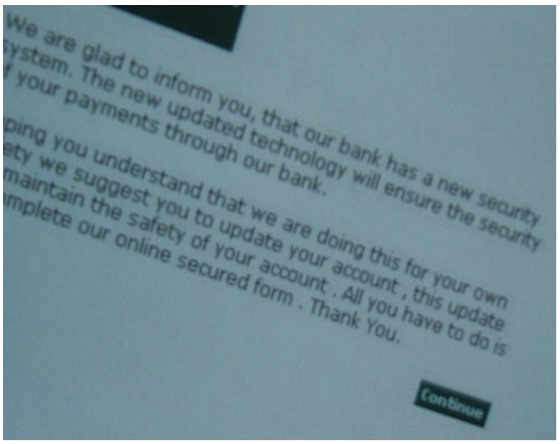
RCMP
ROYAL CANADIAN MOUNTED POLICE

Fraud

Recognize it.
Report it.
Stop it.

Personal Information and Scams Protection

A Student Practical Guide



Royal Canadian Mounted Police | Gendarmerie royale du Canada

Canada

Version 1.2

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

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

March 1, 2006
Ottawa, Ontario

Foreword

Identity fraud, the theft and use of personal information for criminal purposes, is one of the fastest growing crimes in Canada. All Canadians should be aware of the need to protect their personal information and ensure their identity and finances are not compromised.

Nowadays, effective crime prevention requires integration and cooperation between law enforcement and public/private organizations. From these collaborative efforts, practical tools can be created to raise fraud awareness and alert people to some of the more common deceptive practices criminals use to obtain their personal information.

The following guide has been designed by a student for students in partnership with the RCMP Commercial Crime Branch and the University of Ottawa.

Chief Superintendent Wayne Watson
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 citizen/consumer is ultimately responsible for his/her own off/online safety and own education/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 your best interests to do so. This document was designed to provide a holistic approach in learning about Identity Fraud and Scams in general. This document will evolve into newer versions as time goes on. It contains basic knowledge and pertinent tools that any student may use to further his/her 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 or purse** unless you require them for a specific purpose the same day.

According to a telephone poll completed February 2005 by Ipsos-Reid, 9% of Canadian adults have been victims or know someone that have been a victim of Identity Fraud.

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.

1.Online

Online

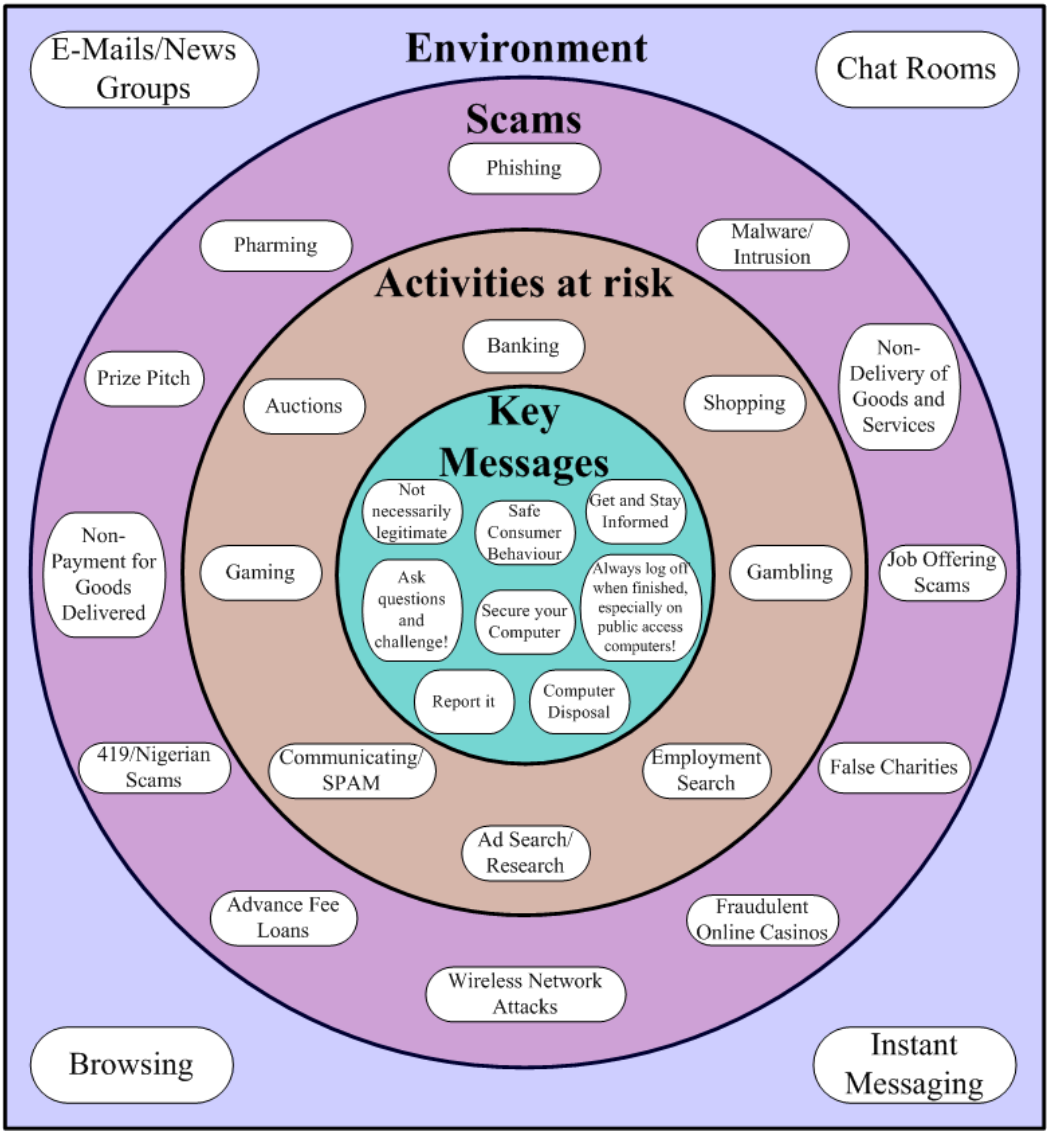


Figure 1: Key Messages to Help Avoid Online Scams Found in Different Environments

Numerous activities can be performed online: shopping, ad searching, researching, auctioning, banking, communicating, employment search 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 terminology, 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 Faked E-Commerce Web Sites

Be cautious of "too-good-to-be-true" offers. Some E-commerce Web sites are set up to capture your personal information. They will operate for a few weeks and then disappear. Companies and people simply do not give out their money, goods or services to complete strangers without obtaining something of at least equal value in return. Successful scams always have rationalizations that potential victims want to believe. The Internet 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.

1.2 Phishing

Spam is the transmission of large quantities of unsolicited electronic messages. Just like Spam, Phishing messages attempt to lure large number of individuals into providing personal information, most often 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 to tell you that you are at risk of being victim of identity theft 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 mean you should me 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
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
Text	not likely to contain incomprehensible text	may contain disguised random text

Table 1.2: Comparison Between a Legitimate and Phishing Site

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 link to some the legitimate site 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 Web site 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 sounds 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 to be read from right to left. Consider the following the domain name in red in the following Web address:

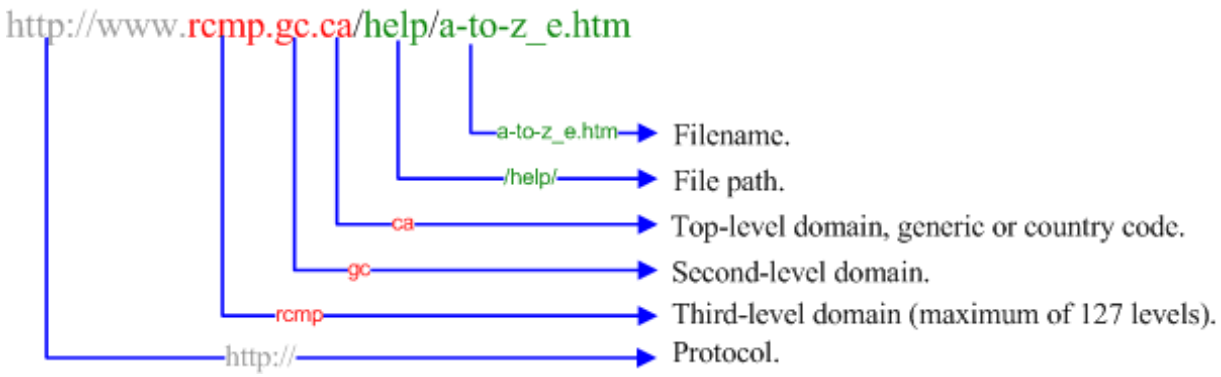


Figure 2: Complete Breakdown of a Web Site Address

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 4). 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 or 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 then 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 Web site 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 Web site'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.

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 direct the user to the requested Web site. 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.

1.4 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, he/she must either pay a series of bogus taxes or fees. Another variation of this scheme is the obligation to purchase a product or service in order to receive the prize. All consumers must 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 a call from someone promising you that they can retrieve 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.

1.5 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 contains information such as proper online payment methods 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.

1.6 Malicious Software (Malware)

A malicious software is designed to introduce 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, by accessing a website, by using infected media or by downloading infected programs such as games. Malicious code may capture personal information from your computer/keyboard and transmit it to another individual.

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. Be aware that malicious code may come disguised as any type of computer file and that a fully protected machine can still contain vulnerabilities.

1.7 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 if you are able to logon with invalid account information.

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 you 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.
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 that 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 in 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.

1.8 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 by 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 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.

1.9 419/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 foreign money transfers in exchange for a percentage of the transfer amount. These letters sent by e-mail, mail or fax transmission and emphasize that trust and honesty are important aspects in this confidential business transaction. The writer will most likely present himself as a Doctor, a major corporate representative usually from the Nigerian National Petroleum Corporation or as someone in the Nigerian or other African national government or military. The same scenarios can also apply to other foreign organizations and countries.

If the victim communicates with the writer by e-mail, mail or phone, he will usually be asked to cover 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.

1.10 Advance Fee Loans

Advance fee loans are commonly advertised in classified adds of newspapers, magazines and tabloids. These ads guarantee a loan regardless of the applicant's credit history, but the victim has to pay an up-front loan fee. Needless to say, the applicant never receives the loan and loses their up-front 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 acceptance, 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 and the financial legitimate institution's security department.

1.11 Job Offer Scams

Be aware of job scams when searching for employment. This includes giving too much information to a possible 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 involves package forwarding, money transfers, wiring funds or well paying telemarketing jobs. You may end up becoming involved in criminal activities. Report suspicious activities.

2. Public, Friends and Acquaintances

Public Settings, Friends and Acquaintances

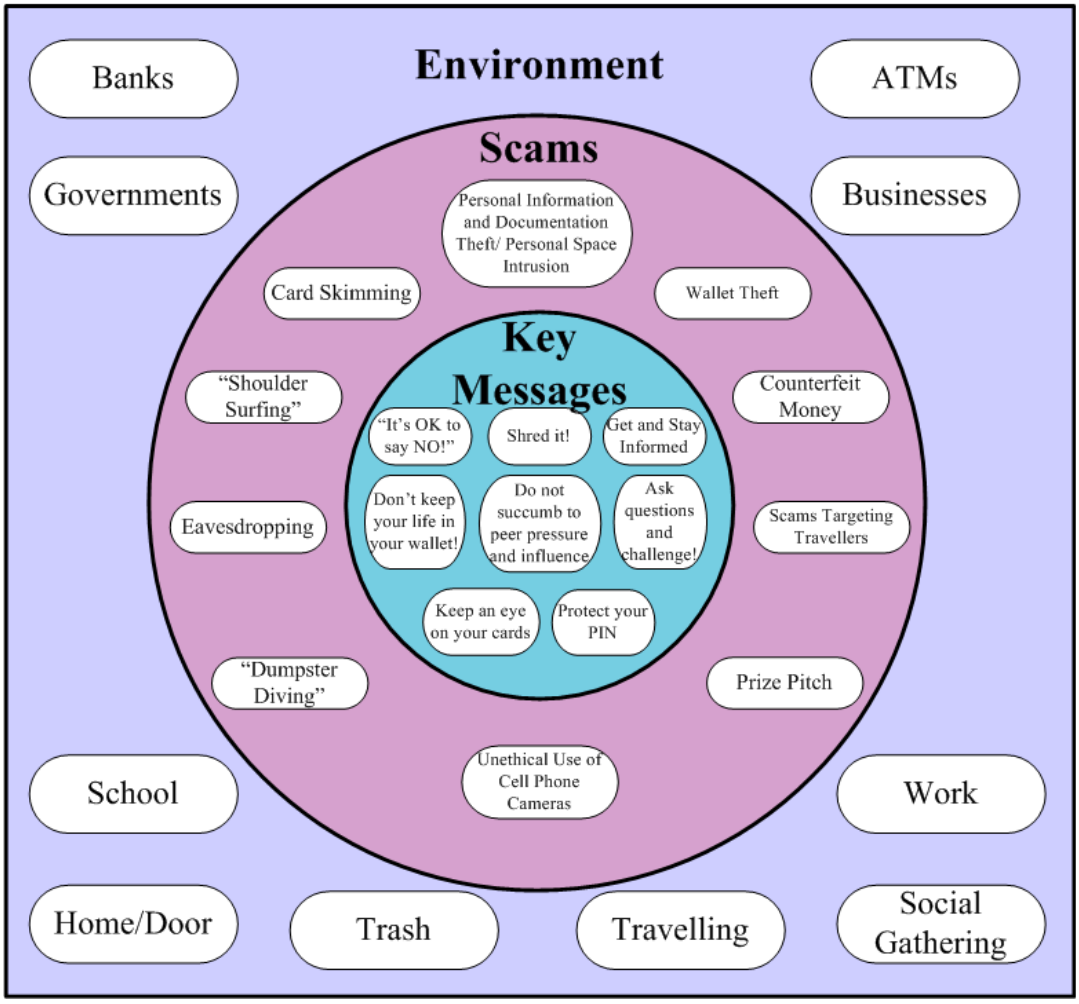


Figure 3: Key Messages to Help Avoid Scams in a Public Setting Found in Different Environments

You lead an active life style constantly alternating between home, school and work. 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, eavesdropping.

2.1 Theft or Loss of Personal Information and Documentation

Do not keep your life in your wallet. An individual should never carry more documents or cards of a personal nature than is needed. Store these documents and cards in a secure place such as a locked drawer, cabinet or safety deposit box. When documentation containing personal and financial information must be thrown away, it is important that you properly dispose of these documents. One of the most common way of proper disposal is shredding.

2.2 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 to verify your bank note you should always feel, tilt and look at and through. To obtain information on how to verify if your 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 as being counterfeit, stop the transaction and request another note. It is your obligation to turn the bank note over to the proper authorities such as local police or a bank teller if received through a ATM machine at the bank. You will not be reimbursed for your counterfeit bank note. But most importantly, you should not try to pass it off to someone knowing it is counterfeit. You could face criminal charges.

2.3 Personal Data Collection

It is important to be cautious when filling out prize entry forms at malls, sport shows and conventions because your personal information maybe later used by third parties to contact you over the phone, sending you spam or by sending you 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.

3. Telephone

Telephone

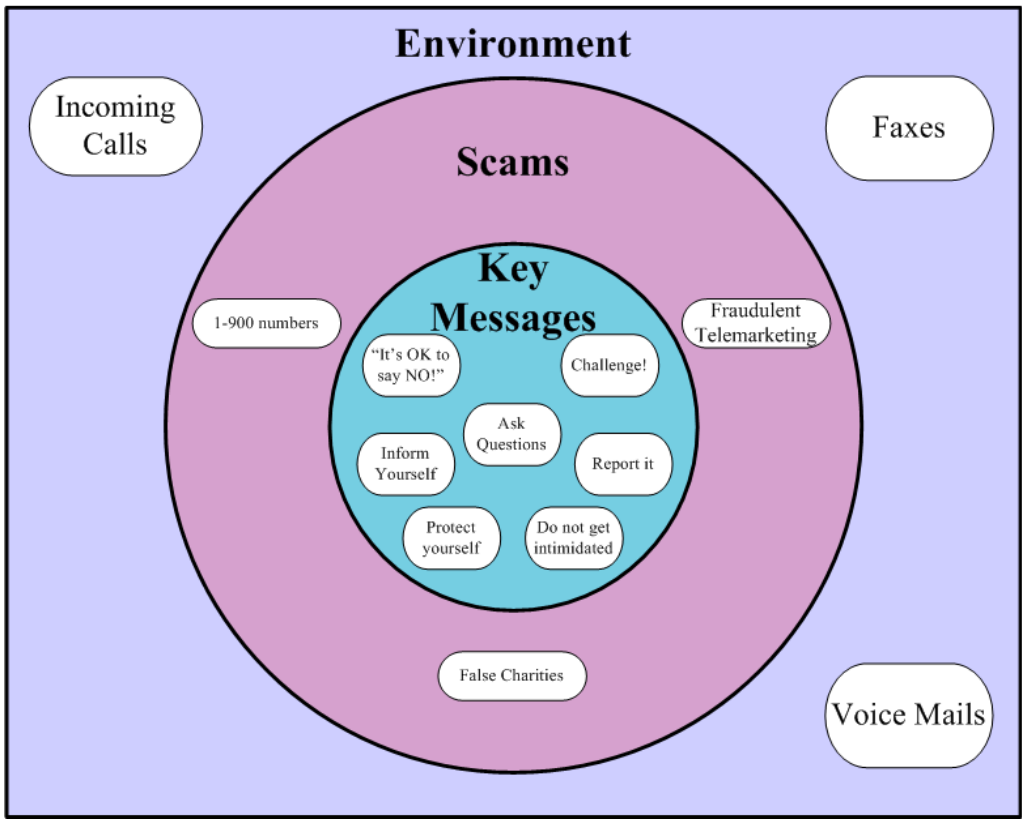


Figure 4: Key Messages to Help Avoid Telephone Scams Found in Different Environments

The most common telephone threats come by fax, voice mail and incoming calls.

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 during an incoming call. Do not be afraid to say no and hang up. If you would like to report any suspicious phone calls, contact PhoneBusters at 1 (888) 495-8501.

Table 3: 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 to 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 willingly 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	Benefits or incentives value are 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 to you
Social Engineering	Could be used as a sales tool	May be used to gain psychological advantage on the victim and to trick them into providing their personal information

3.2 900 Scams

The 900 scams are similar to the prize pitch scams. Consumers will usually receive an offer in the mail enticing the consumer to call a 1-900 number to learn about the type or value of prize they have won. The problem is that usually the call will last several minutes before the caller will find 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.

4. Printed Material

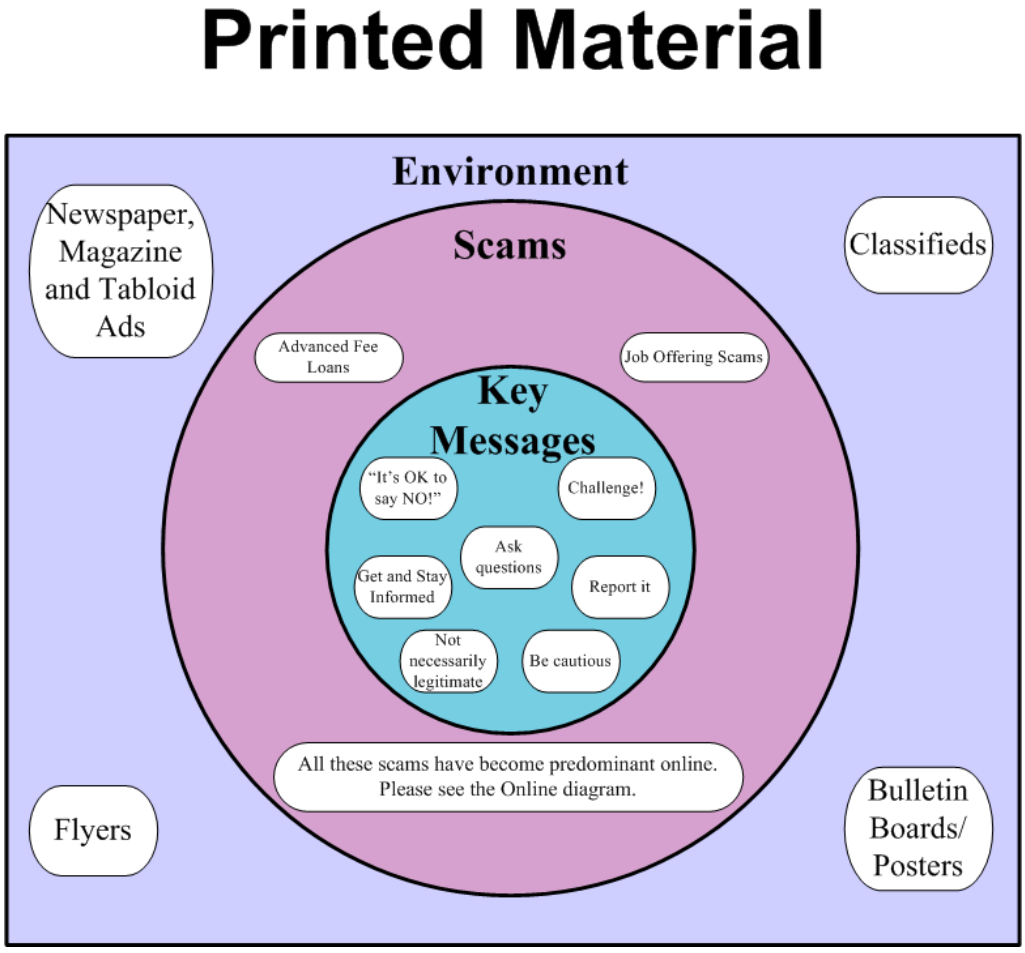


Figure 5: Key Messages to Help Avoid Printed Material Scams Found in Different Environments

Ads for jobs, advance fee loans, sweepstakes, lotteries and valuable merchandise can be found in newspapers, magazines, tabloids, classifieds and flyers or advertised 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 that are published in a local newspaper, a popular magazine or posted on a bulletin board at school, 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 the article to PhoneBusters at 1 (888) 654-9426.

5. Mail

Mail

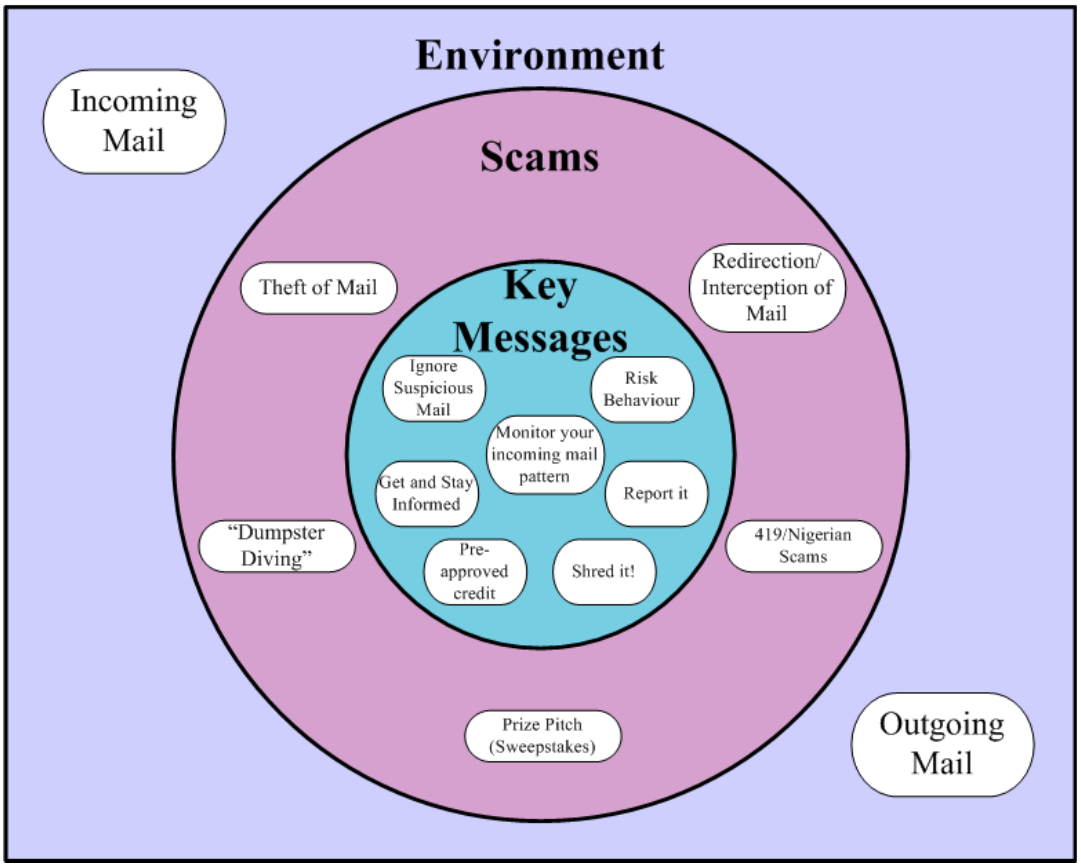


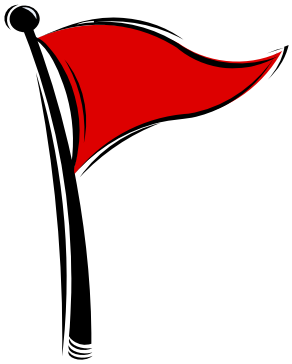
Figure 6: Key Messages to Help Avoid Mail Scams Found in Different Environments

It is mostly likely that you have previously received mail advertising prizes, vacations and services. A major part of these solicitations may not be legitimate. They are variations or copies of scams equivalent to the advance fee loan, the prize pitch, the West African scam and the false charity. 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.

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 insuring 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.

6.Red Flags

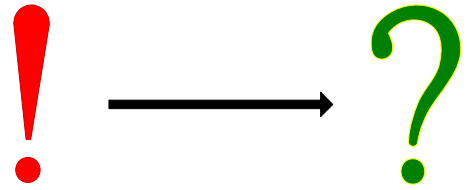
Red Flags



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 he/she is 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?

7. Scenarios

Phishing: You received a e-mail from your bank stating that they have upgraded their safety measures to protect you against identity theft. They urgently need you to log on to their 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 for a government agency or an online auction company. Use common sense, delete these messages, don't respond to them, don't follow any provide links or telephone numbers.

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

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. And it may remain readable for a very long time. Before disposing of a hard drive, consider the two safe alternatives: 1) re-format the hard drive, re-load the operating system (Windows, MacOS) and "wipe" the free space using specialized software. 2) Physically destroy the hard drive.

Credit card skimming: Brian stops at his local self serve gas station. While paying with his debit card, he chats with the very friendly clerk. He is so involved in the conversation that he does not notice the hidden camera and that his card disappeared a moment below the counter.

The next day, his bank account is empty and his credit margin is full. Keep an eye on your card, protect your PIN and don't allow anyone distract you.

Dumpster diving: In this large apartment complex, Mike the janitor has found a profitable new hobby. He recycles trash. Paul, a friend of a friend, gives him 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?

Tenants will likely start receiving notices of credit applications or phone and credit card bills under their name. Some could have their bank accounts emptied. Others could be arrested after boarding international flights and spend needless hours in detention. Careless tenants are risking a lot of time and money to get their reputation re-established. Shred your personal information before disposal.

Personal space intrusion: After a fierce water polo match at the university pool, players return to the locker room to find out that all padlocks have been cut. Most wallets are missing. The players 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 under lock 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: You are in a rush to get cash and get to the nearest ATM that happens to be located in an odd place. After you have typed your PIN the machine indicates to you that it can't process any transaction because the network is down. All you need to worry about is to locate another machine, right?

Be aware that real ATMs can be purchased by criminals and setup for the purpose of capturing your card information and PIN. It is best to use ATMs that are located in banks and reputable businesses locations.

Telephone: Ben receives a telephone call from Bob Smith from the SuperCheap local furniture store where most students buy their furniture. Mr Smith advises that the couch he purchased with his VISA card is on back order. Ben advises that he never ordered that couch and he will not pay for it. The employees apologizes and ask Ben for his card number for credit processing. Should Ben provide this information?

Certainly not over the telephone without validating the identity of that person. Go to the store and ask to see the paperwork. You can call the store using the number published in telephone book. Call the card issuer if it is not possible. Don't get tricked!

Fraudulent credit offer: You found an incredible credit card offer from a major credit establishment in the lobby of your residence with almost no obligations and an interest rate that is well below the competition. You are interested but what should you do?

Contact this credit card company with 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 to Recol.ca or by telephone at PhoneBusters 1(888) 495-8501.

Job offering scam: You find a well paying telemarketing / phone sales part-time job on your campus bulletin board. No experience is required. You call them, are interviewed and get the job the same day. You start working along with ten other people your age. Within a few days your boss starts to pressure you to make more sales but you are growing uncomfortable about the sale of those "credit repair kits". You overheard co-workers trying to convince themselves that it is OK to lie to close a sale. No real harm done, right?

Your instincts are most likely right. It has become obvious that you have been tricked into defrauding others. Less obvious is the fact is 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 offense. Continued participation with this knowledge would make a party to the offense. Quit this job, follow identity theft prevention tips included in this guide and report it electronically to Recol.ca or by telephone at PhoneBusters 1(888) 495-8501. Also call the local police to report the scam. Another version of job scam are home based re-shipping schemes not requiring any experience.

Internet wireless access: You are a busy student and just love 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 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/encrypted sessions hotspots and use an invalid password on the first login attempt. Be suspicious if it lets you connect with an invalid password.

Publicly accessible computers: You can't afford your own laptop and have to rely on your desktop computer at home for your online activities. So you make the most of publicly accessible computers at your school, the public library to stay connected. This should be OK, right?

Just be aware that publicly accessible computers may have had keyloggers installed or could be compromised by spyware.

Online auction scam: You need money for school and can't afford anymore to run your old car. You know decide to 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 that it is really worth if you retract your auction. He has a long a 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 a US $1,000 more than what he is offering for the car. Since you are Canadian he trust that he will get his money.

This one sounds too good to be true. And it probably isn't. This individual is most likely capitalizing on the built-in delay in cheques processing.

Advance fee loan: While reading the local newspaper, you notice a small loan advertisement practically guaranteeing a loan to anyone whether you have good or bad credit or have any past bankruptcies. Like most students, you are short of money this month and 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 fee before receiving the loan. Should you send the money?

No. First check if this is a valid advertisement from a valid Canadian Bank. Valid 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!

Do not underestimate the importance of your personal information. A stolen identity is the key to your credit history and your money. It may as well 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, better practices when handling money, credit or debit cards in public situations or better online safety practices. The best way to minimize your risks of being a fraud victim is by getting informed on the new scams and fraudulent techniques and staying informed.

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 at 1 (888) 495-8501 or at www.phonebusters.com.

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.canadiancouncilbbb.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.cbs.gov.on.ca/mcbs/english/consumer_info.htm
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

Quizs:	
Industry Canada - Consumer Connection - Fraud Quiz,	http://strategis.ic.gc.ca/epic/internet/inoca-bc.nsf/en/ca01960e.html
MailFrontier Phishing IQ Test II	http://survey.mailfrontier.com/survey/quiztest.html
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/home_computer_security.pdf
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
US 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.asp Identity Theft - http://www.privcom.gc.ca/fs-fi/02_05_d_10_e.asp
Service Canada - Lost Identification Cards	http://servicecanada.gc.ca/en/idcards/idcards.html#ide

Glossary

DNS:

DNS is short for Domain Name System. Internet functionality that automatically locate and translate 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 the Fraud.

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.

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 Web site is accomplished by a redirection trojan horse on the client computer or DNS poisoning.

Phishing:

Pronounce "fishing". It is the use of social engineering in electronic messaging to provoke an immediate impulsive reaction from individuals into visiting fraudulent Web sites. 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 consist of a special set of rules designed to manage communications.

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.