A helpful Guide to:
Learn how to spot different types of fraud
Learn tips on how to combat fraud
Learn what to do in case of fraud

Presented by

Ladysmith & District Credit Union™
service since 1944

Our Community. Your Credit Union.™

www.ldcu.ca

INTRODUCTION

In 2022, the Canadian Anti-Fraud Centre reported losses in excess of $530 million dollars. Since it's estimated that only 5-10% of people actually report fraud, the potential losses could exceed 1 billion dollars in Canada alone. In 2023, global losses due to financial scams amounted to approximately $485.6 billion.

Whether it's a romance scam, subscription scam, charity scams, cryptocurrency scam, phishing emails, online shopping scam, CRA scam, tech support scam, lottery scam, inheritance scam, Grandparent scam, ransomware, ID theft or some Nigerian prince who is begging for your help, we're constantly being targeted.

In addition to these digital scams, old fashion in-person scams are still quite common, whether it's a rental scam, a contractor scam, ticket scam, investment scam, or door to door charity donation scam. What's more is now we have hybrid versions where scammers operate online but have local accomplices who physically show up at your door.

With the rapid advancement of technology, especially AI, the landscape has become even more challenging. Social media and AI is enabling crooks to create highly convincing scams, from deepfake videos and realistic voice simulations to spoofed phone numbers that seem to come from people you know. They can also design fake websites that mirror legitimate ones, exploit google through SEO manipulation which pushes their fake listing to the top of the search results. All of which makes it increasingly difficult to tell what's real from what's fake.

But the deception doesn't stop there—there are fraud call centres who are staffed with criminals that are trained in psychological and emotional manipulation. They know how to exploit our fears, desires, and vulnerabilities, using tactics designed to pressure us into making hasty decisions. By playing on our emotions, they gain our trust just long enough to commit their fraud.

Scary right? But there is good news.

Even though the tools are becoming more sophisticated, the core tactics remain as old as history itself. Scammers still prey on emotions like fear, trust, and sympathy, often creating a false sense of urgency to manipulate their victims, just as they have for centuries. Understanding how they work is the first step in protecting ourselves.

HOW THEY DO IT

Fraud relies on:

- **Deception**: Manipulating facts or creating false information.
- **Ignorance**: Targeting a lack of knowledge or weaknesses.
- **Exploitation**: Gaining victims' confidence and trust to lower their guard.
- **Urgency**: Creating pressure to rush decisions without proper checks.

How do they do it?

Crooks have access to a vast and constantly evolving array of tools to commit fraud, both in person and online, and they target victims across all demographics. From seniors who may be more vulnerable to phone scams or identity theft, to young adults who might be lured by phishing emails or social media fraud, no age group or socioeconomic status is immune. Online criminals exploit unsecured networks, steal personal data through breaches, and use advanced techniques like ransomware and deepfake technology. In person, they deploy tactics such as skimming devices, counterfeit documents, and impersonation. Whether targeting individuals or businesses, these fraudsters tailor their methods to exploit the specific weaknesses of each demographic, making it crucial for everyone to stay vigilant and informed.

Tools they use:

- **Phishing Emails:** These unsolicited emails typically appear to come from legitimate sources, such as banks, tech companies, or trusted organizations, and often include urgent or alarming messages to prompt quick action. The goal is to deceive recipients into divulging sensitive information, such as passwords, credit card numbers, or other personal details.

- **Smishing emails:** Same as phishing but though text messaging.

- **Spoofed Caller ID:** Scammers use techniques to falsify caller ID information, making it appear as though the call is coming from a trusted source, like a bank or government agency.

- **Identity Theft:** Using stolen personal data to open accounts, make purchases, or commit other fraudulent activities in the victim's name.

Ladysmith & District Credit Union™
service since 1944

Our Community. Your Credit Union.™

www.ldcu.ca

- **Skimming Devices:** Physical devices attached to ATMs or point-of-sale terminals or gas station pumps to capture credit card information without the user's knowledge. These include overlay skimmers, insertable skimmers, and RFID (radio frequency identification technology) portable skimmers.

- **Dumpster Diving:** Scammers search through discarded documents and trash to find personal or financial information that can be used for identity theft.

AI tools they use:

- **Social Engineering:** This is a manipulation technique used by crooks to trick individuals into divulging confidential information, performing certain actions, or granting access to sensitive systems or accounts. Rather than directly hacking computer systems, social engineers manipulate human psychology, often by leveraging emotions like trust, fear, or sympathy to create a false sense of urgency.

- **Deepfakes:** AI-generated deepfakes can create realistic video or audio recordings of people. AI can synthesize voices to impersonate trusted individuals, like a bank representative or colleague, to deceive victims over the phone.

  Real-World Example: In 2019, a British energy company was scammed out of $243,000 when criminals used AI-powered voice-cloning technology to impersonate the company's CEO. The scammer, using a deepfake voice, called the company's manager and instructed them to transfer funds to a foreign account.

- **Chatbots:** AI chatbots can impersonate humans in conversations online or in customer service, engaging multiple victims at once and adjusting their responses to appear more human, gradually tricking people into sharing sensitive information.

- **Data Mining and Behavioral Analysis**: We all know that social media collects detailed information about us. AI systems can sift through vast amounts of public and private data, such as social media posts, emails, and browsing habits, to build a detailed profile of a target. This allows attackers to create targeted scams by knowing a target's likes, interests, relationships, and vulnerabilities.

  Predictive Behavior: By analyzing patterns in behavior and preferences, AI can predict how a person might respond to different types of scams, AI can identify individuals more likely to fall for scams, such as the elderly, those experiencing financial difficulties, or people dealing with emotional stress, and customize attacks accordingly.

- **Fake Accounts:** AI helps generate fake articles, social media posts, and realistic-looking accounts and profiles, all used to get your personal information. AI can create or manipulate reviews, testimonials, and comments online to make fraudulent schemes seem more legitimate.

DON'T ALLOW YOURSELF TO BE EMOTIONALLY MANIPULATED!

- **Be skeptical:** Assume everything is fraud until proven otherwise. Treat any unexpected/unsolicited requests for money, information, or urgent action with suspicion until you can verify their legitimacy.

- **Don't be pressured:** Scammers are experts at manipulating our emotions, whether through fear, or sympathy. These tactics are intended to create a sense of urgency to trick us into making quick decisions. A common tactic is claiming your account has been hacked or compromised, then, for your protection, demanding payment through gift cards or cryptocurrency. Always pause and assess the situation calmly—legitimate businesses will never ask for payment this way. These methods are frequently used by fraudsters to avoid detection and make it nearly impossible for victims to recover their funds.

- **Don't Be Afraid to Say No:** Whether it's a pushy person, an urgent request for personal information, or an offer that sounds too good to be true, remember that it's okay to say no. Protecting yourself is more important than being polite.

- **Use a Code Word for discussing sensitive information over the Phone:** This will help ensure you're really speaking with a family member or loved one and help prevent you from falling victim to impersonation scams.

- **VERIFY** Always scrutinize emails, websites, or social media messages, before interacting with them. Always be skeptical of unsolicited messages asking for information, or money.

- **Check Website URLs**: Always double-check website addresses in your browser to avoid phishing scams—look for subtle misspellings or extra characters. However, this method may not work if a company uses URL shorteners like TinyURL, which conceal the full address. This makes it difficult to know where the link will lead so be especially cautious when encountering shortened links.

- **Don't Click on Suspicious Links:** Fraudsters often disguise links or use fake email addresses to mimic legitimate companies. You may have received a message purporting to be form Netflix claiming your monthly subscription fee didn't go through. Or Canada Post/UPS or Amazon claiming there's an issue with your package delivery, click on this tracking link. Perhaps you received a message saying your computer is

infected or that your anti-virus subscription has expired? What about a Personality Quiz? This type of scam is often shared on social media. These quizzes appear fun and harmless, asking questions such as "Which celebrity are you most like?" or "What is your spirit animal?" However, behind the scenes, scammers collect personal information that they use for identity theft or targeted phishing attacks.

- **Double-Check Requests**: Always be skeptical of unsolicited messages asking for information or money. If someone asks for sensitive information, especially through unsolicited contact, verify. If an email claims to be from a trusted source (like a bank or service provider), contact the company directly through official channels to confirm before responding. If you receive a suspicious call, hang up and contact the company directly using a number from their official website or the back of your card.

PROTECT

- **Use Strong Passwords:** Opt for complex passwords at least 14 characters long that include a mix of letters, numbers, and special characters. Do not use your name or birth date. Consider using a password manager to generate and store complex passwords securely.

- **Enable two-factor authentication where possible.**

- **Setup text alerts:** This allows real time monitoring of your accounts. Don't know how to set them up? You can find this and other helpful videos on our website www.ldcu.ca under Tips and Tools

- **Regularly review your credit report** to catch signs of identity theft, such as new accounts opened in your name.
  Equifax Canada, www.equifax.ca (1-800-465-7166)
  TransUnion, www.transunion.ca (1-800-663-9980)

- **Shred Sensitive Documents:** If you don't have one, invest in a personal shredder. Shred any documents containing personal or financial information before discarding them.

- **Check your Insurance:** It's a good idea to have extra protection in case you do become a victim.

When you're on social media:

- **Adjust Privacy Settings:** Limit who can see your posts, personal information, and friend list.

- **Be Cautious with Friend Requests:** Only accept friend requests from people you know. Scammers often create fake profiles to gather information or send malicious links.

- **Don't Overshare:** Avoid posting sensitive information like your full name, location, travel plans, or personal details that scammers can use to target you.

- **Educate Yourself and Others:** Stay informed about common social media scams and share this knowledge with your friends and family to help protect them as well.

SECURE

- **Update Software:** Regularly update your operating systems, apps, and antivirus software to ensure you have the latest security patches.

- **Use Secure Connections:** When accessing sensitive information online, use a secure, private Wi-Fi connection. Avoid conducting financial transactions over public Wi-Fi networks. If necessary, use a Virtual Private Network (VPN).

Report Fraud to the Authorities:
Remember, fraud protection is a team effort. If you suspect fraud or have fallen victim to it, it's crucial to report it promptly while providing as much detail as possible. Your cooperation is vital in helping law enforcement agencies along with financial institutions investigate and prosecute fraudsters, giving you the best chance at recovering any loss.

RCMP
Report online at the Canadian Anti-Fraud Centre
(1-888-495-8501)
info@antifraudcentre.ca
www.antifraudcentre.ca

Local RCMP Detachment
www.rcmp-grc.gc.ca
Nanaimo- 250-754-2345
Ladysmith- 250-245-2215
Duncan- 250-748-5522

Your Financial Institution

Equifax Canada,
For lost/stolen ID or ID theft
(1-866-828-5961)
www.equifax.ca

TransUnion, www.transunion.ca
(1-800-663-9980)

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

Resources:

https://www.canada.ca/en/revenue-agency/campaigns/fraud-scams.html

https://competition-bureau.canada.ca/little-black-book-scams-2nd-edition

Remember, stopping fraud is a partnership—by working together, we can create a stronger defense. Following these tips will reduce your risk, but ongoing vigilance and education are essential. This list isn't exhaustive, and no method is foolproof, but staying informed is your best protection.