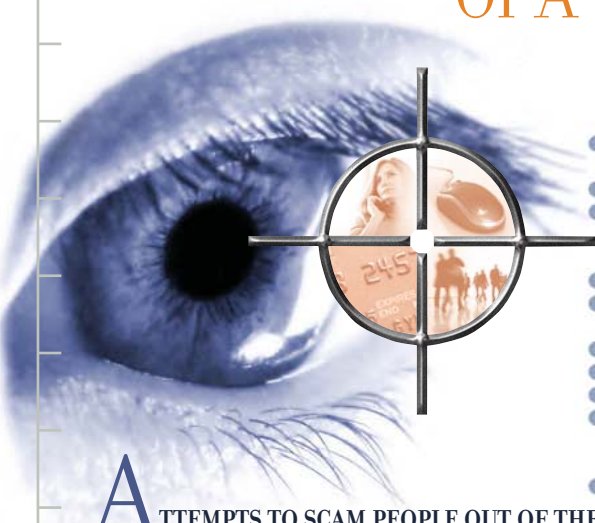


ARE YOU THE NEXT TARGET OF A SCAM?



According to CISC, mortgage-related schemes cost Canadians hundreds of millions of dollars annually.

ATTEMPTS TO SCAM PEOPLE OUT OF THEIR HARD-EARNED MONEY ARE NOTHING NEW, BUT WITH TECHNOLOGICAL ADVANCEMENTS, SCAMMERS ARE BECOMING MORE SOPHISTICATED. LEARNING HOW TO QUICKLY SPOT THESE SCAMS WILL PREVENT YOU FROM BECOMING THEIR NEXT UNSUSPECTING VICTIM.

RCMP'S LIST OF LATEST SCAMS AND FRAUD

Identity Fraud

Identity theft involves stealing, misrepresenting or hijacking the identity of another person or business in order to commit crimes. Phishing involves sending someone an e-mail claiming to be a legitimate enterprise in an attempt to trick the user into disclosing private information.

Advance Fee Fraud

The classic prize pitch scam involves victims receiving notification that they have won a prize. However, in order to collect the prize, the victim is required to pay various fees or taxes in advance. Victims never hear from the organization again. The Nigerian/West African Letter is a well-known example that has been around for years.

Online Auction Fraud

Online auction fraud is the misrepresentation of a product advertised for sale through an Internet auction site, the non-delivery of an item purchased through an Internet auction site or a non-payment for goods purchased through an Internet auction site.

Quick Reference Websites:

Royal Canadian Mounted Police
www.rcmp-gre.gc.ca

Financial Consumer Agency of Canada
www.fcac-acfc.gc.ca

Canada's Office of Consumer Affairs
www.ic.gc.ca

Better Business Bureau
www.bbb.org/canada

Investment Fraud

Investment fraud is any fraud associated with investments that impacts a person or company, including the following:

- **Prime Bank Instrument Investment Scheme:** using official-sounding terms, prospective investors are led to believe they are being invited to participate in an otherwise secret trading or investment group.
- **Fraudulent Investment Schemes:** these are often marketed by telephone salespersons using high-pressure selling techniques. Stock market fraud involves fraudulent manipulation of stock exchange transactions, wash-trading and match-trading and false prospectus.
- **Insider Trading:** unlawful insider trading occurs when privileged, non-public information is used to trade on securities or commodities markets. It may include the purchase or sale of shares prior to the disclosure of a corporate news release or the purchase or sale of shares on the basis of information that would never be disclosed to shareholders.

According to the RCMP, credit card fraud losses in 2008 exceeded an estimated \$400 million dollars.

Millions of Canadians are victims of one or more of the frauds listed each year.

Counterfeiting and Credit Card Fraud

Payment card counterfeiters are now using the latest computer devices to read, modify and implant magnetic stripe information on counterfeit payment cards. Counterfeit cards include forged or falsified credit cards, often manufactured by "skimming" the data contained on magnetic stripes of existing legitimate cards. Criminals steal credit cards from workplaces, vehicles or health clubs, or they intercept the delivery of a card to the cardholder through mail theft. In no-card fraud, specific card details are obtained from victims when a criminal promotes the sale of exaggerated or non-existent goods and services, resulting in subsequent fraudulent charges against the victim's account.





Stay Informed TO STAY PROTECTED.

HERE ARE A FEW PREVENTATIVE MEASURES
AND TIPS YOU NEED TO KNOW TO AVOID
BECOMING A VICTIM OF A SCAM.

Mortgage Debt Elimination Schemes

Be aware of e-mail or web-based advertisements that promote the elimination of mortgage loans, credit card and other debts, while requesting an upfront fee to prepare documents to satisfy the debt. There is no easy method to relieve your debts, and borrowers may end up paying thousands of dollars in fees without the elimination or reduction of any debt.


Foreclosure Fraud Schemes

Perpetrators mislead homeowners into believing that they can save their homes in exchange for a transfer of the deed and upfront fees. The perpetrator profits from these schemes by remortgaging the property or pocketing fees paid by the homeowner without preventing the foreclosure. The victim suffers the loss of the property, as well as the upfront fees. Always seek a qualified credit counselor or lawyer for assistance.

Predatory Lending Schemes

Beware of lenders who tell you that they are your only chance of getting a loan or owning your own home, and avoid "no money down" loans. This is a gimmick used to entice consumers to purchase property that they likely cannot afford or are not qualified to purchase. Be wary of mortgage professionals who falsely alter information to qualify a consumer for a loan.

Do not let anyone persuade you into making a false statement, such as overstating your income, the source of your down-payment or the nature and length of your employment. Never sign a blank document or a document containing blanks.



WAYS TO PROTECT YOURSELF FROM MASS MARKETING FRAUD

Things you should do:

- Insist on learning the full name, address and contact information for any company soliciting your business, personal information or assistance.
- Insist that all solicitors send materials to you in writing so that you are able to study the full details of the offer, as well as any guarantees and/or refund policies.
- Research all solicitors through the Better Business Bureau and/or consumer protection service in the province or city where the company is located.
- To stop receiving telephone solicitations, instruct solicitors to delete your contact information from all call lists and register with the Canadian National Do Not Call List by signing up online at LNTE-DNCL.gc.ca or calling the toll-free number 1-866-580-3625.
- Report suspicious telemarketing calls, mail solicitations or advertisements to your local RCMP by phone or online at www.recol.ca, or PhoneBusters at 1-888-495-8501.

Things you should NOT do:

- Do not make any payments to either secure a prize or improve your chances of winning a prize.
- Do not be intimidated into making hasty financial decisions by high-pressure sales tactics.
- Do not provide anyone with your sensitive personal or financial information unless it is to an entity whose legitimacy is personally known to you or you personally initiated the contact with the entity.
- Do not send funds via wire or electronic money transfer services unless it is to an entity whose legitimacy is personally known to you or you personally initiated the contact with the entity.
- Do not be lured by offers that are simply too good to be true ... they almost certainly are.

IF YOU SUSPECT FRAUD, CONTACT YOUR LOCAL RCMP
OR SUBMIT A TIP ONLINE AT WWW.RECOL.CA

Protecting Your Identity

Credit cards and debit cards have become the most popular payment options for Canadians. Most people today prefer paying with plastic to handing over cash and cheques. At the same time you should be aware of the potential for credit card and debit card fraud.

To protect yourself, learn to recognize the various forms of card fraud and use the preventative tips we've provided below. Increasing awareness about identity theft is an important issue in today's rapidly changing world. We want to provide you with a general overview about identity theft, helpful tips and practical information to help you detect and prevent identity theft. This tip sheet identifies key ways to reduce your risk of becoming a victim of identity theft.

What is identity theft?

Identity theft occurs when someone uses your personal information without your knowledge or consent to commit a crime, such as fraud or theft.

How does identity theft work?

Identity thieves steal key pieces of your personal information and use it to impersonate you and commit crimes in your name. In addition to names, addresses and phone numbers, thieves look for social insurance numbers, driver's licence numbers, credit card and banking information, bank cards, calling cards, birth certificates and passports. They may physically steal important documents, or they may find out your personal information in other ways, without your knowledge. Once they steal the information, they may use stolen identities to conduct spending sprees, open new bank accounts, divert mail, or apply for loans, credit cards and social benefits.

What can I do to protect myself?

- Be careful and aware of sharing personal information
- Minimize the risk.
Be careful about sharing personal information.
- When you are asked to provide personal information, ask how it will be used, why it is needed, whom it will be shared with and how it will be safeguarded.
- Be particularly careful about your Social Insurance Number (SIN); it is an important key to your identity, especially in credit reports and computer databases. Use other types of identification when possible (and when your SIN is not required by law).
- Only provide personal information on the phone or through the mail when you have initiated the contact or know with whom you are dealing.
- Only provide personal information over the Internet when you know that the communication channel is secure.

- If you receive a call from someone claiming to represent your credit card issuer or your bank and the caller asks for your credit card number, do not provide it. If the call is legitimate, the issuer will already know your credit card number.
- Never disclose your Personal Identification Number (PIN) to anyone. No one from a financial institution, the police or a merchant should ask for your PIN.
- Use appropriate security measures
- Keep statements in a safe place - they contain sensitive and personal information.
- When selecting a PIN, always avoid the obvious - your name, telephone number or date of birth.
- Never write your PIN down or disclose the number to anyone.
- Choose difficult passwords - not your mother's maiden name. Memorize them, change them often. Don't write them down and leave them in your wallet, or some equally obvious place.
- Use your hand as a shield to prevent others from observing you entering your PIN to ensure privacy when conducting a transaction by Automated Banking Machine (ABM), debit, telephone or computer.
- Conduct your ABM transactions when and where you feel most secure.
- Guard your mail.
 - Deposit outgoing mail in post office collection boxes or at your local post office.
 - Promptly remove mail from your mailbox after delivery.
- Ensure mail is forwarded or re-routed if you move or change your mailing address.
- Take advantage of technologies that enhance your security and privacy when you use the Internet, such as digital signatures, data encryption, and "anonymizing" services.
- If you use the internet/Online Banking, ensure that you protect yourself by using an updated browser and by installing a personal firewall and up-to-date anti-virus software on your computer.
- Keep records safe and don't leave a paper trail
- After completing an ABM or debit transaction, remember to take your card and receipts. Your statements contain valuable information about your finances.
- Be careful what you throw out. Shred documents containing personal financial information such as statements, credit card offers, copies of credit applications, receipts, insurance forms, etc.
- Keep items with personal information in a safe place. An identity thief may pick through your garbage or recycling bins. Be sure to tear or shred receipts, copies of credit applications, insurance forms, physician statements and credit offers.
- Ensure accuracy of your records, statements and activities
- Check your financial statements as soon as they arrive to ensure all charges gathered are correct.
- Review your account statements, passbooks and online activity on a regular basis. Look for extra or missing transactions and report any discrepancies immediately and always within the time period required by your account agreement.

- Pay attention to your billing cycle. If credit card or utility bills fail to arrive, contact the companies to ensure that they have not been illicitly redirected.
- Access your credit report from a credit reporting agency (Equifax or Trans Union) once a year to ensure it's accurate and doesn't include debts or activities you haven't authorized or incurred.
- Always keep your own notes of all transactions, especially those conducted over the telephone or the Internet and store notes securely.
- Guard your cards, cheques and ID.
- Carry only the identification and credit cards you need when traveling, whether locally or abroad.
- Minimize the identification information and number of cards you carry.
- Don't carry your SIN card; leave it in a secure place.
- Your bank card is the key to your account(s). It is for your personal use only. Keep your card in a safe place and never lend it to anyone.
- Do not carry your cards in your chequebook.
- Never leave your bank cards, credit cards, cheques or identification unattended at work. The workplace is the number one place for thefts.
- Don't leave your bank cards, credit cards, cheques or identification in your car.
- If your chequebook is lost or stolen, immediately call your bank and inform them of the missing cheque numbers.
- Sign your credit cards in permanent ink as soon as you receive them.
- Make a list of all your cards and their numbers and store this list securely. Credit card numbers can be used to conduct transactions without the card present.
- When making a purchase, keep your cards in view at all times; ensure you take your card back as soon as a transaction swipe has been completed with your card.
- Do not sign a blank cheque or charge slip.

How do you know if you might be a victim?

- Your bank statement, online activity or passbook lists transactions that you haven't performed or authorized.
- A creditor informs you that an application for credit was received with your name and address, which you did not complete.
- You receive credit card statements or other bills in your name that do not belong to you.
- You no longer receive legitimate credit card or bank account statements or you notice that not all of your mail is delivered.
- A collection agency informs you they are collecting for a defaulted account established with your identity and you never opened the account.
- Your cheque book, passbook or credit card goes missing.

What should you do if you are or may be a victim?

- Notify creditors and financial institutions immediately if your bank cards, credit cards or identification are lost or stolen.
- Consult Financial Institution(s).
- Discuss whether to close your bank accounts and open new ones.
- Ask your bank to replace your existing bank card with a new one and assign new PINs.
- Ask how to report new problems.
- Consult Issuer(s)
- Discuss whether to cancel your credit cards and get new ones issued.
- Ask the creditors about accounts tampered with or opened fraudulently in your name.
- Notify your telephone, cable, and utilities companies that someone is or may be using your name to open new accounts fraudulently.
- If identification has been stolen, contact all issuers to have the ID coded as stolen.
- Alert Government Organizations if your SIN is lost or stolen, or if you suspect that someone has been using your SIN to get a job, call Human Resources Development Canada toll-free at 1-800-206-7218 and select option 3. Or, contact via mail at P.O. Box 7000 Bathurst, NB E2A 4T1.
- If your Driver's Licence is lost or stolen, contact your local driver and vehicle license issuing office.
- Contact Canada Post if you suspect that someone is diverting your mail.
- Consider whether you should contact the police.
- Advise Credit Agencies
 - Call Equifax toll-free at 1-877-323-2598.
 - Call Trans Union toll-free at 1-877-525-3823.
 - Call Experian toll-free at 1-888-826-1718.

Where can I get help or more information?

Fraud - recognize it, report it, stop it. To learn more or to report a fraud, you can contact the following:

Phonebusters: 1-888-495-8501, www.phonebusters.com

Call Phonebusters to report fraud. They are a national anti-fraud call center operated by law enforcement agencies such as the RCMP. They collect complaints and forward them to the appropriate law enforcement agencies.

Competition Bureau: 1-800-348-5358, www.cb-bc.gc.ca

RCMP: www.rcmp-grc.gc.ca/scams-fraudes/index-eng.htm

The RCMP website highlights the latest consumer scams and how you can deal with them.

Reporting Economic Crime Online: www.recol.ca

Canadian Council of Better Business Bureaus: www.cbbb.ca