Fraud Prevention Tips:
E-Transfer Scams

An e-transfer scam or interception happens when a fraudster gains unauthorized access to an e-transfer recipient's email account or phone number. With this access, the fraudster can use the deposit link to redirect the funds into their accounts if they answer the security question correctly.

How to protect yourself:

- **Register for Autodeposit** – This allows you to have your e-transfer money automatically deposited into your accounts without having to answer a security question, making it more difficult for fraudsters to intercept the transfer.
- **Secure your questions** – Choose a security question with an answer that is difficult to guess or discover and share this answer with the recipient in person or via phone call. Never share the security answer in the e-transfer message area, over text or email.
- **Beware of unexpected transfers** – If you receive a deposit notification that you weren't expecting, contact the sender through a different channel to confirm the transfer is real. Do not click any links in an e-transfer notification from a sender you don't recognize.
- **Don't overshare on social media** – Be mindful of what you're sharing on social media. Fraudsters may be able to find relevant information about you to answer e-transfer security questions.

If you suspect to be the target of a financial scam, please reach out to your local Vision branch for support and report the fraudulent activity to local police and the Canadian Anti-Fraud Centre at 1-888-495-8501.

VISION
CREDIT UNION
We see banking differently.

Fraud Prevention Tips:
Phone Scams

Phone scams can take many forms, but fraudsters always have the same objective — get your money or personal information to commit identity theft. To do this, scammers may act friendly and helpful or they might threaten or try to scare you. Since they usually follow similar patterns, it's important to know how to identify a phone scam.

How to tell if it's a phone scam:

- **There's no prize** – A caller might say you were selected for an offer or that you've won a prize and ask you for personal information to claim it – **don't give it.** Also use caution if the caller asks you to pay for a prize, as this means it's not a prize.
- **They are threatening you with law enforcement** – Scammers often pretend to be law enforcement or government agencies to threaten you with deportation, arrest or a fine if you don't pay a debt. Real law enforcement agencies will not do this.
- **You feel rushed to accept an offer** – Legitimate businesses will give you time to make decisions on offers. Fraudsters will tell you it's urgent and to act fast but don't be pressured to decide on the spot.
- **They ask to send cash or pay with a gift card** – Fraudsters want you to pay in a way where it's hard for you to get your money back, so they often tell you to wire money or put money on a gift card or prepaid credit card.
- **They ask for your personal information** – Never give out personal information like a SIN number or account details to someone you don't know. When in doubt, hang up and call the actual source yourself.

If you suspect to be the target of a financial scam, please reach out to your local Vision branch for support and report the fraudulent activity to local police and the Canadian Anti-Fraud Centre at 1-888-495-8501.

VISION
CREDIT UNION
We see banking differently.

Fraud Prevention Tips:
Cryptocurrency Scams

Cryptocurrency has been gaining momentum in the last few years with more investors wanting to invest. Cryptocurrency investors may be less careful with their investments due to the nature and newness of the asset, causing a ripe environment for scammers.

Most common cryptocurrency scams:

- **Fake ICOs** – A fake initial coin offering (ICO) scam is when a new cryptocurrency pops up and claims investors will make "huge gains" when, in reality, the scammers eventually disappear with the investment funds.
- **Fraudulent wallets** – Fraudulent cryptocurrency wallets and exchanges are known to appear in mobile app stores, imitating a legitimate crypto brand to steal users' data, login information or private keys (keys required to access funds within a wallet).
- **Fake emails** – In the crypto world, phishing emails will usually target crypto wallet private keys where the fraudster will send emails with links directing the individual to a website asking for private key information to enable a transfer.
- **Social media scams** – Fraudsters often create imposter or fake accounts on social media where they pretend to be a cryptocurrency brand, celebrity or known figure in the cryptocurrency space. These accounts provide "hot tips," giveaways or other offers with false promises and unrealistic results.

If you suspect to be the target of a financial scam, please reach out to your local Vision branch for support and report the fraudulent activity to local police and the Canadian Anti-Fraud Centre at 1-888-495-8501.

VISION CREDIT UNION
We see banking differently.

Fraud Prevention Tips:
Romance Scams

Romance scams happen when a fraudster adopts a fake online identity to gain an individual's affection and trust by connecting with them for long periods to build a connection. Ultimately, the new-found "friend" will ask the victim for money and then never speak with them again.

Tips to avoid romance scams:

- **Go slow and ask questions –** Be suspicious if an individual seems too perfect, asks you to leave a dating site or social media site to communicate directly or avoids personal questions or answers with things that don't add up.
- **Play detective –** Research the person online to see if their profile photo and information can be found elsewhere online and keep an eye out for inconsistencies.
- **Never send money to someone you've never met –** Scammers will ask for money to help a sick family member, to pay for a personal emergency or for travel expenses to come visit you, but disappear after the money has been sent.
- **Talk to someone you trust –** Beware if your new online friend attempts to isolate you from loved ones. You might not see the flaws in a new online friend, but someone you trust might be able to help you.
- **Pay attention to excuses –** If the individual promises to meet you in person but always has an excuse not to at the last minute, you have good reason to be suspicious.

If you suspect to be the target of a financial scam, please reach out to your local Vision branch for support and report the fraudulent activity to local police and the Canadian Anti-Fraud Centre at 1-888-495-8501.

VISION
CREDIT UNION
We see banking differently.

Fraud Prevention Tips:
AI Scams

Fraudsters are using artificial intelligence (AI) to target folks for identity theft and other scams. This includes using AI to mimic loved ones' voices, create deepfake videos that look and sound like people we trust and tailor messages to seem more authentic and convincing.

How to stay safe from AI scams:

- **Check for unnatural language** – AI-generated scams often come with awkward phrasing, unnatural tone or small grammar mistakes. Look for robotic language that seems odd.
- **Be wary of impersonation** – AI can mimic voices or writing styles to sound like someone you trust. If you're in doubt if a call, email or text is legitimate, contact the individual directly through a trusted method to confirm. It wouldn't hurt to create a code word with loved ones to be extra safe!
- **Watch for phishing links in emails or messages** – Examine the sender's address and never click links or download attachments unless you're certain they're safe!
- **Always trust your instincts** – If something feels off, don't ignore it. Your intuition is probably right and there's never any harm in double-checking the legitimacy of a message before acting.

If you suspect to be the target of a financial scam, please reach out to your local Vision branch for support and report the fraudulent activity to local police and the Canadian Anti-Fraud Centre at 1-888-495-8501.

VISION
CREDIT UNION
We see banking differently.