asked to purchase a product or service in order to receive the prize. It is important for all consumers to know that if they do win a legitimate prize, there are no taxes or fees to be paid in order to receive a prize in Canada.

The recovery pitch scheme is a variation of the prize pitch scams. If you have been a victim of a prize pitch scheme, chances are that you may receive an e-mail or a call from someone promising you that they can recover your prize or money for a small cost. The caller will most likely pose as a police officer, a government revenue employee, a customs agent or a legitimate company employee.

1.1.7 Auction Fraud

Online auctions consist of a selection of items for sale that may be bought by bidding on the items. Online auction scams include such frauds as the misrepresentation of an item, non-delivery of goods and services, as well as non-payment for goods delivered.

The reason why many consumers are scammed through dealing with online auction houses is because they are either not following or not aware of the proper buying and selling procedures. Most online auction houses have an online learning guide and security tips available which contain information such as proper online payment method systems and precautions. These payment systems are very secure and when used, they may minimize the risk of becoming a fraud victim and may as well offer purchase protection. Do not be lured into switching to other payment methods by sending cash, money transfers or money orders. The safest alternative is paying with your credit card through the proper online payment system.

Escrow services are usually used when high priced items such as automobiles, jewellery and specialized computer equipment are purchased on online auction sites. Escrow agents offer a service where they will hold the buyer’s payment until they have received notification that the goods or services have been delivered. The escrow service then delivers the payment to the seller or provider.

Unfortunately, criminals will create fraudulent escrow sites by mimicking legitimate sites or creating entirely fictitious entities to get money from trusting victims. Also research the credibility of the escrow service approved by the online auction service provider. Promptly report any suspicious activities to the online auction security service.

1.1.8 Malicious Software (Malware)

Malicious software is designed to affect unintended computer behaviour. It can be found in different forms such as viruses, worms, trojan horse programs, spyware and adware. Computers can become infected with malicious software by opening e-mail, accessing a website, using infected media or downloading infected programs such as games. Malicious code may capture personal information from your computer or your keyboard and then transmit it to another individual. As information may be intercepted in its decrypted state on your computer, you should not solely rely on encryption.

Therefore, properly protect your computer by keeping your operating system and software packages up to date. Updated software such as anti-virus, firewalls, anti-spyware and anti-adware should also be used to protect your computer. You increase the risk of your computer being compromised by not updating the software. Be aware that malicious code may come disguised as any type of computer file and that a fully protected machine can still contain vulnerabilities. Be cautious of free software.

1.1.9 Wireless Communications

Any information travelling on airways could be at risk of being intercepted. As a safe practice, avoid transmitting or storing personal information in data or voice format over the following channels: cellular telephones, portable telephone handsets, unencrypted e-mails, unencrypted instant messaging, chatrooms, newsgroups, web pages and wireless network connections.

In the past few years, Wireless Networks (Wi-Fi) convenience has gained a massive increase in popularity with consumers. New products with built-in Wi-Fi capability are appearing on the market. To avoid accidentally exposing your information: disconnect or disable your Wi-Fi card when not in use, limit your use of Wi-Fi to non-sensitive activities like surfing, disable the automatic hotspot search/logon feature, check your computer file sharing settings and use strong passwords. Before initiating a Wi-Fi session, use an invalid user ID and password combination. Do not use the connection if you are able to logon with invalid account information.

A potential problem with wireless networks is called the “Evil Twin” or the “Wi-Phishing” scam. In this case, a legitimate hotspot is hijacked and the unsuspecting users are redirected to an illegitimate hotspot. As a result your information and files on your personal laptop or Wi-Fi device can be captured by the “Evil Twin”.

Table 2: Wireless Networks (Wi-Fi) Tips

Practice	**Tip**
Using an open or unsecured hotspot.	All information that you are sending and receiving is transmitted as a radio signal and can be monitored by all and the owner of the hotspot. This includes your personal information contained in your browser settings.
Using a secured access point or hotspot.	Technically, the administrator of the hotspot will be able to monitor your information but others will not. WEP is recognized as the weaker protocol, use WPA as it is more secure.

Practice	Tip
Using a secured session (https:// online banking or eCommerce session for example) on a secured hotspot.	It is always preferable to use a regular Internet connection for this purpose. If the hotspot is legitimate your information will be fully encrypted from your computer to the secured site.
Use and Configuration of a household Wi-Fi router/device.	Be aware that criminals may actively scan your neighborhood to gain entry to your network /computers. - Avoid purchasing bargain priced equipment. - Consider turning off or disconnecting this equipment when not in use, including routers . - Use a different SSID (service set identifier) than the provided default and do not broadcast it. - Use a WPA encryption key with the maximum level available. - Switch your device to another channel than the default one. - Do not use default IP range or DHCP. - Consider MAC address filtering.

1.1.10 Public Access Computers

Public libraries, Internet Cafés, campuses, hotels and even camp grounds are equipped with public access computers. Avoid using public access computers for online banking, sending emails containing personal information or using your payment cards for online purchases. If you do have to use these computers, sign out of your online accounts, clear your browser's cache, delete the cookies, delete the history and close the browser. To get the instructions for your specific browser make and version, visit the developer's website and search for the following words: "clean browser cache", "delete cookies" or "delete browser history".

Using common sense will also help reduce the risk of having your personal information stolen when using a public access computer. Simple things, such as not leaving the public access computer unattended or hiding your password when typing it, will help reduce the risk. Also note that public access computers are usually secure but there is no way of the user to be completely sure about that.

1.1.11 Social Networking Sites

An online social network consists of Internet applications that create an online social structure facilitating connectivity between individuals. Social networks may also indicate the way that individuals know each other. Online social networks offer services such as instant messaging and may permit users to have blogs and messaging files. A blog, which is short form for weblog, is an online publication of periodic articles usually focusing on a single topic. But more recently, blogs have been used as personal web-based diaries which contain text, images and links to other blogs and web pages.

When you are posting information about yourself online, you should minimize your personal information exposure. When possible, it is recommended not to post information such as your full name, date of birth, home address, telephone number, social insurance number and anything that may be of interest to a financial or sexual predator. Also note that posting your personal interests or hobbies on your profile or blog could be used as a lever for social engineering. Read and clearly understand the terms of agreement and the privacy policy to ensure the proper use and storage of your information. Be aware of the social networking site's default security settings. Some of these default settings will allow anyone to see all of your personal information.

When using the fun and useful technology of online social networks, follow these 10 safety steps to minimize the risks of becoming an identity fraud victim.

Table 3: The 10 Steps To Safe Online Social Networking

Step #1	Do your research. Carefully investigate any online social network you may want to join. Use only well known online services.
Step #2	Once you have picked a service, carefully read and clearly understand their Terms of Use.
Step #3	Carefully read and clearly understand their Privacy Policy. Avoid using services that share your information with other companies.
Step #4	Never expect absolute privacy! Create your account without providing any critical personal information. Do not provide valid critical information like: date of birth, full name, social insurance number or address.
Step #5	Protect your account profile with the highest and most restrictive security setting.
Step #6	Build your profile. For each element of information you add, ask yourself this question: "Can a financial or sexual predator benefit from this information?"
Step #7	You control your online environment. Do not give strangers permission to view your profile.
Step #8	Protect your friends. Be careful of what you are posting on the Internet about them.
Step #9	Monitor your own page for personal information posted by friends in their messages. Also monitor your friends' pages for your personal information. A simple comment or a photo may reveal your date of birth or give information that could be useful to predators.
Step #10	Be creative, be safe and have fun!

1.1.12 Dating Services

An online dating service allows individuals and groups to meet online to hopefully start a romantic relationship. Online dating services are used by scammers. They make false statements in their online profiles and in their communications with potential victims. Often they pose as individuals from foreign countries. They will gain your trust by exchanging heart felt stories through emails, telephone calls and IM (instant messaging). After you are comfortable with this new encounter, they will ask to visit you. The goal of this visit could be either to marry you, to escape their country or to finally meet you. They will most likely ask you to pay for their airfare, passport costs or other costs linked to travelling. After sending the money, chances are you will never see or hear from them again. You will also never retrieve your money.

Remember that with time and practice, a successful con artist becomes skilled at manipulating emotions. Therefore, always keep in mind that the person you meet online might not be who they say they are. Even if the individual has a profile picture and seems very sincere, you might be dealing with a person who is using a false identity to get your money. Promptly report suspicious activity to Recol.ca or PhoneBusters at 1-888-495-8501 or www.phonebusters.com.

1.1.13 Advance Fee Loans

Advance fee loans are commonly advertised in the classified ads sections of newspapers, magazines, and tabloids. They can also be found on the Internet. These ads guarantee a loan regardless of the applicant's credit history, but the applicant has to pay an up-front loan fee. Needless to say, the applicant never receives the loan and loses the advance payment. Legitimate financial companies do not ask for an up-front payment. This practice is illegal in Canada and in the United-States.

Do not agree to pay fees to obtain a loan. Do not believe promises of automatic loan approval, particularly if you have a poor credit rating or no credit history. If in doubt, consult with experts from a known legitimate financial institution. Promptly report suspicious activity to Recol.ca or PhoneBusters at 1-888-495-8501 or www.phonebusters.com.

1.1.14 Job Offer Scams

Be aware of job scams when searching for employment. Keep your online resume anonymous and only provide an email address for contact purposes. Do not give too much information to a potential or new employer. Do not divulge your personal bank account, credit card number and username/password for online accounts. You do not need to provide your Social Insurance Number (SIN) when applying for a job. The employer will only need it once you are hired. Be cautious when applying for job postings found in the classifieds, in the newspaper, on a bulletin board or on the Internet that involve package forwarding, money transfers, wiring funds or well paying telemarketing jobs. You may end up becoming involved in criminal activities. Report suspicious activities.

1.1.15 False Charities

False charities prey on a person's giving nature to scam them into giving a donation. They will often use stories that are heavy-hearted and patriotic. The stories may focus on recent catastrophic events. Bogus charities will often have names that resemble legitimate charities, either adding or changing a word in a legitimate charity's name. There are several things that you may do to avoid becoming a victim of false charities. First, be careful of incoming e-mails or calls because it could be someone misrepresenting a legitimate charity. Also be cautious of similar sounding charity names. If you have any doubts on the legitimacy of a site, independently visit the charity's official website or call the charity. Do not use the web address or telephone number that the charity in question supplies.

1.1.16 419/West African Letters

The 419/West African letter scams, also known as the advance fee letter fraud, are letters sent to individuals or businesses requesting assistance with foreign money transfers in exchange for a percentage of the transfer amount. These letters may be received by e-mail, mail or fax transmission. They emphasize that trust and honesty are important aspects in this confidential business transaction. The writer will often present himself as a doctor, a representative of the Nigerian National Petroleum Corporation or as someone in the Nigerian or some other African national government or military. Be cautious as these scams may use the names of other foreign organizations and countries

If the victim communicates with the writer by e-mail, mail or phone, he will usually be asked to pay various expenses such as bribes, taxes, registration fees and attorney fees up front. This may continue over an extended period of time and be a condition before the money transfer can be completed. Obviously, the victim will never receive any money. Do not respond to these types of letters. Send a copy to PhoneBusters at info@phonebusters.com or fax to 1-888-654-9426.

1.2 Public Settings, Friends and Acquaintances

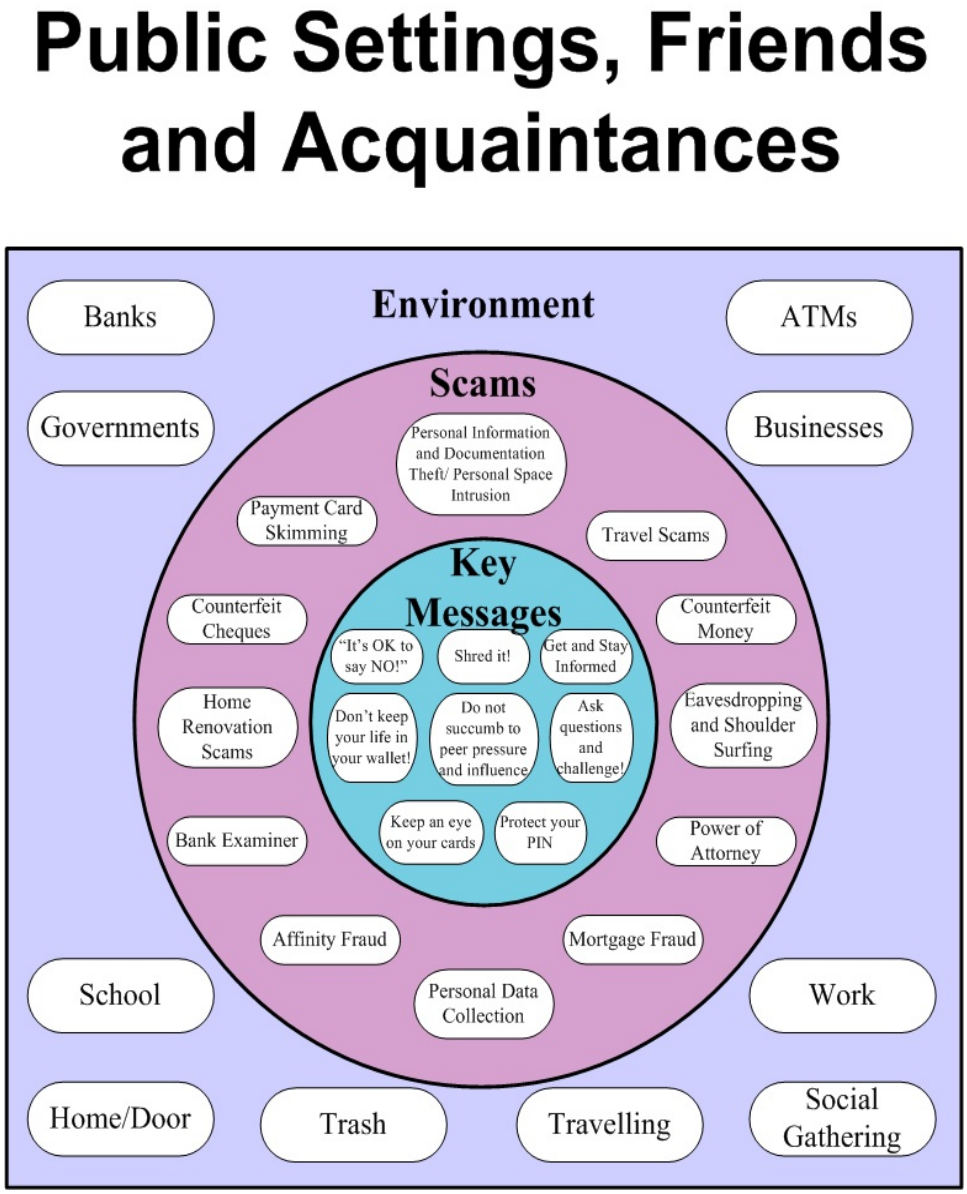


Figure 3: Key Messages to Help Avoid Scams in a Public Setting Found in Different Environments

You lead an active life style constantly alternating between work, home and school. These activities put you in contact with a large number of individuals and organizations. This section deals with such scams as wallet theft, card skimming, counterfeit money, shoulder surfing, dumpster diving and eavesdropping.

1.2.1 Theft or Loss of Personal Information and Documentation

Do not keep your life in your wallet or in your car. Only carry the documents you need for your daily activities. Do not carry your social insurance number card, birth certificate, passport, or any other document containing this information. Documents like old hospital cards may contain more information than you think. Therefore review the content of your purse or wallet. Store these documents and cards in a secure place such as a locked drawer, cabinet or safety deposit box. Shred unnecessary documents.

1.2.2 Counterfeit Cheques

Counterfeit cheques are either altered or fabricated. They are commonly associated with the "too good to be true" scenarios. These scams include prize pitch scams, advance fee loans scams, fraudulent lottery scams, job scams and online auction scams. In a typical scenario, in exchange for goods or services, the potential victim is offered a cheque that the buyer supposedly already has in his/her possession. The amount of the cheque will be more than is owing, the potential victim is asked to take the counterfeit cheque and reimburse the difference. This fraud capitalizes on cheque processing delays. The bank will hold the victim responsible for the counterfeit cheque. Never accept cheques larger than the transaction value and always wait for the cheque to be fully cleared before delivering the goods or services. If it sounds to good to be true, it simply is. Caveat Emptor! (Buyer Beware!)

1.2.3 Counterfeit Money

Canada's bank notes are issued by the Bank of Canada. The Bank is responsible for replacing mutilated genuine bank notes but is not responsible for reimbursing victims of counterfeit notes. The best way to protect yourself from becoming a victim of counterfeiting is to make it a habit of regularly checking bank notes.

There are several security features on Canadian bank notes that are reliable, easy and quick to use. The Bank of Canada suggests that you should always feel, tilt and look at and look through bank notes to verify them. For information on how to verify whether a bank note is legitimate, please visit the Bank of Canada website at http://www.bankofcanada.ca/en/banknotes/counterfeit/security_features.html.

In order to minimize the risk of possessing a counterfeit note, take time to verify most of these features. Verify more than one security feature during a transaction to see if the bank note is legitimate. You may ask the merchant to give you a different note if you are uncomfortable with the note you have received.

If you do come in contact with a counterfeit note or one that you suspect is counterfeit, stop the transaction and request another note. If a counterfeit bank note is received through an ATM machine, it is your obligation to turn it over to the proper authorities such as local police or a bank teller. You will not be reimbursed for counterfeit bank notes. But most importantly, you should not try to pass it off to someone knowing it is counterfeit. You could face criminal charges.

1.2.4 Personal Data Collection

It is important to be cautious when filling out prize entry forms at malls, sport shows and conventions. The personal information you provide may later be used by third parties to contact you by phone, by sending you spam or junk mail in order to lure you into giving them more personal information or to access your accounts. Some fraudulent organizations will even analyse the writing on the entry form to find potential victims for their scams.

1.2.5 Travel Scams

Although vacation solicitations occur all year round, they tend to be more frequent during the travel season. Always use a healthy dose of skepticism when receiving these solicitations whether it be by email, fax or telephone. Especially when an unknown company congratulates you for winning a free or an inexpensive deal on a resort vacation or cruise. This kind of solicitation will most likely be a travel scam. These illegitimate travel companies will ask for your credit card number and some personal information. Hence possibly compromising your identity and your finances. An additional risk is the deceptive practice of dishonest travel agencies to lure a victim to a remote destination and charge extra fees for features and services that were supposed to be included in the initial travel package. Therefore making your dream holiday into a very stressful experience. It is safer to deal with reputable well established travel agents.

1.2.6 Home Renovation Scams

Home renovation scams will normally peak during spring. Victims will be offered home renovations normally by going door to door throughout their neighborhood. Various pretexts can be used to justify an attractive price such as “they are working nearby and they have extra supplies” or “they have a special discount for seniors”. The contractor will request for a down payment upfront and never show up to perform the work.

Before getting into any home renovation projects, get informed with provincial and federal consumers agencies to learn about your rights and how to properly protect yourself. Also do not be shy to shop around and get a few estimates before settling on a contractor.

1.2.7 Payment Card Skimming

Always keep your credit or debit card in your sight when used during a purchase. Do not let the employee leave with your card. In this process called card skimming the employee secretly swipes your card through a small device that captures and stores your card’s magnetic strip information. This information can be used to replicate your card. Be sure to protect your PIN with your hand when typing the keys. This will diminish the chance of a shoulder surfer or a hidden camera to capture your PIN.

Near or on the signature panel of your credit card you will find a 3-digit code which is known as the credit card verification code or card verification value. This code is used by merchants to confirm that the consumer has the card in their possession during an Internet or telephone transaction. This is another piece of information that you should not share with anyone unless you are making one of these transactions or contacting your credit card issuer.

In a recent variation of this scam, dishonest employees or skillful scam artists switch the payment card terminal keypad with their own. Although this keypad may look identical at first glance, it has been modified with the addition of a second reading mechanism in the card swiping slot, and a storage device wired to the keypad. This enables criminals to store your card’s magnetic data and your PIN. The information is subsequently downloaded, fraudulent cards are manufactured and the criminals are ready to shop with your cloned card and your PIN.

Table 4: Tampered Payment Card Terminal Indicators

Indicator	Legitimate	Counterfeit
Terminal Case	The case has no sign of tampering, the components fit together well with no cracks or gaps. In the back, the case is fastened with permanent rivets, proprietary (special) screws or the fasteners are concealed within the case. Wires are never visible through ventilation slots at the back.	The case may show signs of tampering, cracks, gaps or not fitting well. The back of the case may be fastened with regular screws. Wires may be visible through the ventilation slots.
Reading Mechanism	Only one reading head is visible in the terminal card swiping slot.	The presence of two reading heads or evidence of tampering may be visible in the card swiping slot.

Call your local police when you suspect a counterfeit payment terminal. You should also be aware that gas pump payment card devices can also occasionally be altered. Favour the use of credit cards over debit cards in these devices as they offer you more protection.

1.2.8 Bank Examiner Scam

The bank examiner scam is also known as a bank inspector scam, a fake banking official or as the teller trap. A person claiming to represent the victim's bank will get in touch with the victim because the bank allegedly needs an honest client to assist in the investigation of a corrupt customer service representative. The victim is asked to withdraw a large amount of money through a specific customer service representative. The examiner then takes the money to record the serial number for future tracking. He hands out an official bank receipt and promises to return the money in a few days. The money is never returned because neither the receipt nor the bank examiner are real. Variants of this scam may use fraudulent police officers or lawyers. If someone contacts you with such a pretext, do not participate! Immediately advise your bank, the local police and PhoneBusters at 1-888-495-8501 or www.phonebusters.com.

1.2.9 Shoulder Surfing and Eavesdropping

Although these two activities may not be considered scams, they are used in conjunction with a variety of scams. Shoulder surfing and eavesdropping are used to collect personal information and documentation such as building access codes, alarm system passwords, PINs, userid/passwords and credit card information. Hide your keystrokes when punching in this type of information. Use your hand and body to shield the keyboard or number pad to minimize the risk of a shoulder surfer to acquiring your information. Make sure that nobody is eavesdropping when voicing such information. Do not use wireless devices to transmit this information.

1.2.10 Power of Attorney

A Power of Attorney is a legal document authorizing someone else to act on your behalf in a legal or business matter. The level of control can range from minimal to full control. This legal document is revocable but what is not is any action legally undertaken while a valid Power of Attorney is in effect. This is why you want to give careful considerations on how much control over your life you want to give and to whom. Con artists will normally seek financial control over their victims. Always keep in mind that a family member or close friend may be using their privileged access to commit fraud and theft. Do not sign anything unless you read the documents and all attachments. Fully understand what you are signing.

1.2.11 Mortgage Fraud

Your personal information can be used to commit mortgage fraud under your name. A criminal assumes your identity and poses as yourself. They can then gain control of your residential land title, sell the property or obtain a mortgage on it. They can also purchase and acquire mortgages under your name. Mortgage fraud is often facilitated by negligence or the collaboration of some professionals.

Carefully guard your personal information. Check your credit report regularly for unauthorized financial accounts and properties in your name. When in doubt, you can request a property search at your provincial land registry office to ensure that your home's title is still in your name.

1.2.12 Affinity Fraud

An affinity fraud is normally associated with investment scams. Usually the potential victim is approached by a member of the same church, community or professional group. This initial trust is leveraged over time by the criminal to entice the potential victim into an investment opportunity. Before giving your trust away, do your homework. Verify every statement about this investment. Do not hesitate to consult with third party professionals. Be wary of unusually fast and large return on investments, this is a fraud indicator. Remember, if it's to good to be true, it probably is. If you suspect fraud, call your local police and notify PhoneBusters at 1-888-495-8501 or www.phonebusters.com.

1.3 Telephone

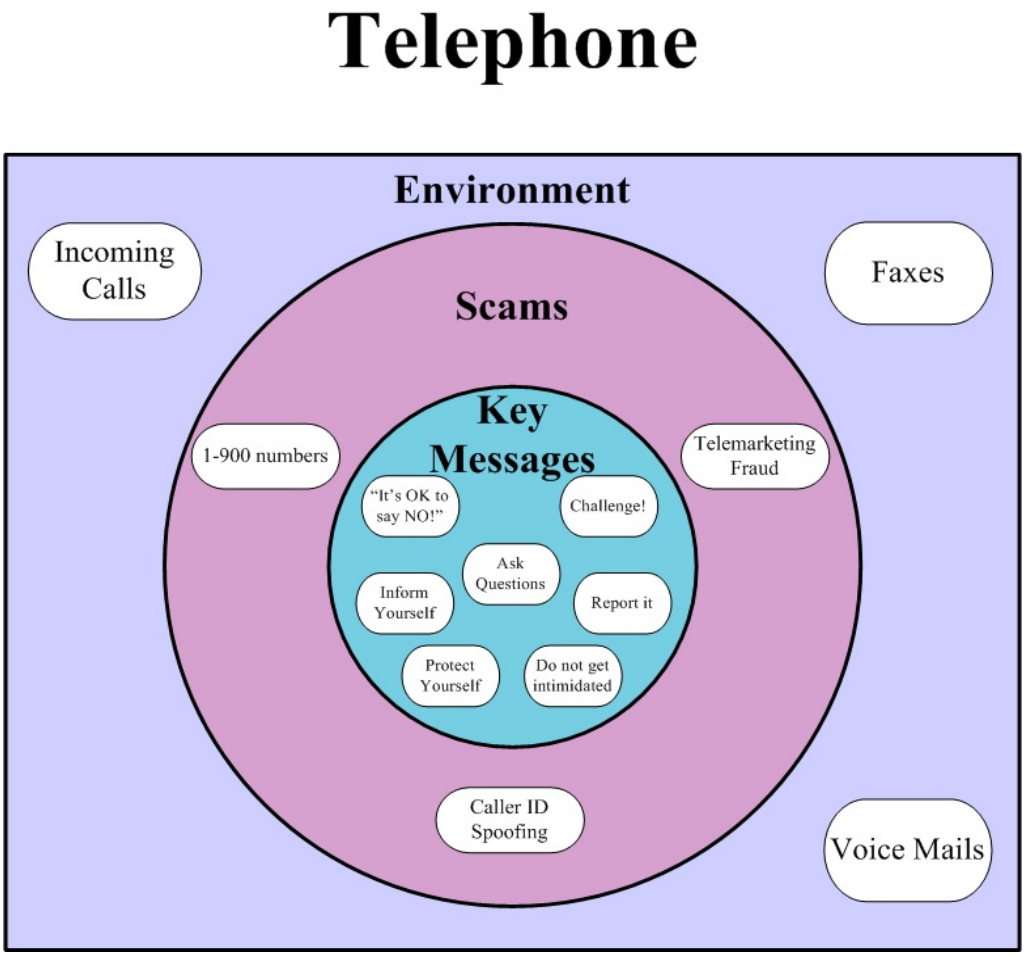


Figure 4: Key Messages to Help Avoid Telephone Scams Found in Different Environments

The most common telephone threats come by fax, voice mail and incoming calls. Caller ID or call display is a service used to identify the number and the name of the person or organization calling. Do not be fooled by always trusting this service. There are other services that allow a caller to spoof the caller ID display of the person they are calling. This is done by falsifying the number and the name that appear on the display. Scammers may use this technology to mislead you into giving your personal and financial information. You should never give out information over the telephone.

1.3.1 Telemarketing Fraud

Telemarketing is used by legitimate businesses to advertise and sell their products and services over the telephone. Unfortunately, criminals also use the same telemarketing techniques to defraud people. You should therefore be cautious when receiving a telephone call stating that there is an amazing promotion or prize to be won. Also be cautious of organizations that you do not know and do not be fooled by their extravagant promises. Remember do not disclose any personal or financial information over the telephone. Do not be afraid to say no and hang up. A mistake made by many consumers is to associate 1-800 numbers with legitimate telemarketing companies. This is not always the case. Therefore, do not use this as an indicator to differentiate between legitimate and fraudulent telemarketing companies. If you would like to report any suspicious phone calls, contact PhoneBusters at 1-888-495-8501 or www.phonebusters.com.

Table 5: Comparison Between Legitimate and Fraudulent Mass Marketing

Indicators	Legitimate	Fraud
Enthusiasm	May be very enthusiastic	The caller is more excited than you are
Friendliness	May act overly friendly	Want to create a personal connection to possibly be leveraged later
Pressure	May be a legitimate technique to close the deal, will not normally get verbally abusive	Want to force you into providing what they want, could get verbally abusive
Urgency	You may have time to think about the offer	Will pressure you into making a decision if you don't act now, may demand an immediate answer
Willingness to provide full references	Normally not a problem, complete contact information will be provided	May be more reluctant or willing to provide only limited information like a telephone number
Mode of payment	Normally, many options are available	Usually limited to courier or wire services
Price	Market value	Unreasonably low price with unrealistic explanation
Benefits	Value of benefits or incentives is realistic in order to turn a profit	Unreasonably high incentives or benefits with unrealistic explanations, too good to be true
Credit offers	Normally based on your credit rating	May make offers regardless of your credit rating
Surveys	Your information will be used for the intended purpose	Your information may be used for criminal purpose
Explanations	When challenged, will normally provide clear explanations that make sense	Explanations are complicated, unclear and confusing
Social Engineering	Could be used as a sales tool	May be used to gain psychological advantage over the victim and to trick them into providing their personal information

1.3.2 900 Scams

The 900 scams are similar to the prize pitch scams. In a 900 scam, consumers receive an offer in the mail enticing them to call a 1-900 number to learn about the type or value of prize they have won. The problem is that the call will usually last several minutes before the caller finds out that the value of the prize is very small. Some 1-900 numbers will advertise a free gift if you call, but you end up paying for the gift by making the 1-900 number call. Remember, 1-900 numbers have a per-minute rate. If you are concerned about a 1-900 number, immediately contact PhoneBusters at 1(888) 495-8501 or www.phonebusters.com.

1.3.3 Caller ID Spoofing

Caller ID is a useful function. However, the information displayed can be altered by criminals. Never use only the displayed information to confirm the identity of the caller whether it be an individual, company or an organization.

1.4 Printed Material

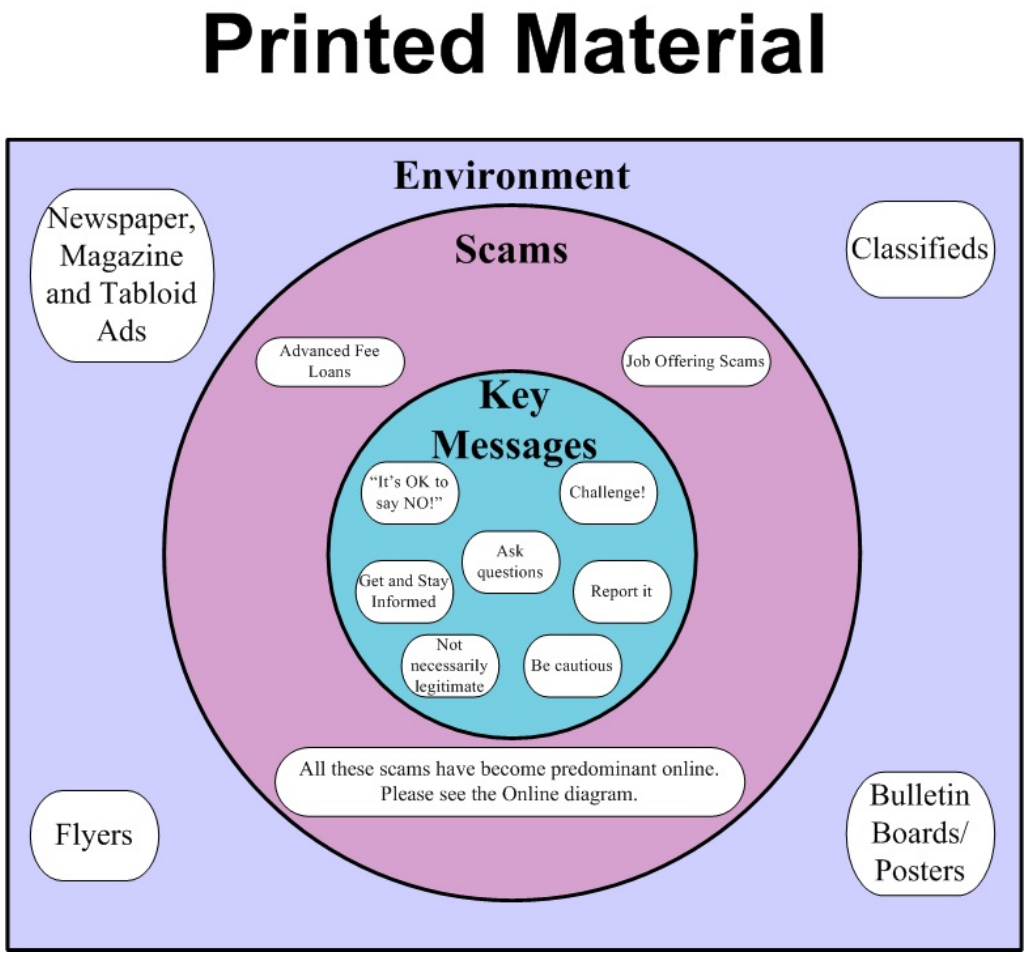


Figure 5: Key Messages to Help Avoid Printed Material Scams Found in Different Environments

Ads for jobs, advance fee loans, sweepstakes, lotteries and valuable merchandise can be found in newspapers, magazines, tabloids, classifieds and flyers or on bulletin boards and posters. Some of these ads could be scams to obtain your personal and financial information or to just steal your money. Be cautious when responding to these printed ads. Keep in mind that ads which are published in local newspapers, popular magazines, or posted on bulletin boards, are not necessarily legitimate. You must take certain precautions such as researching the company's credibility and calling the company to verify if they did publish the ad. You may fax suspect ads to PhoneBusters at 1-888-654-9426.

In certain provinces and territories a significant amount of personal information is printed on prescription bottle labels and associated receipts from pharmacies and hospitals. Before recycling or discarding these items, you should shred anything with personal information on it.

1.5 Mail

Mail

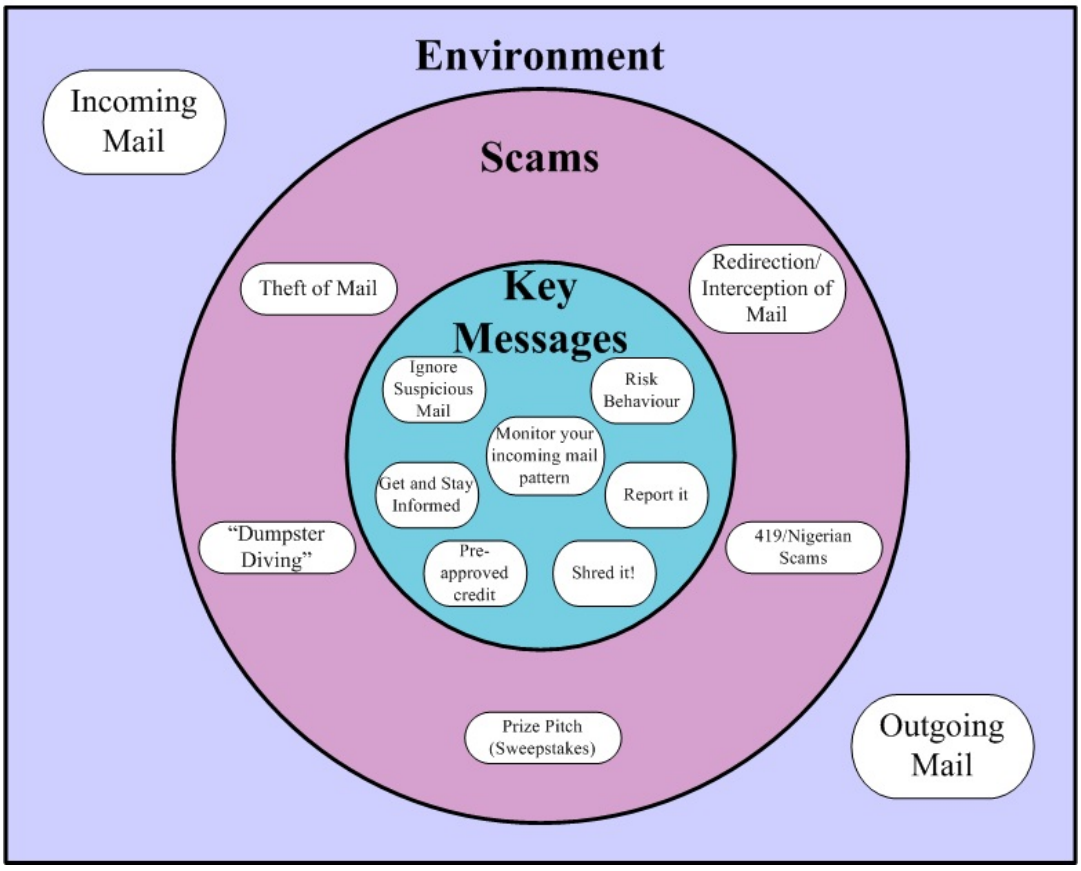


Figure 6: Key Messages to Help Avoid Mail Scams Found in Different Environments

It is likely that you have previously received mail advertising prizes, vacations and services. Many of these solicitations may not be legitimate. They are variations or copies of scams equivalent to the advance fee loan, prize pitch, false charity and the West African scam. These solicitations may come as postcards, certificates, unsolicited cheques, letters congratulating you for prizes or lotteries, free magazine subscriptions, credit card approvals and loans offers. Evaluate all incoming mail carefully. For example, if you receive a pre-approved credit by mail and you decide not to follow up on it, make sure you shred it before throwing it in the garbage. You never know, it could be retrieved by dumpster divers.

There are other mail threats that could be used to steal your information such as mail theft, interception and redirection. Having a locked and secured mail box is the first step to ensuring the safety of your mail and its contents. You should also only deposit mail in post office collection boxes or at your local post office. Being aware of your billing cycle and regularly verifying your mail are good habits to help figure out if your mail is being intercepted and redirected. Also, when moving, you should carefully change your address. Ensure that all the service providers are advised of the move. This will help to ensure that your billing cycle stays consistent.

2. Roles and Activities

2.1 Businesses:

Corporate citizens are the forgotten victims of frauds. Not only can they be directly victimized by criminals, but their clients' and customers' personal information can also be compromised. The imagination of criminals and the ease with which they adapt scams to new technologies will topple unprepared businesses.

Fraud is everyone's problem. Getting actively involved in fraud prevention, detection and reporting will make a business part of the solution.

This section of the guide will specifically focus on teaching businesses to protect themselves against fraud. It has been created as an integral part of this guide and should be read in conjunction with it. We will present fraud as it presents itself to owners and staff.

2.1.1 Identity Fraud

Businesses that collect personal information have the obligation to protect that information. If client personal information is compromised, businesses should inform and help educate their clients about identity fraud. The clients should be informed about the three credit reporting agencies and where to get more information.

The Consumer Measures Committee has published an *Identity Theft Kit for Business*. It is available on their website at http://cmcweb.ca/epic/site/cmc-cmc.nsf/en/fe00091e.html. This kit is a very useful tool for businesses. It has sections on the collection, use, disclosure, data security, storage and disposal of customers' personal information. It also has a section entitled *Steps to Take When Information is Compromised* that proves to be a good guide for this type of situation.

Here are a few key safety measures that should be taken into account to help protect your clients' information.

How to Protect Your Clients' Identity

a) Collection of Client Information

To minimize the risk of information being compromised, store client data on a stand alone computer that does not have internet access and is not connected to your office's local area network (LAN). This computer should have a password login and restricted access within your office.

It is important to be discrete when recording a client's personal information. Use a low voice when repeating the client's information for verification. If the information is written down on paper before recording it electronically, the paper should be shredded. Also note that the computer monitor should not be positioned in a way that public can see the client's information on the screen. Always make sure that the only eyes to see the screen are the ones that are allowed to access that information.

b) Network Security

Properly protect your computer by keeping your operating system and software packages up to date. Updated software such as anti-virus, firewalls, anti-spyware and anti-adware should also be used to protect your computer. You increase the risk of your computer being compromised by not updating the software. Also note that you should use well known business protection software companies. Be aware that malicious code may come disguised as any type of computer file and that a fully protected machine can still contain vulnerabilities.

c) Computer and Electronic Equipment Disposal

Before giving away, selling or throwing out old computers, PDAs (personal digital assistants), cellular telephones, CDs, DVDs, diskettes, backup tapes, memory sticks, and all other memory storage devices, you should consider the following preventative measures. If you intend to give away or sell your old computers, you should use a disk wipe utility that is on a bootable cd that will completely wipe the information on your hard drives. The common misconception is, if you just format the hard drive, all information is erased and unretrievable. This is not true. If someone was to use a file recovery software, much of the information would be retrievable. So, if you are throwing out your old computers, you should first wipe the hard drive or remove it and smash it several times with a hammer. Equally, when throwing out your PDAs, cellular telephones, CDs, DVDs, diskettes, backup tapes, memory sticks or other memory storage devices, if you are not confident that you can erase them, then you should smash these devices with a hammer. The reason is that these devices are highly sought after by criminals and may retain residual information that could be "recycled" for criminal purposes.

d) Physical Access Control

Controlling public and employee physical access to clients' and customers' personal information can help minimize the risk of having their information compromised. Physical access control can be done with lock and keys or access control cards. If you use physical access control for a room or a specific section of your business, you have more control by distributing keys and access control cards to a minimum number of employees. If an employee does not need access to clients' and customers' personal information do not give them access to it. Physical access control should be managed by a trusted administrative assistant or office manager .

e) Laptop Security

Avoid putting sensitive information such as clients' personal information on business laptops. Laptops are unfortunately too easy to misplace or have stolen. When not in use, laptops should always be locked away. Also educate employees to not collect or store clients' information on laptops and PDAs. If there is no other choice, make sure that the laptop's Wi-Fi is turned off, file sharing is disabled, the files are encrypted, and that the laptop does not leave the office.

f) Wireless Networks

Please refer to section 1.1.9, "Wireless Communications," for a short description of wireless networks and their related scams. Please also refer to Table 2 which is found in the same section.

2.1.2 Invoicing Fraud

Invoicing fraud is a common scam that targets businesses. Illegitimate telemarketing or deceptive mail are usually the sources of this type of scam. When receiving an invoice, the business should carefully read and verify it. If the invoice is for a product that the business has not ordered, they should not send a payment. Even if a product has been received, a business should not send payment for a product which was not ordered. They should contact the seller to inform them that they did not want or order the product and that the seller should arrange to have it picked up. The business should make it a habit to properly study incoming invoices and verify that there are corresponding orders. Always make sure that the supplier on the invoice is correct. There are illegitimate suppliers using similar sounding names of companies that businesses usually deal with. Be aware of the small variations of this scam. By way of example, a business may receive a fraudulent invoice to renew a membership with an association, renew an Internet domain name or pay for advertising.

For more information on this scam, visit the *Fraud Awareness Fact Sheet for Small and Medium - Sized Enterprises* page at http://www.competitionbureau.gc.ca/internet/index.cfm?itemID=2051&lg=e .

2.1.3 Spoofed E-Commerce Website

A business can also be the target of phishing. As mentioned previously in section 1.1.2. “Phishing,” do not follow any links that you receive in emails claiming that your business’ information needs to be updated.

Unfortunately for businesses, they can also victimized by a phishing scheme. Their commercial website could be spoofed and therefore their clients’ or potential clients’ information could be compromised. If this is the case, you as the business owner or representative can find out the Internet service provider (ISP) of the spoofed site by using www.whois.net. Inform that ISP about the spoofed website situation. File a report with www.recol.ca and always notify local authorities. The victimized business should post a warning on their website about the spoofed website to inform their clients who may have been victimized.

The business owner or representative should also do a regular search on www.domaintools.com to monitor the use of their business name. This is an extra precaution that should be conducted to ensure that their website has not been spoofed. If the e-commerce website has been spoofed, the damage can either be avoided or minimized by following the aforementioned steps.

2.1.4 Counterfeit Cheques

Please refer to section 1.2.2, “Counterfeit Cheques,” for a short description of counterfeit cheques and their related scams. A business owner or financial officer should be aware that there is the possibility for a business’ cheques to be intercepted, obtained, altered or fabricated for the purposes of comitting fraud. Therefore, it is important for either the business owner or the financial officer to keep track of cheques which are sent out to clients or companies. The business owner or the financial officer should take note of the amounts on the cheques sent out and should compare those amounts to the ones in the bank statements. If there is a discrepancy in the authorized amounts of the cheques, they should contact the bank. It may be that the business’ cheques have been counterfeited. If this is the case the business owner should, if possible, close that account and open a new one to maximize the business’ financial integrity. Therefore, if there is suspicion of foul play with the business’ cheques, contact the bank, close the account, contact the local authorities and report the incident on www.recol.ca .

2.2 Caretakers:

A caretaker is someone who looks after a person. For the purpose of this document a caretaker can be a parent, daughter, son, relative, friend, neighbour, community service representative or someone hired to look after a person.

Table 6: Prevention, Detection and Assistance for Caretakers - Seniors

Environment	**Prevention (Before)**	**Detection (During)**	**Assistance (After)**
Public	1) Get informed and stay informed on threats faced by seniors. 2) Inform the person in a gradual and non-alarming fashion. 3) Create an awareness of the value of personal information to criminals and the problems it can cause once compromised. 4) Teach the senior to not engage in a situation when they are suspicious. 5) Teach the senior that it is OK to be rude and disengage in certain circumstances. 6) Open the communication channels, invite the senior to share any question or concerns on situations they may be experiencing.	Watch for changes: 1) The senior seems overly agitated or excited for no apparent reasons. 2) The senior is evasive to answering questions. 3) Sudden changes of patterns in the amount and nature of visitors. 4) Evidence of unexplained money transfers and money order receipts to obscure places or foreign countries.	1) Reassure the senior. 2) Do not be jugmental. 3) Offer help and support. 4) The key message is that people of all ages and sexes can be victims of fraud. 5) Do not raise any false expectations on recovering lost money. 6) Use education to prevent future victimization. 7) Seek support from local community services if necessary. 8) Consider seeking support, positive reinforcement and follow-up from the senior volunteers at PhoneBusters.
Telephone	Same prevention techniques as identified in the public section.	Same detection techniques as identified in the public section except for number 3. Also watch for: 1) Changes in nature and number of telephone calls. 2) The senior is taking telephone calls in privacy and secrecy when you are present.	Same assistance techniques as identified in the public section as well as: 1) Consider recommending a change of telephone number.

Environment	Prevention (Before)	Detection (During)	Assistance (After)
Mail	Same prevention techniques as identified in public section as well as: 1) The caretaker should help the senior go through their mail and sort out the junk mail from the rest. Disregard and destroy any unsolicited offers, especially announcements of winnings.	Same detection techniques as identified in the public section except for number 3. Also watch for: 1) Changes in the nature and quantity of mail received such as large amounts of mail from foreign countries and large numbers of magazine subscriptions. 2) The senior attempts to hide mail from you. 3) Various brochures and promotional materials start to appear.	Same assistance techniques as in public.

SeniorBusters:

SeniorBusters is a program that supplies seniors with the necessary tools to fight fraudulent scams. The senior volunteers at SeniorBusters will contact the senior victim or potential senior victim, their family members and the local police to assist the senior. Therefore, if requested, SeniorBusters can help teach the senior how to become a fraud fighter instead of a fraud victim. They can be reached through the general PhoneBusters telephone number at 1-888-495-8501. They too will be able to recognize it, report it and stop it.

Table 7: Prevention, Detection and Assistance for Caretakers - Children

Environment	Prevention	Detection	Assistance
Online	1) Get informed and stay informed on youth related threats. 2) Inform them gradually without insistence, in a non-alarming fashion and provide information sources once interested. 3) Teach them to recognize, avoid and report risky situations. 4) Teach youth the merits of assertively disengaging from risky situations. 5) Open the communication channels, invite the young person to share any questions or concerns about situations they may be experiencing.	Watch for changes: 1) Your child seems overly agitated or excited for no apparent reasons. 2) Your child is evasive to answering questions and can't provide logical explanations. 3) Evidence of unexplained money transfers and money order receipts to obscure places or foreign countries.	Do not forbid your child from using the internet at home. They will find other ways to use it. It is better to have them use it in a safe, controlled and monitored environment.
	Create an awareness of the value of personal information to criminals and the problems it can cause once compromised.	Personal information posted on their social networking profile or their personal website.	Keep track of your child's credit report if too much information was given. Erase the information from the profile or website.
		Their friends' personal information posted on their profile or website.	Have them erase the information and, if need be, notify other parents to keep track of their children's credit reports.
Public	Teach your children about the importance of not sharing their PIN or their passwords.	A bank card could be missing or a friend has the bank card.	They should have the PIN or password changed and again explain why they should not share them.
	Teach your children that they should not carry their SIN card or birth certificate on them.		Contact the proper authorities if the cards are lost or stolen and again remind them of the consequences

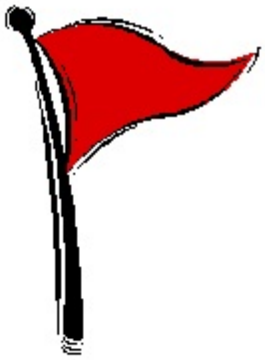
2.3 Travellers

You must remain vigilant for fraud while on holidays or while travelling. If you are travelling to a foreign destination carefully plan your trip by visiting Foreign Affairs and International Trade's travel information website at http://www.voyage.gc.ca. A little prevention goes a long way. Do not forget to pack a copy of their *"Bon Voyage, but ..."* booklet.

Pay special attention to documents containing your personal information. Bring only the necessary documents and carry them with you at all times. Never leave any personal information unattended in a hotel room or any other locations.

3.Red Flags

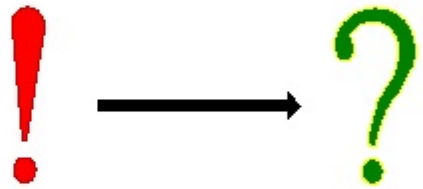
Red Flags



There is no guaranteed method to know that you are being exposed to fraud. Read the following fourteen indicators and apply them to your daily life. Remember, a situation that raises one or several red flags does not automatically make it a fraud. It only means that you should be careful, do your research and ask the right questions. If the provided answers or your research does not lower all flags, just opt out.

Fraud

Identify it.
Report it.
Stop it.



Indicators

1. Who am I really dealing with?
2. Why are they asking for more information than actually needed?
3. Am I getting rushed or pushed into making impulsive decisions?
4. Is this person overly enthusiastic?
5. Is it too good to be true?
6. Anything unusual about this ATM?
7. Is a hidden/cell phone camera or person reading my PIN?
8. Is this job offer legitimate?
9. Is this Web site trustworthy and legitimate?
10. Will this employer/organization protect my personal information?
11. Why are they asking for a processing fee to give me a loan?
12. How did they get my contact information?
13. Am I broadcasting my personal information over the airway?
14. Why does this stranger suddenly want to become my best friend?

4. Scenarios

Phishing:

You receive an e-mail from your bank stating that they have upgraded their safety measures to protect you against identity fraud. They urgently need you to log on to their web site and conveniently provide a link to it. You have been a customer with this bank for a long time, you trust them and you know they want to protect your information. You are concerned. What should you do?

Banks simply do not do this. Your bank already has all your personal information! It does not make sense that they would contact you to get it again, right? Why would they send an e-mail asking for personal information when they are actually working very hard at protecting you against phishing? This e-mail could also pretend to be from a government agency or an online auction company. Use common sense and delete these messages. Do not respond to them. Do not follow any provided links nor telephone numbers.

Disposal of personal computer:

You know you have to protect your personal information. Before selling your old computer, you erased all the folders where you stored your information. Should you feel safe now?

When you delete your information on a computer, it does not actually physically erase it. It simply hides information from the active file system. Unless freed disk space is later overwritten by another new file, the information will still be readable. In fact, it may remain readable for a very long time. Therefore, before disposing of a hard drive, consider these two safe alternatives: 1) re-format the hard drive, re-load the operating system (Windows, MacOS) and "wipe" the free space using specialized software or 2) physically destroy the hard drive.

Payment card skimming:

Brian stops at his local self-serve gas station. While paying with his debit card, he chats with the very friendly clerk. Brian is so involved in the conversation that he does not notice the hidden camera and that his card was swiped a second time through a second smaller device. Should he have been more vigilant to his environment?

Yes. Because two weeks later, Brian's bank statement arrived and while reviewing his statement, he noticed several large transactions that he did not make. Brian could have avoided this from happening, by simply keeping an eye on his card and environment and properly protecting his PIN.

Dumpster diving:

At a large apartment complex, Mike the janitor has found a profitable new hobby. He recycles trash. Paul, a friend of a friend, gives Mike good money for useless junk like pre-approved credit applications. As a matter of fact, Paul will even pay for any garbage that contains personal information. Mike is an honest guy, nothing wrong with selling useless trash, right?

Wrong. Mike may be an honest guy however Paul uses the information and applies and receives several credit cards under the tenants' names. Subsequently, large purchases are made with these cards. As a result, the tenants credit ratings are affected. Careless tenants are now spending a lot of time and money to get their reputations re-established. This could have been avoided by shredding personal information before disposal.

Personal space intrusion:

At the local community pool, swimmers return to the locker room to find out that all padlocks have been cut. Most wallets are missing. The swimmers all agree, they will file a police report and all cards can be replaced.

Don't carry your life in your wallet, keep SIN cards, birth certificates and passports locked in a safe place. If personal information has been compromised , report to the credit bureaus and ask for a fraud alert on your file, report to the police and PhoneBusters/Recol.ca.

Eavesdropping:

While having lunch in the cafeteria, Diane realizes she forgot to check the balance in her account. She picks up her cellular phone and accesses the information.

Diane actually broadcast information about her bank, her account identifier and her PIN over the airways. The same would be true by using a wireless network or a cordless telephone handset. Within the broadcast range of the device, criminals could be monitoring the traffic and capturing the numbers she punched or voice information. Her account could now be at risk. Also be careful of casual voice or visual eavesdropping in a public place.

Shoulder surfing:

At his local pharmacy, Arthur is in line waiting patiently to pay for his medication. When his turn comes, he swipes his debit card and types his PIN while leaving the keypad flat on the counter without protecting his PIN.

Arthur gets attacked in the parking lot by an individual who was also standing in line. He was able to memorize Arthur's PIN and now he has his debit card. Arthur's account is emptied before he even has a chance to finish reporting the incident. Today, Arthur learned his lesson, unfortunately his shoulder was also dislocated.

Telephone:

Right after supper, Beatrice answers her telephone. A man with a nice, soothing voice properly introduces himself as an investment counsellor for a major insurance company. He takes the time to talk and explain various investment options. At first, Beatrice fights the urge to disengage but, gradually, she starts enjoying the conversation. The initial conversation is relatively short and pleasant. At the end of his sales pitch, this individual announced that he will give her some time to think about it and call her back in a few days.

There is nothing wrong with this so far. This could very well be a legitimate sales call. Most importantly, Beatrice should be aware that she could be caught in a process called grooming, where a scammer gradually builds a rapport with his victim in small incremental steps. He will rapidly build trust by calling at regular intervals and increase the victim's comfort level by using a combination of charm and coercion. Beatrice should not let her guard down and should listen to her instincts. She should disengage from these call if she suspects a fraud or simply does not need an investment counsellor.

Fraudulent credit offer:

You found an incredible credit card offer from a major credit establishment in a local mall with almost no obligations and a small interest rate that is well below the competition. You are interested but what should you do?

Contact this credit card company by locating a published telephone number and ask them about this offer. If the offer is fraudulent, provide all details to the credit card company, advise local police and report it electronically at Recol.ca or by telephone to PhoneBusters 1-888-495-8501 or www.phonebusters.com.

Job Offer Scam:

You answer an advertisement for a work-at-home job which entails re-shipping a product from one point to another. Initially you complete an employment application form that requires your date of birth and social insurance number. So now you are hired and you immediately start working from the comfort of your home. You wonder, is this a legitimate job?

Your instincts are most likely right. It has become obvious that you have been tricked into defrauding others. Less obvious is the fact that you have also provided your personal information to criminals. They may decide to use it months or years down the road. You now have enough knowledge to understand that you were unknowingly participating in an offence. Continued participation with this knowledge would make you a party to the offence. Quit this job, follow identity theft prevention tips included in this guide. Make a report electronically at Recol.ca or by telephone to PhoneBusters 1-888-495-8501 or www.phonebusters.com. Also call the local police to report the scam. Home based re-shipping jobs not requiring any experience is another version of a job scam.

Internet wireless access:

You are very busy at work and learn to appreciate the on-the-go connectivity your Wi-Fi laptop offers. New hotspots are popping up all the time and some of them are even free. You are now at the point where you use this for most of your Internet transactions and communications. No problem, right?

There is nothing wrong with using Wi-Fi. Just be aware that using this type of access uses radio frequencies and your data could be intercepted or your favourite hotspot may be hijacked by an Evil Twin site in a van across the street or in a backpack a few tables down. When you have the choice use a regular Internet connection, use password and encrypted session hotspots. Use an invalid password on the first login attempt. Be very suspicious if it lets you connect with an invalid password.

Online auction scam:

You want to sell your car and decide to try the online auction services. You put it up for sale on your favourite online auction. Shortly after, you receive a message from an individual in the US offering you a lot more than it is really worth if you retract your auction. He has a long, complicated story that you don't really care to understand. A final detail, he has a Texas bank cheque for an amount that is approximately US $1,000 more than what he is offering for the car. Since you are Canadian he trusts that he will get his money.

This one sounds too good to be true. And it probably is. This individual is most likely capitalizing on the built-in delay in cheque processing.

Advance fee loan:

While reading the local newspaper, you notice a small loan advertisement practically guaranteeing a loan to anyone whether they have good or bad credit or have any past bankruptcies. Seeing that this is a good opportunity to get a little extra money to be able to take that trip you promised the kids, you decide to call the toll-free number. You receive and fill out forms with your personal information. Within a few days you receive a telephone call telling you that your loan application has been approved and that they need you to electronically transfer money to cover insurance and processing fees before receiving the loan. Should you send the money?

No. First check to see whether this is a valid advertisement from a legitimate Canadian Bank or lender. Legitimate Canadian banks are listed on the Canadian Bankers Association under Schedules I, II or III, please refer to the "Useful Links" appendix at the end of this document. Call the corresponding bank to ask them about their promotion. If the bank is not listed or is not aware of this promotion, report it!

Social Networking Sites:

Your 11 year old daughter has decided to create her first online profile on a popular social networking site. She fills out the information section in great detail to impress her friends. You can find her date of birth, phone number, address, school and sports teams. She adds pictures of the summer family trip, of her soccer team and her class picture. This seems harmless right?

Wrong! Before your children create their first online profile make sure you explain to them that certain personal information should not be posted on their profile. They should be aware of the negative consequences of posting certain information online. They should never post their date of birth, home address and school address. Even pictures can divulge to much information that could be used by a scammer to get more information. Help them create their profile and choose the proper security setting to maximize your child's protection.

Renovation Fraud:

Your door bell rings and you are greeted by a roofing contractor. He informs you that your roof appears to be in disrepair and requires immediate attention. Luckily he has extra supplies from a previous renovation he just completed in your neighbourhood. He offers you a great deal. You have already contemplated getting your roof fixed but have not gotten around to calling a contractor. You decide to accept his offer.

This good offer could turn into a roofing nightmare. These types of offers are most likely fraudulent. Therefore you will probably end up with a poor job done on your roof or a job that is incomplete. Make sure to properly research the contractor and shop around for prices because if it sounds too good to be true, it probably is.

Dating Services:

Greg was contacted online through a dating service by a woman from a foreign country. They started chatting online regularly and exchanging phone calls. After several weeks Greg had complete trust in this woman. She explained that she wanted to meet him in person but needed money for her trip expenses such as food, airline ticket and passport. She will be able to pay him back when she sees him because she has a wealthy uncle that just passed away in Canada, but she cannot access the money unless she comes to Canada. Should Greg send her the money?

No, Greg will most likely lose his money. Be very careful when meeting someone online. Although the other person may sound completely genuine and trustworthy, you do not really know who you are dealing with.

Public Access Computer:

While relaxing by the lake at your favorite campground, you suddenly realize that you did not transfer enough money into your bank account for the monthly payment on your recreational vehicle. Instead of getting dressed and driving into town to the bank, you decide to use the campground public access computer. Can you resume your relaxation session?

No. You may not relax as much in the long run if this computer was modified with a keylogger or is infected with malware. It is preferable to avoid using secure web sites on public access computers. If you do have to, make sure to logoff when finished. Unknown to you, browsers will copy information onto the local hard disk and your information may be visible to other users. Learn how to remove cookies and delete the cache on a computer.

Do not underestimate the importance of your personal information. A stolen identity is the key to your credit history and your money. It may be used for criminal purposes. It takes a lot of work, time and money to fix your credit and to retrieve your money. Remember that it is not always possible to completely fix these problems. Use the tips enumerated in this guide to help prevent becoming an identity fraud victim. The importance of your contribution to the control of personal information and scam protection problem is generally not sufficiently recognized. In your circle of influence, you have the power to educate others. In your daily activities, take a few moments to transmit some of your newly acquired knowledge to your family, friends and colleagues. Specifically, use and encourage better practices when handling money, credit or debit cards in public or online situations. The best way to minimize your risk of being a victim of fraud is to keep you informed of new scams and fraudulent techniques.

Fraud.

Recognize It.
Report It.
Stop It.

Law enforcement needs your support to be able to find the criminals which use this information to their advantage. Report any scam information to:

- www.recol.ca or,
- PhoneBusters also known as the Canadian Anti-Fraud Call Centre at 1-888-495-8501 or at www.phonebusters.com.

Please note, the information that was used to compile this guide was obtained from various organizations that are found in the Useful Links section.

Appendix 1 - Useful Links

Consumer Awareness/Government:	
Consumer Measures Committee - Protect Your Identity	http://cmcweb.ca/epic/internet/incmc-cmc.nsf/en/fe00088e.html
Canadian Consumer Information	http://www.consumerinformation.ca/
Canadian Council of Better Business Bureaus	http://www.ccbbb.ca/
Financial Consumer Agency of Canada	http://www.fcac.gc.ca/eng/consumers/default.asp
British Columbia Government - Personal Information Protection (English only)	http://www.mser.gov.bc.ca/privacyaccess/Privacy/
Ontario Government - Smart consumers are good for business	http://www.gov.on.ca/MGS/en/ConsProt/050451.html
Quebec Government - OPC Jeunesse (French only)	http://www.opc.gouv.qc.ca/jeunesse/accueil/affiche.asp?page=18plus
Counterfeit:	
Bank Note Security Features	http://www.bankofcanada.ca/en/banknotes/counterfeit/security_features.html
Credit Bureaus:	
Equifax Canada	http://www.equifax.ca
Trans-Union Canada	http://www.tuc.ca/
Northern Credit Bureaus	http://www.creditbureau.ca/
Domain Names:	
Canadian Internet Registration Authority	http://www.cira.ca
Internet Assigned Numbers Authority	Country Codes - http://www.iana.org/cctld/cctld-whois.htm Generic Top-Level Domains - http://www.iana.org/gtld/gtld.htm Infrastructure Top-Level Domain - http://www.iana.org/arpa-dom/ Whois Service - http://whois.iana.org/ Regional Internet Registries - http://www.iana.org/ipaddress/ip-addresses.htm
SamSpade.org - Whois	http://www.samspade.org/
Whois Source - Whois	http://www.whois.sc/
Personal Banking Security:	
Canadian Bankers Association Schedule I Banks Schedule II Banks Schedule III Banks	http://www.cba.ca/en/section.asp?fl=3&sl=308&tl=&docid= http://www.cba.ca/en/ViewDocument.asp?fl=2&sl=204&tl=160&docid=354 http://www.cba.ca/en/ViewDocument.asp?fl=2&sl=204&tl=161&docid=350 http://www.cba.ca/en/ViewDocument.asp?fl=2&sl=204&tl=162&docid=353
10 Ways to Protect Your Credit Cards	http://www.cba.ca/en/viewdocument.asp?fl=3&sl=11&tl=129&docid=257&pg=1
Your Money - for students and teachers	http://www.yourmoney.cba.ca/eng/tsamprogram/protecting/index.cfm
RCMP/Deal: How to be Plastic Smart	http://www.deal.org/content/index.php?option=com_content&task=view&id=565&Itemid=32&lang=en
Interac - Protect your PIN	http://www.interac.org/en_n1_50_protectyourpin.html
Phishing:	
The Anti-Phishing Working Group	http://www.antiphishing.org
Public Safety:	
PSEPC - Identity Theft – Questions and Answers	http://www.safecanada.ca/identitytheft_e.asp

Telemarketing:	
Canada Radio-television and Telecommunications Commission	http://www.crtc.gc.ca/eng/INFO_SHT/t1022.htm
Travel:	
Federal Trade Commission - FOR THE CONSUMER	http://www.ftc.gov/travel/
Quizzes:	
Industry Canada - Consumer Connection - Fraud Quiz,	http://strategis.ic.gc.ca/epic/internet/inoca-bc.nsf/en/ca01960e.html
SonicWALL Phishing IQ Test II	http://www.sonicwall.com/phishing/
Reporting Canadian Fraud:	
PhoneBusters	http://www.phonebusters.com
Reporting Economic Crime Online	http://www.recol.ca
Spam/Spyware:	
Industry Canada - Stopping Spam	http://www.stopspamhere.ca/
Anti-Spyware Coalition	http://www.antispywarecoalition.org/index.htm
Terminology/Encyclopedia:	
CERT.ORG - Home Computer Security	http://www.cert.org/homeusers/HomeComputerSecurity/
How Stuff Works	http://www.howstuffworks.com/
Wikipedia	http://wikipedia.org/
Education/Awareness/Assistance:	
Fraud Prevention Forum	http://www.competitionbureau.gc.ca/internet/index.cfm?itemID=122&lg=e
Federal Trade Commission - ID Theft	http://www.consumer.gov/idtheft/
Human Resources Canada - Lost or (SIN) Card	http://www.hrsdc.gc.ca/asp/gateway.asp?hr=en/cs/sin/130.shtml&hs=sxn http://www.hrsdc.gc.ca/asp/gateway.asp?hr=/en/cs/sin/0300/0300_in125.shtml&hs=sxn
Office of the Privacy Commissioner of Canada	SIN - http://www.privcom.gc.ca/fs-fi/02_05_d_02_e.aspIdentity Theft - http://www.privcom.gc.ca/fs-fi/02_05_d_10_e.asp
Service Canada - Lost Wallet	http://www.servicecanada.gc.ca/en/lifeevents/wallet.shtml

Glossary

Browser Cache:
is data that is copied to a computer to optimize the computer performance of the application.

DNS:
DNS is short for Domain Name System. Internet functionality that automatically locates and translates domain names into Internet Protocol addresses.

Domain Name:
A domain name is an easier to remember and meaningful equivalent for a numeric Internet Protocol (IP) address.

Fraud:
Dishonest deprivation of someone's economic interest.

Fraudster:
One who commits fraud.

HTTP Cookies:
are pieces of information that are sent to and from the server. They are used to trace and keep information of the user's online habit. These habits can range from the user's site preference to the frequency of use of a specific site.

Identity Fraud:
RCMP definition: The unauthorized acquisition, possession or trafficking of personal information, or, the unauthorized use of personal information to create a fictitious identity or assume/takeover an existing identity, in order to obtain financial gain, goods or services or conceal criminal activities.

Internet Protocol (IP) address:
Unique number that devices use in order to identify and communicate with each other on a network utilizing the Internet Protocol standard.

Keylogger:
is malware that secretly captures, stores and sends a computer user's key strokes to a different user's computer. With this type of software anything you type can be recorded.

Malicious Code/Malware ("malicious software"):
Program deliberately designed to capture/modify/damage data or change a computer behavior without the user's explicit knowledge or intention. Malware includes Trojan horses, spyware, viruses and worms.

Personal Information:
For the purpose of this document, personal information refers to any element or combination of information that can normally be used to uniquely identify an individual in the delivery of goods and services, government services or law enforcement activities. Alternatively, it can also designate information to be used to acquire additional information on someone.

Pharming:

Variation of a phishing scam. The difference is the lack of an electronic messaging bait. The redirection to the fraudulent website is accomplished by a redirection Trojan horse on the client computer or DNS poisoning.

Phishing:

Pronounced "fishing". It is the use of social engineering in electronic messaging to provoke an immediate impulsive reaction from individuals into visiting fraudulent websites. The ultimate goal is to acquire personal or sensitive information.

PIN - Personal Identification Number:

A security code used to access personal data or accounts.

Protocol:

An industry or international standard that consists of a special set of rules designed to manage communications.

Screen scrapers:

is malware that permits someone else to see what you can see on your screen. This type of software takes a picture of your screen and sends it off to a different computer.

Social Engineering:

The practice of manipulating someone's trust for the purpose of gaining some advantage.

SPAM:

The practice of indiscriminately sending unsolicited, unwanted or inappropriate electronic messages in mass quantities.

Spoofing:

Modification of identification or authentication information to mislead the reader on the true identity of the originator.

URL:

Short form for Uniform Resource Locator. Unique address for a file that is accessible on the Internet.

WEP:

"Wired Equivalent Privacy" is network standard for wireless networks. As its name implies, it is designed to provide privacy / security equivalent to wired networks.

WPA:

"Wi-Fi Protected Access" is a wireless network standard designed to improve over the security provided by the WEP standard.