

OCCCU's 2024 Book of Common Frauds



Read about the latest scams and how to best
protect yourself!

Protect Yourself: Know the Signs of Fraud

Fraud and scams are on the rise in Canada due to a combination of factors, including the shift towards digital transactions and the increased vulnerability created by the COVID-19 pandemic. Cybercriminals exploit fears and uncertainties, using tactics like phishing and impersonation of trusted organizations to steal personal information. Vulnerable populations, particularly seniors and those less tech-savvy, are often targeted with high-pressure tactics. Additionally, the emergence of cryptocurrencies has introduced new scams, while social media provides a platform for reaching potential victims. Many individuals do not report these scams due to embarrassment, making it challenging to fully understand the problem's scope. Authorities are responding with public awareness campaigns and improved cybersecurity measures to help combat this growing threat.

Being aware of current scams will help to protect you!

Top Scams in Canada:

- **Romance Scams:** Fraudsters create fake profiles on dating sites to exploit emotional connections for money.
- **Phishing Scams:** Emails or texts that appear to be from trusted sources, aiming to steal personal information.
- **Tech Support Scams:** Scammers pose as tech support representatives, claiming your device has a virus to gain access or charge for services.

- **Elder Fraud:** Targeting seniors with scams related to fake lotteries, government grants, or high-pressure sales tactics.
- **Investment Scams:** Promises of high returns on investments, often in cryptocurrency or real estate, that turn out to be fraudulent.
- **Government Impersonation Scams:** Calls from individuals claiming to be government officials demanding payment for supposed debts or taxes.
- **Online Shopping Scams:** Fake websites or social media ads that sell non-existent products.
- **Employment Scams:** Job offers that require upfront fees for training or supplies, or those that ask for personal information.
- **Emergency Money Scams:** Scammers impersonate family members or friends, claiming they're in a crisis and need immediate financial help.


How to protect yourself:

- **Be Skeptical:** Always question unsolicited calls, emails, or messages asking for personal information. Verify the source before responding.
- **Secure Personal Information:** Keep sensitive information like Social Insurance Numbers, bank details, and passwords private. Use strong, unique passwords for different accounts.
- **Monitor Financial Statements:** Regularly check your bank and credit card statements for any unauthorized transactions. Report suspicious activity immediately.
- **Use Two-Factor Authentication:** Enable two-factor authentication on accounts whenever possible for an added layer of security.
- **Be Cautious with Links and Attachments:** Avoid clicking on links or downloading attachments from unknown or suspicious sources, as they may contain malware.

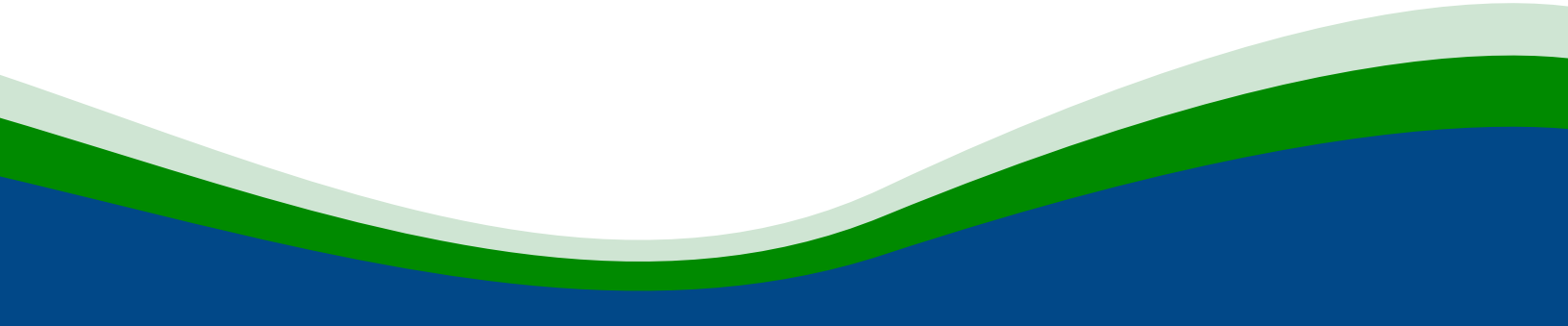
- **Shred Sensitive Documents:** Shred bank statements, credit card offers, and any documents containing personal information before disposal.
- **Educate Yourself:** Stay informed about common scams and fraud tactics. Knowing what to look out for can help you avoid falling victim.
- **Trust Your Instincts:** If something feels off, it probably is. Don't hesitate to seek advice or report suspicious activity.
- **Report Fraud:** If you suspect you've been targeted or fallen victim to fraud, report it to local authorities or consumer protection agencies.
- **Be Aware of Phishing Scams:** Look for signs of phishing, such as poor grammar, generic greetings, and urgent requests for information.

What to do if you've been scammed:

- **Stay Calm:** Take a deep breath and gather your thoughts before acting.
- **Document Everything:** Keep records of all communications related to the scam, including emails, texts, and any receipts.
- **Report the Scam:** Contact your local authorities and report the incident to organizations like the Canadian Anti-Fraud Centre. This helps them track trends and prevent further scams.
- **Notify Your Bank or Credit Card Company:** If you provided financial information or made payments, inform your bank or credit card company right away. They may be able to reverse transactions or protect your accounts.
- **Change Passwords:** Update passwords for any accounts that may have been compromised, and enable two-factor authentication where possible.

- 
- **Monitor Your Accounts:** Keep a close eye on your financial statements and credit reports for any unauthorized activity.
 - **Consider a Fraud Alert or Credit Freeze:** Place a fraud alert on your credit report or consider freezing your credit to prevent new accounts from being opened in your name.
 - **Seek Support:** If the scam has caused emotional distress, consider talking to friends, family, or a professional for support.

If you have any questions or concerns about fraud, please reach out to us—**we're here to help**. You can contact our Fraud Ambassadors Suzanne Bramham by email suzanneb@oshawacu.com or phone 905-436-5417 or Patricia Albrecht by email patriciaa@oshawacu.com or phone 905-436-5412.



Pet Scam

A pet scam is when a scammer makes a fraudulent posting online in an attempt to steal money or sensitive information from individuals. The fraudster will post a fake ad listing a new litter available, often puppies and kittens. These types of scams are more common on websites such as Kijiji and Craigslist. Pet scams have been on the rise since Covid-19, seeing an average reported loss of \$850.00 in 2022.

Pet scammers will generally list animals for prices that are too good to be true and will often ask for a deposit to “hold” the animal before ever meeting with a potential buyer. These fraudsters will try to rush you into a decision and be vague with answers to your questions. Remember that responsible breeders will be happy to share any information you request.

Pet Scam Scenario:

- You decide that you would like to adopt a puppy.
- You think a big dog would be nice, so you start looking online.
- You come across the following advertisement (flyer) for German Shepherd puppies
- You notice the great price and the puppies are available for pick up already, so you decide to reach out to the seller.
- Read the text exchange with the “seller” below:

SELLER'S MARKET

Purebred German Shepphard Puppies for sale



\$500.00 EACH
Price Negotiable

Purebred puppies for sale. 3 male 1 female.

Looking for there forever .home!

Ready to go asap.

Puppies have been dewormed and have received their
first shots.

For faster response please text Belinda (123)456-7890



Belinda- Dog lady >

Mon, Jan 15 at 4:34 PM

Hi there!

I saw your German shepherd puppies on Seller's Market! I am very interested! Are they still available

Yes they are available

Awesome! Would I be able to come see them and take one home that day?

Yes but i need a deposit first 100

Etransfer

emmasmith16@sellersmarket.ca

Will do! Can I come Wednesday?!

That should be fine but I need deposit first

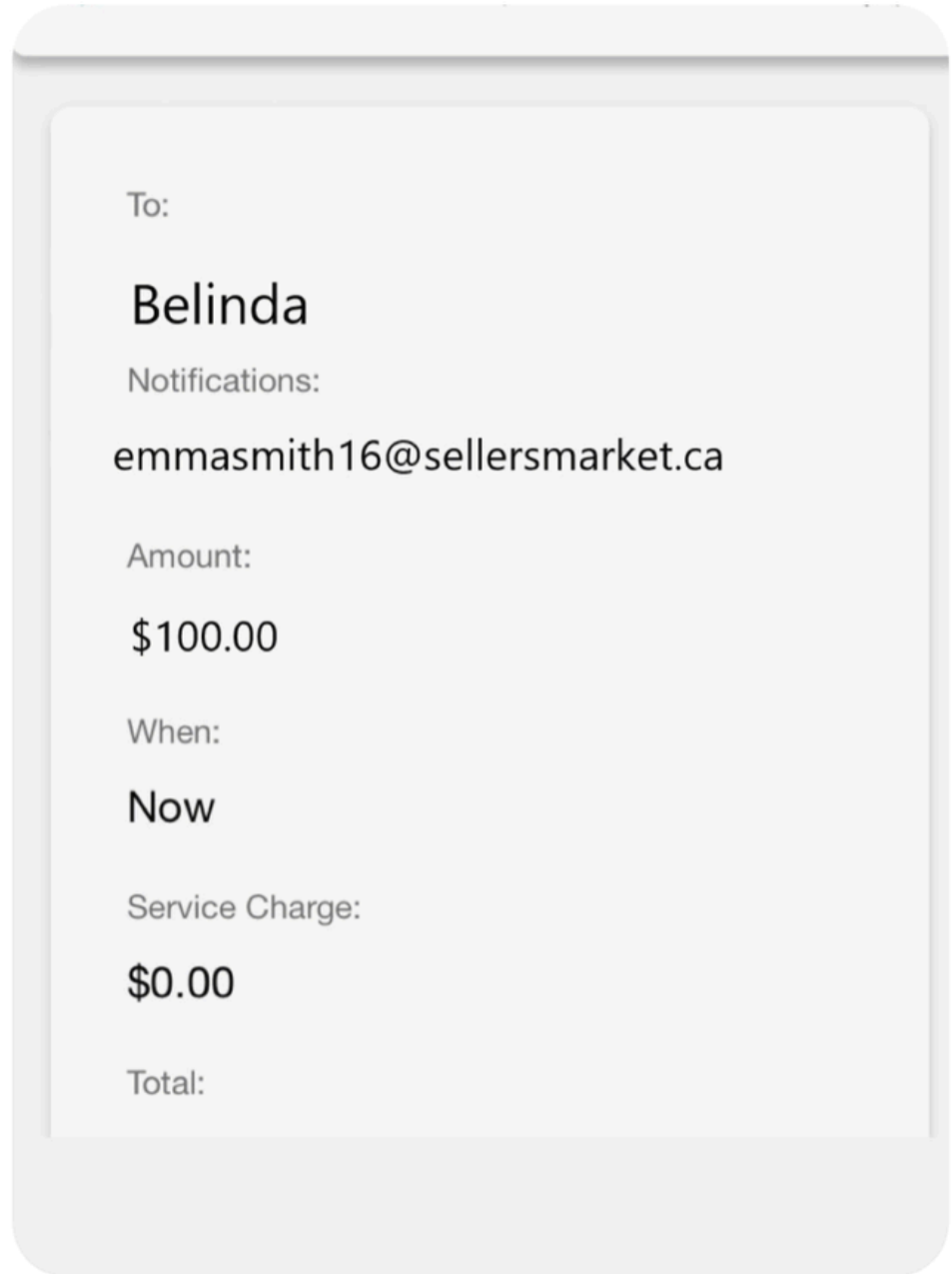
Once sent please let me know by the payment screen

Sent!



Belinda- Dog lady >

Do you have the screen shot



Does Wednesday at 6:00 work?

Should be ill let you know

Awesome! Cant wait! 😊



Belinda- Dog lady >

Hey so the vet fees we're higher than i thought so im gonna need another 100 e-transferred

Oh ok.. your ad says they've already had their shots and have been dewormed.

Yea but this was an extra shot the vet said they needed

Okay... I'll send the additional \$100 now

Can you send the screenshot

To:

Belinda

Notifications:

emmasmith16@sellersmarket.ca

Amount:

\$100.00

When:

Now

Service Charge:

\$0.00

Total:



Belinda- Dog lady >

Thx

What was the extra shot for?

Wednesday 9:15 AM

Hi Belinda, does 6:00 tonight still work to come and pick up the puppy?

No it doesnt work anymore I have to take the puppy ti the vet

Tomorrow should work

Again?

Yea he needs that new shot and tonight was the only time I could get an appointment

Ok.. please let me know what time tomorrow

Thursday 9:33 AM

Hi, what time works for you to come pick up the puppy?

Thursday 2:05 PM

Hello?

Delivered

Unfortunately, the seller does not respond to your repeated requests to pick up the puppy. You come to the conclusion that you have been scammed and are out \$200.00.

What **RED FLAGS** or **WARNINGS** can you notice in this scenario?

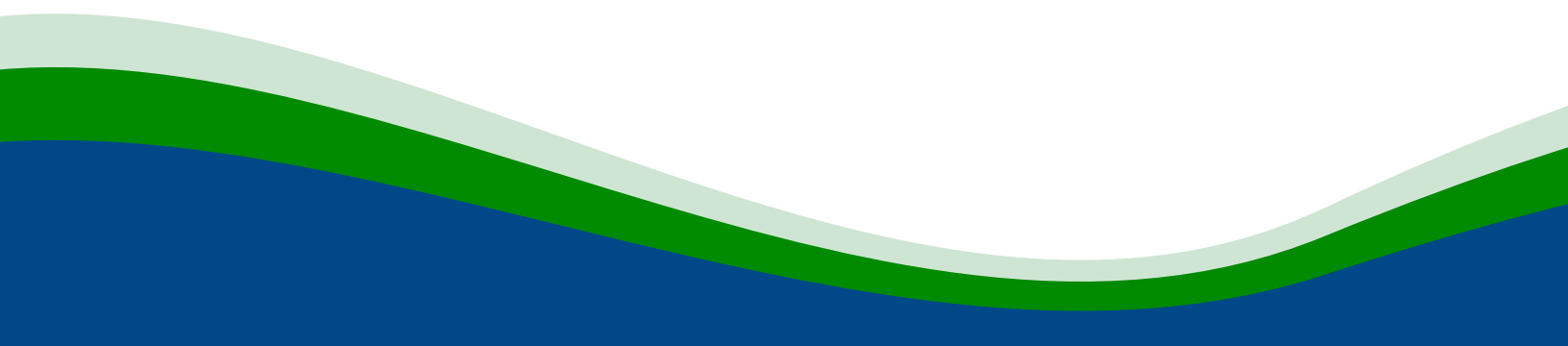
- The price is too good to be true for a purebred dog.
- A deposit is asked to be sent prior to meeting and seeing the dog.
- There are spelling and grammar mistakes in the ad.
- Once funds have been sent, you are asked to send more money.
- The seller is requesting photos of the e-transfer being sent.
- The person's name and email address do not match.
- The fraudster is vague with the information they provide you.

What to do instead:

- Do your research on the average market price of the animal you are interested in purchasing.
- Insist on seeing the animal before making a deposit and ask for the deposit to be in cash upon seeing the animal. If you are not able to see the animal in person, demand a video chat.
- Do a reverse image search of the animal, and see if it shows up on other sites. Many scammers will use stock photos in their fake ads.
- Look for animals from a local animal shelter or breeder, if possible.
- **Call your Credit Union for advice.** If you are unsure or have any inkling of doubt or suspicion, speak to one of our employees prior to proceeding with any transaction.



What to do if you believe you have been scammed:

- **Call your Credit Union** and other financial institutions.
 - **File a police report:** Most police departments allow you to report frauds online by visiting their website.
 - If your credit card number is compromised, **call your credit card company.**
 - **Contact the Canadian Anti-Fraud Centre** to report the scam by visiting their website or calling their toll free number 1-888-495-8501.
 - **Report the scam** to the website where you found the fraudulent posting.
- 

Compromised Account Scam

A compromised account scam occurs when you receive an email, text message, or phone call informing you that your bank account has been compromised or there has been suspicious activity. Often, these scammers will want you to act with a sense of urgency, and follow their instructions immediately. Sometimes this is through an email or text message that contains a link for you to click on. This link will lead to a website that asks for sensitive personal information. These sites are usually spoofed, or fake, and the information you input is given directly to the fraudster who is then able to access your account information and steal your money.

Recently, the Durham Regional Police have been made aware of a new way fraudsters are using compromised account scams to steal money from unsuspecting people. People are receiving a call from a fraudster claiming to be from their bank and informing them their accounts have been compromised. The fraudster goes on to explain that you will need to provide your credit and debit cards, as well as the pin numbers for the cards to the police. The scammer advises that they will be sending a courier to your house to pick up the cards and take them to the police. The cards are then used to withdraw money and make purchases.

If you have been scammed, report the incident to the Durham Regional Police online or by calling 905-579-1520, or to the Canadian Anti-Fraud Centre toll free at 1-888-495-8501



Tips to Avoid Compromised Account Scams:

- **Do not panic!** Be skeptical of unsolicited calls, emails and text messages.
- **Do not act immediately!** Contact your bank or credit card company directly using the number listed on your card, statement, or their official website.
- **Never give your personal identifiable information** to anyone you do not know and trust.
- **Do not feel intimidated or pressured!** Legitimate businesses will not pressure you to act quickly.
- **Don't share your PIN numbers!** Bank employees and police officers will never ask for that information.

If you are ever unsure if an email or phone call you have received is from Oshawa Community Credit Union, call our office at 905-576-4200.



CRA Scams

Especially in the midst of tax season, keep in mind that CRA scams will be on the rise! Many fraudsters are using the Canada Revenue Agency name and logo in their elaborate schemes to deceive people. These types of scams target people through phone calls, emails, and text messages. Some of these scammers will ask for your personal information over the phone, or you may be sent a link that leads to a fake CRA website. Remember, the CRA will never contact you through text messages or instant messages such as Facebook Messenger or WhatsApp and you will never be asked to send payment by Interac e-transfer, Cryptocurrency (Bitcoin), prepaid credit cards, or gift cards such as iTunes, Amazon, etc.

Often, these scammers will attempt to steal money by demanding immediate payment, or stating there is a fee for speaking with a contact center agent. They will also try sending an email or text message with a link to your refund or other benefit payment (such as GST/HST rebate, the Climate Action Incentive, the Canada Child Benefit, etc.) where you are required to input your banking details to receive the funds. Fraudsters will also try to scare you by being aggressive and threatening an arrest or prison sentence. Keep in mind that representatives from the CRA will never use aggressive or threatening language when speaking with you.

How to protect yourself from CRA Scams:

- **Educate yourself** about possible CRA scams.
- **Be cautious** when you receive unexpected contact from the CRA. Verify you are speaking with a legitimate CRA employee.
- **Know what to expect** when the CRA contacts you.

When in doubt, ask yourself:

- Does the CRA have my most recent contact information, such as my email and address?
- Do I have an installment payment due soon?
- Did I file my tax return on time? Have I received a notice of assessment or reassessment saying I owe tax?
- Why is the caller pressuring me to act immediately? Am I certain the caller is a CRA employee?
- Have I received written communication from the CRA by email or mail about the subject of the call?
- Is the caller asking for information I would not give in my tax return or that is not related to the money I owe the CRA?

Online Gambling Scam

Online gambling scams, sometimes referred to as online casino scams, have become more prevalent in recent years. There are many different types of online gambling scams. Some aim to steal your identity or sensitive personal information, while others want to steal your money. Being aware of possible scams will help to protect yourself and your money. Read below for some common online gambling scams.

Deposit Scams:

Some disreputable online casinos will attempt to steal your money. This is done when a player deposits funds into their account but the money doesn't appear in the account. Another way this is done is when the player deposits money but then receives a notification saying the deposit request has been declined despite having enough money in their bank account. These funds are withdrawn from the player's bank account but never deposited into their online casino account. If this happens, players are advised to get in touch with the casino's customer support.

Email Scams:

A fraudster will send an email, imitating a casino, that contains a link that leads to a spoofed website. Once on the fake website the player will unknowingly enter their login information, giving the fraudster access to their account. These scammers monitor players' social media accounts to determine which sites the players frequent in order to deceive them.

Non-Payment Fraud:

This is when an online casino makes it a difficult process for players to withdraw their winnings. Some gambling platforms claim that the wagering requirements aren't met, when they have been, and others will simply refuse using odd excuses. If you have issues withdrawing your winnings, you have likely been scammed.

Bonus Scams:

A lot of online gambling sites will attempt to entice players by offering bonuses, such as welcome bonuses, reload bonuses, refer a friend bonus, etc. Once they have you hooked, some casinos will offer lower bonuses than originally advertised. Further, some scammers create fake bonus offers in an attempt to steal login information and money from players.

Rigged Games:

Some fraudsters will create fake online gambling platforms and rig the games so players have no chance of winning, thus allowing the casino to profit by stealing the player's money. Most players keep playing in hopes they will get out of their losing streak, but just end up losing more money than they intended. Unfortunately, this type of scam is difficult to prove as casino games don't offer the best chances of winning.

Spyware and Ransomware:

Be cautious clicking on links and downloading content from online gambling sites. Some shady gambling sites have relaxed security protocols which makes it easier for hackers to compromise their information that players will click on and download. This then allows the hackers access to a player's sensitive information that they can steal or hold for ransom.

Illegal Sites That Look Legal:

Scammers have started making bogus gambling sites. The sites either look like legitimate gambling sites, or they are online sites for local casinos that do not operate online gambling sites. Both schemes are an attempt to steal sensitive information and money from unsuspecting players. Most frequently, these types of scams are shared on social media sites. Recently, Casino Nova Scotia and Casino New Brunswick have been used in one of these deceptive schemes. The fraudulent ads and websites feature real photos of the casinos. Be cautious when clicking on advertisements for online casinos on social media sites.

How to Protect Yourself from Online Gambling Scams:

- **Educate yourself** about possible online gambling scams.
- **Do your research** before entering a new gambling website.
- **Read reviews** from other players. If there are more negative reviews than positive, that's a red flag.
- **Check that the casino** is backed by a regulated authority and have strict security protocols in place.
- **Use antivirus software on your computer** to protect your data from cyber threats.
- **Consider making small deposits to start**, that way you don't end up losing a lot of money if the casino is fraudulent.

Vishing Scams

Vishing is a type of scam where fraudsters use voice calls, often impersonating legitimate organizations like banks or government agencies, to deceive people into revealing personal information such as credit card numbers, passwords, or Social Insurance Numbers. They might use techniques like caller ID spoofing to make their calls appear legitimate, creating a false sense of trust. The goal is to steal sensitive information or manipulate victims into making financial transactions that benefit the scammers.

Vishing scams are on the rise, and more people are losing money because of them. With the increase in online shopping and banking, scammers have more opportunities to target unsuspecting individuals. It's important to be careful and never give out sensitive information over the phone unless you are absolutely sure who you are talking to.

These types of frauds are happening close to home. Recently, a man and a woman were charged for their involvement in a scam that targeted seniors by pretending to be representatives from their bank or credit card company. They would call the seniors and claim that their accounts were compromised, tricking them into believing they needed to hand over their cards and passwords for safety. Once the victims gave up this information, the scammers sent a courier to collect their bank cards and passwords. With this stolen information, the scammers made fraudulent purchases. The victims of this scam included a couple in their 90s. The two suspects, Lakshanth Selvarajah and Akshayah Tharmakulenthiran from Ajax, are now facing 40 charges, including fraud and unauthorized use of credit cards.

Tips to avoid Vishing Scams:

- **Be cautious when receiving calls from individuals requesting sensitive information from you:** Refrain from sharing personal information such as your full name, DOB, SIN, or banking information over the phone unless you can verify the legitimacy of the caller. Never share your username or password with anybody. Request a contact name and end the call. Call back and communicate with the organization through an official channel, such as their publicly listed phone number or website.
- **Be aware of scare tactics:** Scammers aim to catch you off guard and create a sense of urgency, making you feel like there's no choice but to share the information they're asking for. Some might resort to using threatening language to pressure you into immediate action. Some scammers will attempt to intimidate you by saying you must provide information or your account will be closed/deactivated.
- **Exercise caution with calls from unfamiliar numbers or automated systems:** Allow such calls to go to voicemail if the number isn't recognized. Refrain from utilizing your phone's callback feature or any numbers provided by the caller. Instead, communicate with the site or service using a trusted contact method.
- **Be informed on how your devices work:** Note that many smartphones come equipped with built-in spam protection features capable of filtering, blocking, or reporting spam calls. Refer to your smartphone's manual for guidance on how to activate these functionalities.
- **Implement a code word with family members:** This can enhance safety and security in communication when someone legitimately needs help, but will also protect you from being scammed.

- **Be cautious of unusual requests:** If the individual contacting you via phone or email requests something unusual, such as sending a courier to pick up compromised credit or debit cards, this probably indicates they are a scammer. Keep in mind, credit card companies and financial institutions find it simpler and more cost-effective to deactivate your current cards and provide you with replacements.

Steps to take if you've fallen victim to a Vishing Scam:

- **Contact your financial institutions.** Inform them you have been scammed and inquire about cancelling any fraudulent transactions and blocking future charges.
- **Immediately change your passwords.** This should apply to all affected accounts, as well as any accounts that used the same compromised passwords.
- **Keep an eye on your financial accounts regularly.** Most financial institutions have alerts you can implement to help monitor your accounts and credit cards. Also, think about enrolling in a credit monitoring service that can notify you of possible fraudulent activity, especially if you suspect you've been targeted for identity theft.
- **Report the scam** to the Canadian Anti-Fraud Centre. Provide as much information to them as possible, such as names, phone numbers, and websites you were asked to visit.

Marketplace Scam

Online marketplace scams involve fraudulent activities where scammers exploit buyers or sellers through deceptive practices on platforms designed for commerce, such as eBay, Craigslist, Amazon, Facebook Marketplace, and various other e-commerce websites. These scams can take several forms, targeting either buyers, sellers, or both. Here are some common types of online marketplace scams:

For Buyers:

1. **Non-Delivery Scam:**

- The buyer pays for an item that is never delivered. The scammer may provide a fake tracking number to make it appear that the item is on its way.

2. **Non-Payment Scam:**

- The scammer provides a counterfeit payment confirmation or pretends to send payment through a fraudulent method, and the buyer receives nothing in return.

3. **Counterfeit Goods:**

- The buyer purchases a high-value item (like branded clothing, electronics, or luxury goods) and receives a counterfeit or inferior product.

4. **Phishing and Fake Websites:**

- Scammers create fake marketplace websites that look like legitimate ones. When buyers enter their personal and financial information, the scammers steal it.

5. **Bait-and-Switch:**

- The buyer is lured by an attractive listing at a low price, but once they engage, the scammer switches the product to something of lesser value or a different item altogether.

For Sellers:

- **Overpayment Scam:**
 - The scammer sends a check for more than the item's price and asks the seller to refund the difference. The original check bounces, leaving the seller out of the money they refunded.
- **Chargeback Fraud:**
 - The scammer pays with a stolen credit card or claims the item wasn't received after the legitimate transaction, then initiates a chargeback, leaving the seller without the item and the money.
- **Fake Payment Confirmation:**
 - The scammer sends a fake confirmation of payment (such as a fake PayPal email), convincing the seller to ship the item without having received actual payment.

General Tips to Avoid Scams:

- **Verify Buyers and Sellers:**
 - Check profiles, ratings, and reviews. Look for any red flags like new accounts or negative feedback.
- **Use Secure Payment Methods:**
 - Prefer platforms with secure payment systems (like PayPal or credit card transactions) that offer buyer/seller protection.
- **Avoid Wire Transfers and Gift Cards:**
 - Scammers often ask for these methods because they are hard to trace and non-refundable.
- **Be Cautious of Too-Good-to-Be-True Offers:**
 - Extremely low prices or unusually high payments are often indicative of a scam.

General Tips to Avoid Scams:

- **Communicate Within the Platform:**
 - Keep all communications and transactions within the platform's messaging and payment systems for better protection and dispute resolution.
- **Inspect Items Before Payment:**
 - For local transactions, meet in person and inspect the item before making payment. Use public, safe locations for meetings.
- **Report Suspicious Activity:**
 - Report any suspicious listings, buyers, or sellers to the platform administrators immediately.

Being aware of these common scams and practicing cautious behavior can significantly reduce the risk of falling victim to online marketplace fraud.

Cryptocurrency Scam

Cryptocurrency fraud happens by fraudsters misleading others in the world of digital money. These scam artists might promise big profits to get people to invest in fake coins or schemes. Sometimes, they use sneaky tricks like fake websites or emails to steal passwords and steal digital money from people's wallets. Because cryptocurrencies aren't closely watched like regular money, it's easier for fraudsters to cheat others, making it important for everyone to be careful and learn about staying safe in the crypto world.

Cryptocurrency fraud has been on the rise in recent years. In 2022, Canadians suffered \$308.6 million in losses due to investment fraud, a significant increase from the \$164 million reported in 2021, as revealed by the Canadian Anti-Fraud Centre. A notable portion of these cases involved Canadians falling victim to deceptive cryptocurrency advertisements.

Cryptocurrency scammers employ a range of tactics to deceive individuals. They instill a sense of urgency and exploit the fear of missing out on lucrative opportunities. Utilizing fabricated websites with counterfeit reviews and endorsements from well-known figures, along with fraudulent videos, they create an illusion of legitimacy for their investments.

These scammers utilize familiar communication channels such as misleading advertisements on social media, applications, and websites, as well as through phone calls, emails, and text messages. Their consistent promise revolves around the allure of significant returns on investment.

What distinguishes cryptocurrency scams is the intricate nature of digital finance and currencies. Many Canadians possess a limited understanding of cryptocurrency beyond recognizing it as a modern payment method. Exploiting this lack of knowledge, scammers manipulate individuals. With cryptocurrency being a trending topic, the desire to participate in this "action" attracts many. No one is exempt from the risk, and even businesses can fall prey to these schemes.

10 Most Common Cryptocurrency Scams:

- **Pump-and-dump, or rug pull**
 - Imagine a group of people talking up a new cryptocurrency, saying it's going to be the next big thing and urging others to invest in it quickly. This hype causes the price of the cryptocurrency to skyrocket. Once the price has risen significantly, the group sells off their own holdings at a profit. After they've made their money, they stop promoting the cryptocurrency, causing its price to plummet. This leaves those who bought in later with worthless coins and significant losses.
- **Giveaway scam, or 2-for-1 scam**
 - In a giveaway crypto scam, scammers pretend to be a famous person or a legitimate company offering a giveaway of cryptocurrency. They often use social media platforms or emails to reach out to people, claiming that if you send them a small amount of cryptocurrency, they'll send you a much larger amount in return as part of the giveaway. However, once you send them your cryptocurrency, they disappear with your money, and you never receive anything in return. It's like someone promising you a prize if you give them a little money upfront, but they never deliver the prize and run away with your cash instead.

- **Phishing scams**

- A phishing crypto scam is when scammers create fake websites or emails that look like they're from a legitimate cryptocurrency exchange or platform. They trick people into entering their login credentials, private keys, or other sensitive information by claiming there's a problem with their account or offering a fake reward. Once you enter your information on these fake sites or emails, the scammers use it to access your real cryptocurrency accounts and steal your funds. It's like someone pretending to be your bank and asking for your account details, but instead of helping you, they steal your money.

- **Airdrop scam**

- An airdrop crypto scam is when scammers pretend to give away free cryptocurrency tokens to attract attention and lure people into their scheme. They often promote these "airdrops" on social media, forums, or through emails. Here's how it typically works:
- **Promotion:** Scammers advertise that they're conducting an airdrop, claiming that if you send them a small amount of cryptocurrency or provide your personal information, you'll receive a much larger amount of free tokens in return.
- **Fake Airdrop:** Once you fall for the scam and send them your crypto or information, they either disappear without giving you anything, or they send you worthless tokens that have no real value.
- **Loss:** As a result, you end up losing your cryptocurrency or exposing your personal information to scammers, and you don't receive any of the promised free tokens.
- It's like someone promising you free money if you give them a bit of your own money first, but in the end, you get nothing in return and may even lose what you originally had.

- **Service provider support scams**
 - Service providers like cryptocurrency exchanges, wallets, and payment processors can sometimes support crypto scams, either intentionally or unintentionally. This happens when they have weak security, do not verify user identities, fail to monitor for suspicious activity, or provide poor customer support. Scammers take advantage of these weaknesses to steal money from people. To stay safe, it's important to use reputable services, enable security features, and research before investing.
- **Mining or staking pool scams**
 - Mining or staking pool crypto scams happen when scammers create fake pools, promising high returns. People invest their money or computing power, but the scammers disappear with the funds or never pay out the promised rewards. To avoid these scams, research the pool, look for transparency, and check reviews from other users.
- **Blackmail scams**
 - Blackmail crypto scams occur when scammers threaten to expose sensitive or embarrassing information about someone unless they pay a ransom in cryptocurrency. Scammers obtain personal or sensitive information about their target, such as private photos, emails, or financial details. They send threatening messages, stating they will expose this information publicly or to friends and family unless the victim pays a sum of money. Scammers demand that the victim pays the ransom using cryptocurrency, as it's harder to trace compared to traditional payment methods. They may use intimidation tactics, urgency, or fake deadlines to pressure the victim into paying quickly. Even if the victim pays the ransom, there's no guarantee that the scammers will delete the information or stop their threats.

- **“Pig butchering” or romance scams**

- "Pig butchering" crypto scams are a type of fraud where scammers build a fake relationship with their victims over time to gain their trust. Here's a simple breakdown:
- **Building Trust:** The scammer contacts the victim, often through social media or dating apps, pretending to be a friend or romantic interest.
- **Grooming:** The scammer spends weeks or months building a relationship, gaining the victim's trust.
- **Introducing Crypto Investment:** Once trust is established, the scammer talks about a supposedly lucrative cryptocurrency investment opportunity.
- **Initial Profits:** To lure the victim in, the scammer might show fake profits or even let the victim withdraw small amounts of money.
- **Large Investments:** Encouraged by these fake gains, the victim invests more money.
- **Disappearance:** Once the victim has invested a significant amount, the scammer disappears with the funds, leaving the victim with nothing.

- **Investment recovery pitch scams**

- Investment recovery scams target people who lost money before. Scammers promise to get back the lost money fast, asking for fees or personal information, such as banking information, upfront. After paying, they vanish or ask for more money, never delivering what they promised. It's important to be careful, check if recovery services are legit, and avoid giving out personal info until you're sure it's safe. To avoid these scams, be cautious of anyone promising easy recoveries and never pay upfront fees to unknown contacts.

- **Celebrity impersonation**

- Celebrity impersonation crypto scams happen when scammers pretend to be famous people, like actors or influencers, to trick others into sending them money or cryptocurrency. Scammers create fake social media accounts or emails that look like they belong to well-known celebrities. They use these fake accounts to promise unrealistic returns or exclusive deals involving cryptocurrencies. Scammers ask their targets to send them money or cryptocurrency, claiming it's for investments or donations. After receiving the funds, the scammers disappear, and victims never get the promised returns or benefits.

How to Protect Yourself from Cryptocurrency Scams:

- **Be skeptical!** If the offer sounds too good to be true, it probably is.
- **Don't act quickly!** Take time to do your research and verify all links. Fraudsters use high-pressure tactics to get consumers to react quickly.
- **Verify!** You can look up investment companies on the Canadian Securities Administrators' National Registration. You can check if a person or company has been flagged as a risk to investors by visiting the Investment Industry regulatory Organization of Canada website.
- **Never disclose confidential information!** Don't share your passwords, Social Insurance Number, address, or bank account with anybody under any circumstances.
- **Be cautious!** Don't answer random or "wrong number" texts from contacts you don't know.

2- Step Verification

What is 2-Step Verification?

2-Step Verification (2SV) is a security process that requires users to provide two different authentication factors to verify their identity. This is done by sending a 6-digit verification code through text message, email, or voice call for high-risk activities. This includes logging in from a new device, adding a new e-transfer recipient, editing an existing e-transfer recipient, and changing your password. By requiring two different types of authentication factors, two-step verification significantly enhances security by making it more difficult for unauthorized users to gain access to an account or system. It adds an extra layer of protection beyond just a password, mitigating the risk of unauthorized access due to stolen or compromised passwords.

In the credit union sector, the implementation of 2-Step Verification has yielded significant reductions in fraud losses. When employed solely during the initial login process, this security measure has led to a remarkable 50% decrease in fraud losses. However, its efficacy becomes even more pronounced when applied during high-risk transactions, resulting in an impressive 80% reduction in fraud losses. This underscores the pivotal role of 2-Step Verification in bolstering security measures within credit unions, thereby safeguarding member assets and enhancing overall trust in the financial institution.

How is 2-Step Verification being bypassed?

Two-step verification, designed as an added layer of security, can occasionally be bypassed through various sophisticated methods, including compromised email accounts, vishing, call center fraud, remote access scams and SIM card swapping. When an email account is compromised, attackers can intercept verification codes sent via email, gaining access to the target's accounts. Vishing, or voice phishing, involves fraudsters calling victims and manipulating them into revealing their verification codes or personal information. Call center fraud exploits human error and procedural weaknesses in customer service centers; attackers impersonate the victim and trick representatives into divulging information or changing account settings. Remote access scams deceive individuals into granting control of their devices to fraudsters, who then exploit this access to steal personal information, install malware, or demand payment for fake services. SIM card swapping is another tactic where the attacker convinces the mobile carrier to transfer the victim's phone number to a new SIM card under the attacker's control, thereby intercepting SMS-based verification codes. Thus, while two-step verification enhances security, it is not impervious to all forms of attack, necessitating continuous advancements and user awareness.

How can you protect yourself?

To protect yourself from two-step verification scams, it's essential to maintain vigilant cybersecurity practices. First, use reputable two-factor authentication (2FA) methods, such as authentication apps or hardware tokens. Regularly update and strengthen passwords, ensuring they are unique and complex for each account. Be cautious of phishing attempts by scrutinizing emails, texts, and phone calls for signs of fraud, and never share verification codes or personal information with anyone. Enable account alerts to monitor for unauthorized access attempts, and use security software to protect against malware. Additionally, contacting your mobile carrier to add an extra layer of security, such as a PIN or password for SIM card changes, can help prevent SIM swapping attacks. By combining these strategies, you can significantly reduce the risk of falling victim to two-step verification scams.

Online Marketplace Scam

Online marketplace scams are deceptive schemes where fraudsters create fake listings or misrepresent products on platforms like eBay, Craigslist, Kijiji, or Facebook Marketplace. They often use enticing prices or appealing descriptions to lure victims into making payments. However, once the payment is made, the victim either receives nothing at all or a counterfeit or inferior item.

Common tactics include:

- **Fake Listings:** Scammers create ads for products that don't exist or that they don't intend to deliver.
- **Misrepresentation:** They may advertise a product as genuine or in good condition when it's actually damaged or fake.
- **Overpayment Scam:** They send a fake payment for more than the item's price and ask for the difference to be refunded, leaving the seller out of pocket when the original payment is found to be fake.
- **Phishing:** They send messages pretending to be from legitimate marketplace websites to steal personal information or login credentials.

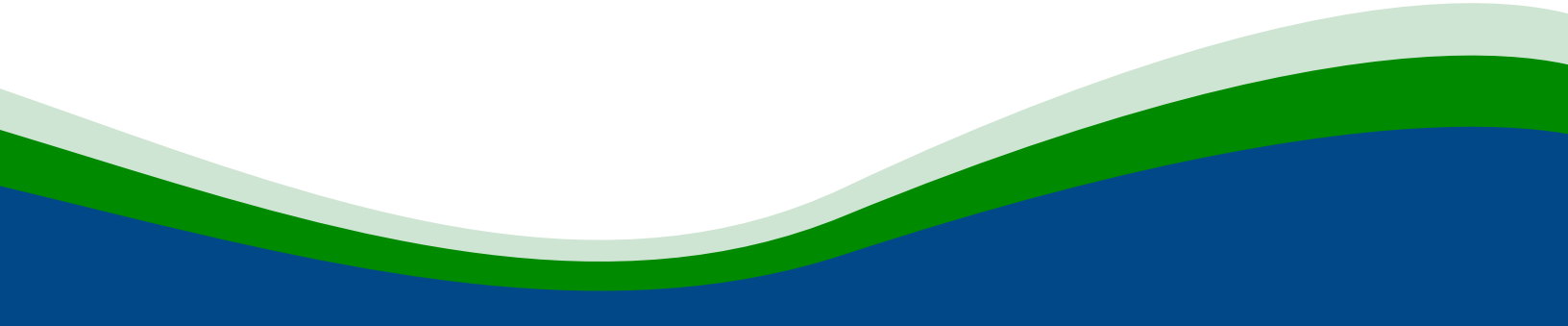
General Tips to Avoid Scams:

- **Verify Buyers and Sellers:** Check profiles, ratings, and reviews. Look for any red flags like new accounts or negative feedback.
- **Use Secure Payment Methods:** Prefer platforms with secure payment systems (like PayPal or credit card transactions) that offer buyer/seller protection, if those are not available insist on paying cash. Never eTransfer, especially prior to seeing or picking up an item.
- **Avoid Pressure:** If someone is rushing you to pay or ship, take a step back.
- **Avoid Wire Transfers and Gift Cards:** Scammers often ask for these methods because they are hard to trace and non-refundable.
- **Be Cautious of Too-Good-to-Be-True Offers:** Extremely low prices or unusually high payments are often indicative of a scam.
- **Communicate Within the Platform:** Keep all communications and transactions within the platform's messaging and payment systems for better protection and dispute resolution.
- **Inspect Items Before Payment:** For local transactions, meet in person and inspect the item before making payment. Use public, safe locations for meetings.
- **Report Suspicious Activity:** Report any suspicious listings, buyers, or sellers to the platform administrators immediately.

Being aware of these common scams and practicing cautious behavior can significantly reduce the risk of falling victim to online marketplace fraud. **Be cautious of sending funds for an item before pick up**, instead ask to pay for the item once you have been able to see and examine it. **Remember to stop, take a moment to think, and follow your instincts.** If the offer seems too good to be true, it probably is!



What to do if you believe you have been scammed:

- **Call your Credit Union** and other financial institutions.
 - **File a police report.** Most police departments allow you to report frauds online by visiting their website.
 - **If your credit card number is compromised,** call your credit card company.
 - **If you have released any personal information,** contact Equifax at 1-877-227-8800 and TransUnion at 1-800-565-2280.
 - Report the scam to the to the website where you found the fraudulent posting.
- 

Credit & Debit Card Fraud

Debit card fraud occurs when someone illegally gains access to your debit card details and uses them to make unauthorized transactions, often draining your bank account.

Credit card fraud involves the unauthorized use of your credit card for purchases, either online or in-person, or to take out cash advances. These types of fraud can result in financial losses, identity theft, and damage to an individual's credit reputation.

Common Types of Debit Card Fraud:

- **Card Skimming:** Thieves use a small device (skimmer) to capture your card's information when you swipe it at an ATM or point of sale terminal (POS).
- **Phishing:** Fraudsters may pose as legitimate organizations (e.g. credit unions, banks) and attempt to trick you into giving away your debit card details, such as your confidential 4 digit PIN, via phone, email, or text.
- **ATM Fraud:** Criminals may install fake keypads or cameras on ATMs to record your PIN or card details.
- **Lost or Stolen Cards:** If your debit card is lost or stolen, and someone uses it to make unauthorized purchases, this is a form of fraud.

Common Types of Credit Card Fraud:

- **Stolen Card Information:** Criminals may steal physical credit cards or the card details (card number, expiration date, CVV) and use them for unauthorized transactions.

- **Account Takeover:** Fraudsters gain access to your credit card account, change the contact details, and make fraudulent purchases.
- **Online Fraud:** This happens when someone makes unauthorized online transactions using stolen card details (e.g., data breaches or phishing scams).
- **Card Not Present (CNP) Fraud:** Occurs when fraudsters use stolen card information to make online or phone purchases where the physical card is not required.

How to Identify and Respond to Scams:

- **Hang up and call the financial institution directly:** If you receive a suspicious call, hang up and contact your financial institution or credit card company using the official phone number found on your account statement or their website. This ensures you're speaking with a legitimate representative.
- **Never share personal information over the phone:** Do not provide your account numbers, PINs, passwords, or credit card details to anyone over the phone, especially if you didn't initiate the call.
- **Verify any claims of account issues:** If someone claims there is suspicious activity or a security issue with your account, ask for details in writing or through official communication channels.
- **Use two-factor authentication:** Enable two-factor authentication (2FA) on your online accounts and credit cards for an extra layer of security, making it harder for fraudsters to access your information.
- **Report any suspicious activity:** If you believe you've been targeted by a scam or have provided personal information to fraudsters, immediately report it to your financial institution and local authorities to minimize potential damage.

Recently, the Durham Regional Police have seen an increase in a new scam involving debit cards and credit cards that is targeting seniors, this scam is known as a “banking fraud” or “carding scam.” This scam involves fraudsters pretending to be representatives from a victim's banking or credit card company, claiming that their accounts have been compromised. The scammers create a sense of urgency and convince the victims to hand over their ATM cards, PINs, or passwords. They send a courier to collect these items from the victims' homes, which are then used for fraudulent purchases. The victims, believing they are resolving a security issue, unwittingly provide the information, leading to financial theft. This type of scam relies on manipulation and the victim's trust in authority figures. Instead of trusting unsolicited calls from anyone claiming to be from your financial institution or credit card company, it's important to be cautious and take the above mentioned steps

Prevention Tips for Both Debit and Credit Card Fraud:

- **Use Strong, Unique Passwords:** Protect your online accounts with strong passwords, including multi-factor authentication (MFA) where possible.
- **Monitor Statements:** Regularly check your financial institution or credit card statements for any unauthorized transactions.
- **Report Lost or Stolen Cards Immediately:** If your card is lost or stolen, report it immediately to your financial institution or issuer to prevent further unauthorized transactions.
- **Avoid Public Wi-Fi for Financial Transactions:** Do not enter sensitive information when using unsecured public networks.
- **Shred Documents:** Shred any documents containing your card information before disposal.

- **Enable Alerts:** Many financial institutions and card issuers offer transaction alerts that notify you of purchases or suspicious activity.
- **Use Secure Websites:** Ensure that websites are secure (look for "https://" and a padlock icon) when making online transactions.
- **Be Cautious of Phishing Scams:** Be wary of unsolicited emails, calls, or texts requesting card details.

What to do if you have been scammed:

- **Contact Your Credit Union or Card Issuer Immediately:** Report the fraud to stop further transactions.
- **Dispute the Charges:** If fraudulent charges appear, dispute them with your financial institution or credit card company.
- **File a Police Report:** In some cases, filing a report with the police may be necessary, especially if you've been the victim of identity theft.
- **Monitor Your Credit:** Consider checking your credit report regularly to ensure there are no unauthorized accounts or activities. You can contact Equifax at 1-877-227-8800 and TransUnion at 1-800-565-2280.
- **Place a Fraud Alert:** You can place a fraud alert or credit freeze on your credit file to protect yourself from identity theft.

Gift Card Fraud

Gift card fraud is a prevalent and increasingly sophisticated form of financial scam where criminals exploit the popularity and convenience of gift cards to steal money from unsuspecting victims. Scammers often prefer using gift cards in their schemes due to their anonymity, ease of use, and difficulty in tracking or reversing transactions. A growing trend involves manipulating the barcode on the back of the card, making both consumers and retailers victims. Gift cards are easily accessible both in stores and online, with those from popular companies like Amazon and Apple being accepted globally. In these scams, fraudsters exploit the information encoded in the barcode or magnetic strip, allowing them to access the card's value without needing the physical card.

Fraudsters often buy large quantities of gift cards from retailers like Apple, Google Play, or Amazon, either in-store or online. In physical stores, they may use devices to skim barcodes or serial numbers from the cards without detection, while in some cases, they steal barcode information by hacking websites or intercepting emails. Once they have the barcode or serial number, scammers can redeem the funds online or sell the information on the black market. Victims may unknowingly purchase compromised cards from third-party sellers or be tricked into scanning and sending the barcode details to the scammer, who can then use the funds before the victim tries to redeem the card.

Detecting a Barcode Manipulation Scam

- **Check for Tampering:** If you're buying a physical gift card, carefully inspect the packaging and back of the card for signs of tampering, such as scratches, missing security seals, or unusual marks near the barcode.
- **Scan the Card Before Use:** If possible, use a retailer's official app or website to scan the card and check its balance before using it. Many retailers allow users to check card balances online, so it's a good idea to verify before using or giving the card away.
- **Beware of Online Deals:** Avoid purchasing gift cards from unfamiliar websites or resellers. Stick to trusted sources like the retailer's official site or reputable third-party vendors.
- **Confirm Gift Card Number:** Before leaving the store you purchased the gift card from, confirm the number on the gift card matches the gift card number shown on your receipt.

Preventing Barcode Manipulation Scams

- **Buy From Trusted Sources:** Always purchase gift cards directly from the retailer or from authorized third-party vendors. Avoid buying cards from online auction sites, unverified sellers, or stores with poor reputations.
- **Inspect Gift Cards:** Before purchasing, check the back of the card for any signs of tampering, including altered or missing barcodes or numbers.
- **Avoid Scams Asking for Card Details:** Never share gift card details (barcode or PIN) with anyone, especially if they're pressuring you to do so quickly. Legitimate companies and friends will never ask you to pay for things via gift cards.

What to Do If You Are Scammed

- **Report to the Retailer:** If you suspect your gift card was tampered with or the barcode was compromised, contact the retailer immediately. Some retailers may be able to trace the card's activity and freeze the funds before they're entirely drained.
- **File a Complaint:** Report the scam to authorities or consumer protection agencies. In Canada, report scams to the Canadian Anti-Fraud Centre. You can also file a police report with your local police station.
- **Monitor Your Accounts:** If you have shared sensitive information (such as credit card details) with the scammer, monitor your accounts for suspicious activity.