MEMBER AWARENESS

Defend Yourself From Fraud

Table of Contents

Awareness is Security

The confidentiality and security of your personal information should be one of your top priorities. Identity theft is one of the fastest growing crimes in North America, and scams by telephone, mail, and online, continue to be a serious international problem. It is important to protect yourself by always being aware and learning how to recognize these dangers.

Gather as much information as possible and learn how to protect yourself from various types of scams that are prevalent today. Awareness is security, so familiarize yourself with the valuable tips and information included within this booklet.

Talk to your credit union if you have any concerns about the safety and privacy of your personal information. They will be happy to answer your questions.

Fraud: Recognize It. Report It. Stop It.

The Face of Fraud: It's not who you think

Believe it or not, there is no typical fraud victim in Canada. It can happen to anyone.

The risk of becoming a fraud victim is not linked to your age, race, income or geographic location. Scammers don't care about any of that — they just want your money.

These are professional criminals. They know what they're doing and, unfortunately for their victims, they do it well.

2Good2BeTrue?

Thousands of Canadians are defrauded each year involving scams that are too good to be true. Scam artists are up to date and well organized. They use the latest trends and sophisticated techniques:

- Professional marketing materials.
- Well-crafted and researched telephone scripts and email messages which are traded among criminals.
- Putting you at ease with their friendly tone and "generous" offers.
- Having believable answers ready for your tough questions.
- Impersonating legitimate businesses, charities and causes.
- Offers that involve sending money via wire transfers.

- Expertly using your own emotions to persuade you.
- Offering pricing of a product that is much less than the price for the same product on the market.
- Offering you a large payment or reward in exchange for allowing the use of your financial account — often to deposit cheques or transfer money.
- Overpaying for your goods or services with instructions to wire excess funds back to fraudster…the original cheque gets returned as counterfeit leaving you responsible for the whole amount.

Common Scam Scenarios

Job and employment scams

The Pitch: An employment advertisement offers a work-at-home opportunity, a fee for "Mystery Shopping", a multi-level marketing plan or other means to "be your own boss" and earn significantly higher income. Beware also of Internet job sites. Some of the job postings are made by organized crime and are meant only to set up phone interviews with individuals to gather personal information.

The Facts: Sending fees for job information or to be listed for jobs in Canada or abroad is risky. In many cases, scammers advertise all kinds of job opportunities from envelope stuffing to filling out forms, or covert testing of wire transfer services under the guise of Mystery Shopping. The common theme in these scams is that they make promises they don't keep. This can result in financial loss or the compromise of important personal info. For a phone interview, if the interviewer asks too many personal questions you should be suspicious. A prospective employer does not need to know your social insurance number (SIN) or your driver's licence number. Beware of odd questions that reveal too much personal information that could later be used to assume your identity. Never include your SIN on your resume.

Medical and health scams

The Pitch: Medical scams prey on human suffering and offer solutions where none exist, or promise to simplify complex health treatments. **Miracle cure scams** may offer a range of products or services that can appear to be legitimate alternative medicines, and often promise quick and effective remedies for serious medical conditions. The treatments claim to be effective against a wide range of

ailments and are often promoted using testimonials from people who have used the product or service and have been "cured." Also watch out for **weight loss scams** that promise dramatic weight loss with little or no effort (for example, "while you sleep") and often require large advance payments or ask you to enter into a long-term contract to participate in the program. Beware of spam emails or online ads for **fake online pharmacies** that offer drugs and medicine at very cheap prices and/or without the need for a prescription from a doctor.

The Facts: Legitimate online pharmacies will require a valid prescription before they send out any medicine that requires one. Remember, there are no magic pills or miracle cures for serious medical conditions, or rapid weight loss with no effort. Don't trust an unsubstantiated claim about medicines, supplements or other treatments. They may not work and you will waste your money, and in the worst case scenario, they may actually harm your health. It's best to consult your doctor or a licensed healthcare professional. You can also research published medical and research papers online or in your library to verify the accuracy of the claims made by the promoters. Never commit to anything under pressure.

Is your credit really protected?

The Pitch: They say, "We'll protect you from scammers who could run up huge debts on your credit cards without you knowing. Just send us your card numbers and we'll protect you for a nominal fee."

The Facts: Offers of credit protection or "insurance" against fraud are just attempts to get your credit card numbers and your money. Call your credit card companies or your credit union first. If someone fraudulently uses your cards, most companies hold you responsible only for the first $50, and many waive all losses.

Emergency scam

The Pitch: In the Emergency Scam scenarios (also called the "grandparent scam"), a grandparent receives a phone call from a fraudster claiming to be one of his or her grandchildren, frantically asking for money to bail them out of an emergency situation.

The caller says that he/she is in some kind of trouble — a car accident, trouble returning from another country or in need of bail money to get them out of a jail — and that he or she needs money immediately. The calls often come in at night and could include other people who impersonate

lawyers, police officers or other authorities to create a sense of urgency.

Victims of the emergency scam don't verify the story until after the money has been sent because the caller specifically asks that they do not want other relatives to know what has happened by asking "Can you please help me? I'm in jail (or in the hospital, or in some type of financial need). But don't tell Dad. He would kill me if he found out, please send the money ASAP. I'm scared." Wanting to help their grandchild, the victim sends money by a money transfer company.

The Facts: Be suspicious and make sure to verify any emergency situation before sending any funds. Even if the situation seems urgent, take the time to review it by contacting a family member or a friend. Don't feel bad about verifying the claim. Thanks to the Internet, it's easier to find personal information such as phone numbers, family names, and more, in order to carry out this scam.

This scam is typically directed towards the grandparents, though keep in mind that other variations on the scam also exist, such as an old neighbour or a family friend.

Money transfer request scam

The Pitch: Also called the "West African Scam," or the "Advance Fee Fraud." A person will receive a call, letter or email stating that someone has money stuck in a foreign country and they are looking for outside assistance to get their money out. The person will be offered a large portion of the money if they help. This person will then be told that they just need to provide their financial account information so that the money can be transferred to it. They will be given an address to send a cheque or wire the money to cover the costs of getting through the red tape for the release of funds. If the person provides the requested funds they might eventually be asked for more and more money to assist in getting the funds released. They could also find their account has been attacked and their money has been transferred out. Sometimes a cheque is sent to a person and they are requested to cash it, keep their portion and wire the rest back to the sender or a third party. In all cases the cheque they receive will be a counterfeit cheque and they will lose the funds they wired to the criminal sender. Letters or email messages for these types of scams can be badly written and have many spelling mistakes. However, they may also be very sophisticated.

The Facts: Be skeptical of individuals representing themselves as foreign business people or foreign government officials asking for your help in placing large sums of money in overseas bank accounts. Do not believe the promise of large sums of money for your co-operation. Guard your account and personal information carefully.

Charity scams

The Pitch: Beware of scammers collecting money for a fake charity or by impersonating a real charity. Scammers can approach you anywhere, including at your doorstep or via email, and play on your emotions by pretending to be from charities that help children who are ill or victims of a recent natural disaster. Fraudsters can try to pressure you to give a donation and refuse to provide details about the charity, such as their address or their contact details. In other cases, they may simply provide false information.

The Facts: Not only do these scams cost you money — they also divert much needed donations away from legitimate charities and causes. All registered charities in Canada are overseen by the Canada Revenue Agency and are listed in its database, so check it to make sure that the charity that has approached you is genuine. If the charity is genuine and you want to make a donation, get the charity's contact details from the phone book or a trusted website. If you have any doubts at all about the person asking for money, do not give them any cash, credit card or bank account details or any other personal information. If in doubt, approach an aid organization directly to make a donation or offer support.

Dating and romance scams

The Pitch: There are many legitimate dating websites operating in Canada — but unfortunately, there are just as many dating and romance scams as well. In some cases, scammers set up a bogus dating website where you pay for each email or message you send and receive. They try to hook you in by continuing to send vague-sounding emails filled with talk of love or desire, to keep you writing back and paying for use of the scammer's dating website. Even on a legitimate dating site, you might be approached by a scammer — for example someone who claims to have a very sick family member or who is in the depths of despair, and is often from abroad. After building a friendship with you, they may ask you to send them money to help their situation. Some scammers even arrange to meet with you, in the hope that you give them presents or money — and then they disappear.

The Facts: Make sure you only use legitimate and reputable dating websites. Scammers often set up fake websites with very similar addresses to legitimate dating websites, so remember to check the web addresses carefully. Never send money, or give credit card or online account details to anyone you met online. Protect yourself by not giving out any personal information in an email, text message, or when you are chatting online.

Pre-qualified never means pre-pay

The Pitch: You're told you've been "pre-qualified" for a low-interest loan or credit card, or to repair your bad credit even though financial institutions turn you down. They ask for your social insurance, driver's licence and financial account numbers — and a processing fee of several hundred dollars.

The Facts: Beware of advertisements or phone calls offering credit, especially if you have been turned down by financial institutions. Legitimate lenders never "guarantee" a card or loan before you apply. A legitimate pre-qualified offer means you've been selected to apply — you must still complete an application and you can still be turned down. Verify the business you are dealing with.

Small business scams

The Pitch: An invoice says an urgent delivery of photo-copier or office supplies is awaiting confirmation of your business address. It appears that someone in your office ordered services or supplies but the bill hasn't been paid.

The Facts: Scam operators trick many businesses into paying for goods and services they haven't ordered. They bet that many small business owners and their staff are just too busy to check that every invoice is legitimate. Carefully examine all invoices, even those under $50.

Don't fall for a winning prize scam

The Pitch: A caller (or email, text message, or pop-up screen on your computer) says you won a big lottery prize. You must act now and send money to cover taxes or handling or make a purchase before you can collect your prize. Some lottery scams may also try to trick you into providing your banking and personal details to claim your prize.

The Facts: This is one of the most common scams — if you send money you will never get it back. Legitimate lottery and sweepstakes administrators never charge fees or taxes to deliver your prize. Never send money to anybody you don't know and trust.

It's a rip-off! Here's the tip-off:

- The caller is more excited than you are.
- The caller demands an immediate answer but refuses to send you anything in writing.
- You must pay fees or buy a product before you can collect your prize or obtain credit.
- You are asked for credit card or financial account numbers, or copies of personal documents.
- You can only send payment by wire service or by courier.
- You receive an unexpectedly large cheque.
- Your business is invoiced for supplies or directory listings you did not order.

Fraud: Recognize It. Report It. Stop It.

Protect yourself!

Crooks can do bad things with your good name. Protect your precious personal information. Ask all marketing, research or charity callers for:

- Detailed, written information that you can check yourself.
- Time to think about the offer. Scam artists pressure you for an answer, saying the offer will expire or go to the next person if you don't act now.
- Valid references and the means to contact them.
- A call-back number. But beware — a crook can give you a number where a colleague is standing by to finish taking your money. Instead, you may want to hang up and verify the call's legitimacy using an independent source such as Canada 411, the phone book or the service provider's website.

You should also remember to shred unwanted personal documents such as transaction records, credit applications, insurance forms, cheques, financial statements and tax returns.

If a scam artist contacts you or if you've been defrauded, call the Canadian Anti-Fraud Centre at 1-888-495-8501.

The Canadian Anti-Fraud Centre will gather evidence and alert law enforcement in Canada and abroad. By reporting, you can prevent others from becoming victims and help put an end to fraud.

Identity Theft and Protection

Imagine this…

Unexpectedly, you get turned down for a loan, you get a call from a collection agency about an account you never opened, or worse yet, a call from the police about a crime you didn't commit. Suddenly, you're a victim of identity theft.

Identity theft — a fast-growing crime

Identity theft is one of the fastest growing crimes in North America. It happens when someone steals your personal information, such as your SIN, driver's licence number, date of birth, health card number, credit card or debit card number, online passwords, or your Personal Identification Number (PIN).

Criminals get this information by stealing your cards, posing as an employer, credit union or utility company employee, grabbing information from websites that are not secure, compromising email accounts, sorting through garbage, or using devious ways to find out your PIN. It can happen to anyone. In the course of a busy day people use an Automated Teller Machine (ATM) to get money for groceries; charge tickets to a hockey game by phone; mail their tax returns; call home on their cell phones; or apply for a new credit card online. We don't give these everyday transactions a second thought. But someone else does — someone who is interested in using these everyday transactions to steal your personal information and use it to commit fraud or theft.

Once they have a few pieces of your information, criminals can open a new credit card account or financial account in your name. And the worst thing is, you won't know about it until it's too late.

How identity thieves get your personal information

- They steal wallets and purses containing your identification, credit and debit cards.
- They steal your mail, including your debit and credit card statements, pre-approved credit offers, telephone calling cards and tax information.
- They complete a 'change of address' form to divert your mail to another location.
- They rummage through your garbage or the garbage of businesses for personal data.
- They fraudulently obtain your credit report by posing as a landlord, employer or someone else who may have a legitimate or legal right to the information.
- They get your business or personnel records at work.
- They find personal information in your home.
- They use personal information you share on the Internet.
- They buy your personal information from 'inside' sources — e.g. a dishonest store employee.
- They hack your email.
- They infect your computer with malware.

How identity thieves use your personal information

- They attempt to take over your financial accounts through impersonation.
- They open a new credit card account using your name, date of birth and SIN. When they use the credit card and don't pay the bills, the delinquent account is reported on your credit report.
- They establish phone or Internet service in your name.
- They buy cars by taking out car loans in your name.
- They mortgage your home.

Your credit union takes steps to protect you

Credit unions actively work to detect and investigate any irregular activity in your accounts. Your credit union debit and credit cards contain only the minimum amount of information necessary to make a transaction. As soon as you enter your PIN at an ATM or point-of-sale machine, it is automatically scrambled before it's sent on the network and the transaction begins.

If you lose your debit card or credit card, or you suspect someone has fraudulently created a duplicate card and is using it to take money from your account or run up your credit card, let your credit union know immediately.

Refer to your cardholder agreement for further details on liability.

There are important steps you can and should take to protect your identity and secure your personal information. Steps like managing your personal information wisely and cautiously, and taking steps to minimize your own risk.

Take steps to protect your personal identity

- If you have several debit and credit cards, carry only those that you need. Leave the others at home in a safe place.
- Sign your new cards immediately.
- Don't write your PIN on anything — memorize it.
- Don't carry your social insurance card or birth certificate with you. Keep them in a secure, safe place.
- Don't attach or write your social insurance number on anything you are going to discard, such as transaction records or scraps of paper.
- Check your receipts to make sure they belong to you and not someone else.
- Don't disclose personal information or account numbers to anyone unless you initiated the contact. Use an independent source such as Canada 411, the phone book, or the service provider's website to obtain the contact number. You should also ask how the information will be used and whether it will be shared with anyone else. Ask if you have a choice about providing personal identifying information and, if you can, choose to keep it confidential.
- Frequently check your credit report so you're aware of any changes or unusual activity. Basic credit information can be obtained once a year at no charge from Equifax Canada at **equifax.ca** or **1-800-465-7166**, and TransUnion at **transunion.ca** or **1-800-663-9980**.

- For additional security, or in the event that your house is broken into and you have reason to believe that confidential financial information may have been compromised, consider putting a fraud alert on your credit file with the two major credit bureaus listed on the previous page.
- Pay attention to your billing cycles. Follow up with creditors if your bills don't arrive on time. A missing credit card bill could mean an identity thief has taken over your credit card account and changed your billing address to cover their tracks.
- Guard your mail from theft. Promptly remove your mail from the mail box. Notify Canada Post to hold your mail if you're going to be away for some time and ensure that your mail is forwarded or re-routed if you move or change your mailing address.
- Protect your computer with a good firewall and anti-virus software. Take advantage of technologies that enhance security and privacy when using the Internet, such as using digital signatures, data encryption, and different ways of making the information anonymous.
- Avoid posting personal information on publicly accessible websites and online bulletin boards.
- Give your SIN only when it's absolutely necessary. Don't include your SIN and other sensitive personal information in resumes.
- When you register for websites, use strong passwords and avoid words that are easy to guess. Don't use the same password for different sites and don't store your password on your computer.
- Be wary of online offers from websites you don't know and trust.
- An identity thief will pick through your garbage or recycling bins. Be sure to shred any document that contains your debit card or credit card number, receipts, outdated bills, tax documents, copies of credit applications, insurance forms, physician statements, credit offers you get in the mail, or any other sensitive information.

Take action immediately if you suspect identity theft

- Call your credit union immediately if you suspect you have been a victim of identity theft or if there is unusual activity in any of your accounts. We can provide advice on what to do with your credit card accounts, financial accounts and investments with your credit union.
- Call the police and file a report. Ask for a copy of the police report.
- Contact each credit grantor who has opened a fraudulent account and tell them you did not open that account. Have them close these accounts right away.
- Change your PIN immediately. If you open new accounts, make sure you put new passwords on the accounts.
- Contact Canada Post if someone is diverting your mail.
- Document all the contacts you make along with dates, phone numbers, names of persons you spoke with, and exactly what they said.

Your security is important!

At your credit union, we're working with you to protect your identity. By taking steps to carefully guard your PIN, safeguard your debit and credit cards, and by being aware of any unusual signs, you can minimize your risks.

Online Transactions Protection

Are you secure?

To protect your financial and personal information while online, your credit union's Internet transaction application uses a variety of security measures to maintain your privacy and security. For example, while you are performing online financial transactions, your data is encrypted or scrambled to ensure that your information cannot be read or modified while it is being transmitted.

You are the key to your financial transactions security

Even with your credit union's online security measures in place, it's important to remember that YOU need to take steps to keep your computer secure. There are ways to control access to the valuable information that you maintain on your computer or input to access a secure site.

Don't be the weak link

Internet fraud continues to be on the rise. Not only your home computer but any computer can become infected with malware (malicious software), such as spyware, key loggers, trojans or viruses that attempt to collect your online transactions location and login information prior to entering the secure environment that your credit union provides. With today's powerful online transaction systems, someone pretending to be you may be able to:

- transfer funds to another person or entity
- apply for loans that you are not aware of
- set up automatic credit card payments for cards that are not yours

Regardless of the operating system you have on your computer, you need to be concerned about computer security. Some things to keep in mind:

- Do not use software components (especially operating systems) for which the vendor has ceased to provide security updates. An example would be Windows 95®*.
- Make sure you apply all recommended security updates in a timely manner to critical software components on every computer that you use. In a Windows®* environment, this would include, but not be limited to, Microsoft®* (Windows, Office and others), Apple®* (QuickTime®* etc.), Sun®* (Java®*), and Adobe®* (Acrobat®*, Flash®*).
- Subscribe to security newsletters from software vendors like Microsoft which will keep you informed about updates and issues.
- Uninstall software you don't use and do not download anything if it comes from a program you did not install or do not recognize.
- Do not be tricked into clicking **Agree, OK** or **I accept** in any banner ad, unexpected pop-up window, warning or offer to protect your computer or remove viruses. Press Ctrl + F4 to close this window. If it remains open, press Alt + F4 to close the browser, then close all tabs without saving them.
- Be cautious using flash drives and only open files you are expecting. For added security, hold down the Shift key when inserting the flash drive. This will block malware. If a pop-up window appears use Ctrl + Alt + F4.
- Use care in opening links or attachments in any email, instant message or on social networks.

For more information about protecting your computer, visit: Microsoft.com/security/pypc.aspx.

Invest in peace of mind

Reputable retailers sell a variety of software and hardware solutions to make your computer more secure. Here are a few recommendations to enhance the security of any computer that is connected to the Internet:

Firewall

Considered the first line of defense for protecting private information, a firewall helps prevent unauthorized access to or from your home or office network. Although some computers come with a standard operating system firewall, it should not be considered sufficient to keep out intruders. An additional firewall, that will detect new forms of attacks or attempted intrusions, should be installed and upgraded regularly. Firewalls can be implemented in both hardware and software, or a combination of both. Never turn off your firewall.

Anti-virus program

Computer viruses are pieces of destructive computer codes that are easily spread from computer to computer without the user's knowledge. In some cases they are used to collect and transmit personal information, such as passwords and online transaction locations, to a third party. Other viruses are intended to harm the computer they infect and make it unusable. Virus protection programs or anti-virus software is now a must for computer users because the number and the destructiveness of new computer viruses is increasing exponentially. To ensure you are protected from new viruses, ensure your anti-virus is enabled and configured to run daily updates and regular virus scans to detect if your computer has become infected with a virus. With a good quality program, updates are available online through the software provider's website and in many cases can be set to automatically update as new releases become available.

Anti-spyware program

Spyware will not harm your computer as a virus might. It is programming that is usually picked up through accessing websites, or phishing or spam attachments, and downloaded on to your computer without your knowledge or consent. Spyware secretly gathers information about you and relays it to advertisers or others who want to know more about you and your online habits. Criminals are using this technology to install keyloggers or screen capture programs that allow them to collect personal information and passwords to secure sites and the sites' URL locations which is a breach of your personal privacy. Because spyware is becoming increasingly powerful and difficult

to remove, specialized anti-spyware programs should now be considered as important as anti-virus technology. To ensure you are protected from new spyware, make sure your anti-spyware program is enabled and configured to run daily updates and regular spyware scans to detect if your computer has become infected. Good quality products have an automatic or requested update feature where updates are available online through the software provider's website.

Other security suggestions

Here are some additional things you can do to protect your personal and financial information while online:

- Use a multi-character, alphanumeric password — one that is difficult to guess. Generally, longer passwords provide greater security.
- Change your passwords frequently and regularly.
- Do not use software that 'memorizes' passwords unless the product keeps them in an encrypted form and displays them only in a masked form on the screen.
- Keep your passwords and PIN safe and never share them.
- Do not use the same password for different applications such as social networking sites, email, or online banking.
- Install new security patches as soon as your operating system and Internet browser manufacturers make them available.
- Pay attention to the look of the website you're using for online transactions. If it changes, check the URL carefully to ensure that you have not been hijacked to a bogus site.
- Never leave your computer while it is logged on to a password protected site that can perform online transactions. Follow the instructions provided to properly exit online secure sites and then clear your cache.
- Always exit Internet banking using the "log out" button, and close your browser if you step away from your computer. Your browser may retain information you entered in the login screen and elsewhere until you exit the browser.
- If you do have to send personal or confidential information via email, send it in an attachment (Word or Excel file, for example) that is secured via a strong password and an industrial-strength encryption technique. The password should not be provided to the recipient via email but instead via a more secure medium such as the phone.

- All attachments or website links that are sent in an unsolicited email message should be considered suspect and not opened.
- Do not conduct online financial transactions where you can be observed or at Internet cafés or libraries where a previous user may have accessed a site that downloaded a keylogger.
- Always confirm that you are accessing online transactions through the correct credit union website address.
- Disable file sharing in Windows®* products.
- Do not follow links provided in an email form, that appears to be from your credit union or any other financial institution, that request you to provide personal information. If you are unsure, call your financial institution through a known number, other than one that may appear in the content of the email, to verify if the message was sent from them.
- The easiest way to tell if an email is fraudulent is to bear in mind that your credit union or another financial institution will never ask you for your personal information, passwords, PIN, or login information in an email.
- Social networking sites are the first place criminals look for information about you, often by pretending you have common interests. When using these sites, limit the amount of personal information you share or post to your profile (e.g. full birthday or address), and don't accept friend requests from people you don't know. Also, be sure to check your security settings on these sites.
- Before you connect your laptop, tablet or smartphone: be cautious of free or unsecured wireless Internet connections (wi-fi) in public places. While there are many legitimate free wireless connections available, such as at libraries or airports, some unsecured networks may be set up by criminals to access your personal information. Always check with the establishment to ensure you're connecting to their wireless network.
- Beware of malicious cell phone apps disguised as games or apps from credible brands designed to steal information from your smartphone, or send out expensive text messages without your consent. Be cautious and try to download apps from well-known and trusted brands.

Online Fraud: Phishing, Malware and Tabnabbing

Phishing — What is phishing?

Phishing, or 'brand spoofing' attacks use 'spoofed' (look alike) email and text messages, as well as fraudulent websites. These are designed to fool recipients into divulging personal and financial data such as credit card numbers, account usernames and passwords, SIN, etc. By hijacking the trusted brands of well-known financial institutions, government agencies, online retailers and credit card companies, phishers are able to convince some of the recipients to respond to them.

What should Internet users do about phishing schemes?

Internet users should follow three simple rules when they see emails, texts or websites that may be part of a phishing scheme: Stop, Look and Call.

1. **Stop.** Phishers typically include upsetting or exciting (but false) statements in their email or text messages with one purpose in mind. They want people to react immediately to that false information, by clicking on the link and inputting the requested data before they take time to think through what they are doing. Internet users however, need to resist that impulse to click immediately. No matter how upsetting or exciting the statements in the message may be, there is always enough time to check out the information more closely. Mobile Internet users need to be extra cautious. A smaller screen and different layout can make identifying a fraudulent web site more difficult.
2. **Look.** Internet users should look more closely at the claims made in the email or text. Think about whether those claims make sense, and be highly suspicious if the message asks for any items of personal information such as account numbers, usernames or passwords.

   For example:

- If the email or text indicates that it comes from a financial institution where you have a debit or credit card account, but tells you that you have to enter your account information again, that makes no sense. Legitimate financial institutions already have their customer's account numbers in their records. Even if the message says a customer's account is being terminated, the real financial institution will still have that customer's account number and identifying information.

- If the email or text says that you have won a prize or are entitled to receive some special "deal", but asks for financial or personal data, there is good reason to be highly suspicious. Legitimate companies that want to give you a real prize don't ask you for extensive amounts of personal and financial information before you're entitled to receive the prize.

3. **Call.** If the message or website purports to be from a legitimate company or financial institution, Internet users should call, text or email that company directly. Ask whether the message or website is really from that company. To be sure that they are contacting the real company or institution where they have accounts, credit card account holders can call the toll-free customer numbers on the backs of their cards. Financial institution customers can call the telephone numbers on their financial statements. Never call the number given in the email or text to confirm the contents validity as it will lead to the criminals who sent the message and they will verify whatever was said.

Remember, never respond to a message from someone you don't know and never click on a link in any unsolicited message.

Drive-by malware infections and tabnabbing

Internet users should also be aware of other online fraud —drive-by malware infections and tabnabbing.

Malware is intrusive software aimed at gaining access to private computer systems and causing disruption. A computer can become infected while you visit even legitimate websites or click on a deceptive pop-up window. Keep your computer as safe as possible by applying the latest updates to all your software including your operating system and disable all unnecessary Plug-ins. Consult an expert if you require assistance.

In tabnabbing, an attacker will access one of many tabs you may have open at one time and create a new tab that mimics a real site. You may be fooled into logging on and providing personal information, if the mimicked site indicates your session has expired. You can protect yourself against tabnabbing by always looking for the little padlocked icon that appears in your browser (often at the bottom right) when you visit a secure site. And remember to check the Internet address that appears at the top of your browser. A tabnabbed page will show something that does not resemble the legitimate web site address, even if it contains the name of the company or organization you are trying to access.

Protect Your Money

Be PIN Smart…

Canadians use their debit cards millions of times each day for purchases and cash withdrawals from Automated Teller Machines (ATMs). In fact, Canadians are one of the biggest users of debit cards and ATMs in the world. With the *INTERAC*† shared services, cardholders have convenient access to their cash 24 hours a day, seven days a week.

While *INTERAC* shared services are among the most secure in the world, debit card fraud can occur. Interac Association and its members continue to work together to protect cardholders from debit card fraud.

Protecting your PIN is up to you

Think of it like a key. Instead of unlocking the door to your house or car, your PIN unlocks the gateway to your financial and personal information. We regularly lock our houses and cars, but too often, we're careless about the "keys" to our financial accounts and information.

Cardholders can help keep their money safe by protecting their debit cards and PIN and by following these 10 important steps:

1. Use your hand, body or other blocking method such as a piece of paper or envelope to shield your PIN when you are conducting transactions at an ATM or at the point-of-sale.
2. Never let your debit card out of your sight when conducting a transaction at the point-of-sale. It is preferable that you insert your chip-enabled card in the point-of-sale device yourself. If you do not yet have a chip-enabled card, or if the merchant is not yet able to accept the chip, then your card will need to be swiped. In that case, keep an eye on your card to ensure that it is only swiped once and that you see it being swiped. Always remember to take your debit card and transaction record with you once your transaction is completed.
3. Regularly check your statements and balances to verify all transactions have been properly documented. If entries do not accurately reflect your transactions activities, for example, if there are missing transactions or additional unknown transactions, you should contact your credit union immediately.

4. If your debit card is lost, stolen or retained by an ATM, notify your credit union as soon as you become aware of the problem.
5. Your debit card and PIN are the keys to your account(s). Never disclose your PIN to anyone or you could be liable for any losses. You are the only person who should know it. Keep your card in a safe place and never lend it to anyone.
6. Memorize your PIN — it's your electronic signature. If you suspect that someone knows your PIN, change it immediately or contact your credit union to cancel the card and obtain a new card.
7. When selecting your PIN, never use obvious information. You could be liable for losses if you create your PIN by using your telephone number, date of birth, address or SIN.
8. Be aware of any changes regarding the look of the device you are using. Has it changed in any manner that might indicate a skimming device is attached? There is a simple test you can perform if using a chip-enabled card. As your thumb is pointed at the device, you should be able to insert your card, while your thumb remains completely on your card. If you cannot, stop what you are doing, do not enter your PIN and remove your card. Report any changes to your credit union or owner of the device.
9. Only conduct transactions when and where you feel secure. If anyone tries to distract you, complete what you are doing and retrieve your card before doing anything else. If you cannot retrieve your card, call your credit union immediately.
10. In a proven case of fraud, victims are protected by the Canadian Code of Practice for Consumer Debit Card Services and will not suffer any financial losses. The Code is available on Credit Union Central of Canada's website at: http://www.cucentral.ca/Documents/CanadianCodeofPracticeforConsumerDebitCardServices.pdf

    Each case is reviewed on an individual basis by your credit union.

For more information about the *INTERAC*† shared services or PIN security tips, visit interac.ca.

Important Contacts

The Canadian Anti-Fraud Centre
1-888-495-8501
info@antifraudcentre.ca
antifraudcentre.ca

The Competition Bureau of Canada
1-800-348-5358
competitionbureau.gc.ca

The Little Black Book of Scams
Your Guide to Protection Against Fraud
competitionbureau.gc.ca/blackbook

Government of Canada (Public Safety Canada) Resources on Identity Theft
publicsafety.gc.ca/prg/le/bs/consumers-eng.aspx

Canadian Council of Better Business Bureaus
ccbbb.ca

Major Credit Bureaus

Equifax Canada
To report lost or stolen identification or identity theft:
1-866-828-5961
To order your credit report: 1-800-465-7166
equifax.ca

TransUnion
1-800-663-9980
transunion.ca

MAWB0ZZZA