Protecting against **fraud**

In this increasingly digital world, it's important to keep your personal information safe to avoid financial fraud. The first step to protecting yourself and your financial information is prevention. Learn more about common types of financial fraud, tips on how to avoid becoming a victim and what to do if you are.

What is financial fraud?

Financial fraud occurs when a fraudster gets a hold of and uses your personal information to essentially steal your money for their own gain. Financial fraud comes in many forms including identity theft, credit card fraud, investment fraud and fake emails or websites that trick you into providing personal financial information. One hallmark of financial scams is that they seem "too good to be true", offering incentives and benefits that are not realistic. In addition to emotional distress, victims of fraud often suffer financial losses and have to spend time trying to clear their financial records.

Anyone can be a victim of fraud and the risk is not linked to your age, race, income or geographic location. Scammers just want your money, but you can reduce the likelihood of this happening by educating yourself and using and applying the information that follows.

Identity theft

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

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 acquire your PIN. Once they have a few pieces of your information, criminals may be able to open a new credit card account or financial account in your name without you even knowing.

Here are some ways identity thieves can get your personal information:

- Steal your wallet, purse or mail
- Complete a change of address form to divert your mail to another location
- Rummage through your garbage or home
- Obtain your credit report by posing as a landlord or employer
- Use personal information you share online including social media sites
- Hack into your email
- 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
- They establish phone or internet services in your name
- They buy cars by taking out car loans in your name
- They mortgage your home

Online fraud – phishing, pharming, tabnapping and malware

Phishing is the attempt to acquire sensitive information and defrauding an online account holder of financial information by posing as a legitimate company,

such as a financial institution, the government, or credit card company. Phishing is designed to fool recipients into divulging personal and financial data such as credit card numbers, account usernames and passwords, SIN, etc.

Pharming (pronounced 'farming') is another form of online fraud very similar to phishing. Pharmers rely on bogus websites and thefts of confidential information. Pharming re-directs victims to the bogus website even if the victim has typed in the correct website address.

Tabnabbing is one form of phishing where an attacker will access one of many tabs you may have open in your website browser at one time and create a new tab that mimics a real site. You may be fooled into logging on and providing personal information. You can protect yourself by always looking for the little padlocked icon that appears in your browser when you visit a secure site.

Inform yourself of the common scams so you know the warning signs.

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.

Common scams

Job and employment scams – An employment advertisement offers a work-at-home opportunity to earn significantly higher income. Paying money for job information or to be listed for jobs in Canada or abroad is risky. A common theme in these scams is that they make promises they don't keep. This can result in financial loss or can compromise important personal information. During a phone interview, beware if the interviewer asks too many personal questions that could later be used to assume your identity, such as your SIN.

Medical and health scams – Medical scams prey on human suffering and offer solutions where none exist, or promise to simplify complex health treatments, such as miracle cure scams and weight loss scams. They often require large advance payments or ask you to enter into a long-term contract to participate in the program.

Credit protection – The fraudster will say that they will protect you from scammers who could run up huge debts on your credit card. The fraudster will then ask you to send your credit card number and offer to provide protection for a nominal fee. Offers of protection or insurance against fraud are just attempts to get your credit card numbers and your money.

Emergency scam – Typically a grandparent receives a phone call from a fraudster claiming to be their grandchild or friend, asking for money immediately to bail them out of an emergency situation, like a car accident or jail. Be suspicious and make sure to verify any emergency situation before sending any funds, even if the situation seems urgent.

Money transfer request scam – You 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. You will be offered a large portion of the money if you help and are told to provide your financial account information that the money can be transferred to. You will likely be asked for more money and could also find your account has been attacked and your money has been transferred out. 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 – These scammers will play on your emotions and are collecting money for a fake charity or by impersonating a real charity. The scams cost you money but 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 their database, so check to make sure that the charity that has approached you is genuine before making a donation.

Dating and romance scams – Scammers set up a bogus dating website where you pay for each email or message you send and receive. You may even be approached by a scammer on a legitimate dating website. 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-qualification scam – You're told you've been "pre-qualified" for a low-interest loan or credit card or to repair your bad credit and they ask for your SIN, driver's license and financial account numbers. 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 – An invoice states an urgent delivery of office supplies is awaiting confirmation for your business address, but the bill hasn't been paid yet. Scam operators trick many businesses into paying for goods and services they haven't ordered.

Winning prize scam – A caller, 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 to make a purchase before you can collect your prize. If you send money, you'll never get it back. Legitimate lottery and sweepstakes administrators never charge fees or taxes to deliver your prizes.

Tips on how to detect scams:

- 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 for 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 that you did not order

How to protect yourself

Prevention is the key to keeping yourself protected from fraud. Here are some quick tips:

- Don't disclose personal information or account numbers to anyone unless you initiated the contact, such as contacting one of our branches or Member Hub
- Memorize your PIN and don't disclose your PIN to anyone. Use your hand and body to block anyone from seeing you enter your PIN
- Notify your financial institution immediately if your debit card or credit card is lost or stolen
- Regularly check your account activity and balances to verify all transactions were conducted as planned by you
- Properly shred any important personal and financial paperwork when it's no longer required
- Memorize your SIN and keep your SIN card in a secure place
- Protect your computer with firewall and anti-virus software and use strong passwords
- Keep your smartphone locked using a password and use an app that will track and report the location of your phone
- Check your mail regularly and notify Canada Post to hold your mail if you will be away. Or better yet, sign up for electronic statement and bill services to reduce your reliance on mail
- Regularly check your credit report

Report fraud and learn more

To report financial fraud, contact us immediately at 604-419-8888. Connect with us to learn more about how to protect yourself and loved ones from financial fraud. Visit us in-branch, call our Member Hub (604-419-8888) or book an appointment with an advisor online. (https://www.gffg.com/Personal/AboutUs/ContactUs/Financial/)

Important contacts

The Canadian Anti-Fraud Centre, 1-888-495-8501
The Competition Bureau of Canada, 1-800-348-5358
Public Safety Canada

Major credit bureaus

Equifax Canada, 1-866-828-5961
TransUnion, 1-800-663-9980

G&F FINANCIAL GROUP