CIBC

CIBC PRIVATE WEALTH

WOOD GUNDY

SCAM TIP SHEET

As technology increasingly becomes a greater part of our lives, everyone needs to stay vigilant of the risks they face on all digital platforms. Fraudsters continually create new and evolving schemes aimed at illegally obtaining and exploiting victims' personal information, with the goal of financial gain.
CIBC is committed to keeping you and your banking information safe and providing you with information about the risks that may affect you.

The basis of many scams

Fraudsters use social engineering tactics in order to take advantage of and obtain confidential information from victims. Tactics are often in the form of suspicious emails, calls and text messages that may impersonate family members, friends, government agencies and financial institutions. Once fraudsters obtain confidential information, they will use it to commit financial fraud and deplete their victims' funds.

Social engineering:
The use of psychology to manipulate our human instinct to respond to urgent requests and fear, so that victims are lured into revealing confidential information that may be used to commit financial fraud.

Here are three key characteristics of social engineering techniques:

1. **Using fear as a motivator** by sending threatening emails or texts, or making phone call to scare you into revealing information or conducting transactions
2. **Urgent and unexpected requests** for personal or business information through written communications, such as email or text messages
3. **Offers, prizes or contests that sound too good to be true,** often claiming to provide a reward in exchange for login credentials or other personal or business information

Know the signs

Red flags that may indicate you are dealing with a fraudster

Requests to conduct a wire transfer or pay using untraceable methods.
Scams typically request victims to wire money electronically such as through *Interac* e-transfer, purchasing prepaid gift cards, or the transfer of cryptocurrencies, due to their nature of being untraceable and often irreversible once sent.

An offer that sounds too good to be true.
Promotions, investment opportunities, or sales that sound too good to be true, are likely as such. Fraudsters want you to act quick to a time sensitive deal or a "once in a lifetime" opportunity that does not exist so that you are pressured to conduct transactions or provide information without considering whether the offer is legitimate.

Suspicious and unsolicited emails, text messages or telephone calls.
Be skeptical of unexpected calls, emails or text messages from individuals or entities claiming you owe taxes, your accounts have been suspended or compromised, or other suspicious claims. These communications purposely instill a sense of urgency and lure you into clicking a suspicious link that can download malware onto your devices, or providing sensitive information, such as your social insurance number. Take note of spelling or grammar errors, and email and web addresses and examine whether there are subtle mistakes or differences.

You've been overpaid.
When receiving a payment, be cautious of individuals or entities who have overpaid you and have asked you to send back the difference. A fraudster may give you a counterfeit cheque for an amount greater than discussed and ask you to deposit the cheque and wire back the excess funds. Once the money is sent back, the fraudster will cease all communication before the cheque bounces back, leaving you on the hook for the money withdrawn and out of the money transferred.

How CIBC protects your account with two-step verification

Two-step verification is an extra layer of security that lets us confirm your identity and make sure you're the only one using your account. We've replaced Personal Verification Questions with one-time verification codes. This means you may be asked to enter a unique code when you complete certain online activities instead of answering security questions.

How one-time verification codes work:

1. **Ensure your contact information is up to date.** You can choose to receive your verification codes by text or voice call. You may also choose to receive your code by email, only if your email address is associated with a corporation or educational institution.
2. **To complete certain transactions on your account, you will be prompted to enter a verification code.** Certain transactions such as resetting your password or changing your security contact information will require you to enter a one-time verification code. Whenever you receive a prompt for a verification code, follow these steps:

   a. Choose your preferred contact method
   b. Enter the verification code within 10 minutes of receiving it

3. Remember that each code is unique, can only be used once and should never be shared with anyone. For extra security, you can choose to receive a verification code every time you sign on to Mobile or Online Banking. Fraudsters frequently attempt to intercept these codes.

Common types of scams

Business Email Compromise

This happens when fraudsters send an email appearing to be someone you know and trust — typically a colleague, manager or vendor – by using a slight variation of the original email address. The email seems like a legitimate request that tricks you into transferring money to the fraudster or sharing confidential information. Fraudsters rely on impersonation and social engineering tactics to carry out different versions of the scam.

Types of business email compromise scams:

- **Fake invoice scam:** The fraudster impersonates a vendor the business regularly deals with and sends an invoice with updated banking information.
- **Fake boss scam:** The fraudster impersonates a manager and asks an employee to purchase multiple gift cards for clients. The fraudster requests the employee to send the gift card serial numbers as soon as possible.

Warning signs:

- Urgent requests that are brief and encourage you to avoid normal procedures
- Grammar and spelling errors or design inconsistencies
- Language that's unusual for a vendor
- Emails from personal accounts, like Gmail or Yahoo, instead of an organization's account
- Emails are sent from a high-level executive who asks for information that seems strange.

Tips to stay safe:

- Don't click on anything in an unsolicited email that asks for information. Search for the company on your own and ask them if the request is legitimate.
- Be diligent about what you download. Don't open an email attachment from an unknown sender and be wary of business emails forwarded to you.
- Verify any payment or purchase requests or updates by calling the person on a known number to ensure it's valid.

Romance scams

A fraudster creates a fake social media or online dating profile and reaches out to you. They develop a relationship with you solely through online communication and always avoid meeting face to face. The fraudster shares invented tales of hardship, such as needing life-saving surgery or having legal troubles, and they'll ask you for money to help them. After they receive your money, the fraudster will either continue creating stories for more money or will cut off all contact with you.

Warning signs:

- The fraudster tends to communicate in a very reassuring manner to get you to trust them
- The fraudster quickly professes their love for you and avoids face-to-face interactions
- Their online profile is a new account that lacks much of an online presence
- The fraudster claims they need financial assistance for emergency situations
- You may be called by the wrong name, as the fraudster interacts with several targets at the same time

Tips to stay safe:

- Always keep personal and business information confidential.
- Don't feel pressured or rushed to send money to someone you've met online. Only send money to people you're familiar with and have met in person.
- Never share your personal or financial information with anyone, especially online. Fraudsters will try to get this data to get money.
- When developing a connection with people online, investigate their profiles and online presence to find out if they're who they claim to be.
- Search Google Images to see if their profile picture appears on the internet under another name.

Cryptocurrency scams

There are many different cryptocurrencies, including some well-known ones, such as Bitcoin and Ethereum, and also new ones that are constantly being created. Fraudsters use a variety of scams to target you into purchasing and sending cryptocurrency as a form of payment or as an investment opportunity.

Common types of cryptocurrency scams:

Crypto-only payments
A seemingly credible person or business demands a payment with cryptocurrency. They may claim they don't accept any traditional forms of payment, such as credit and debit card payments. Fraudsters demand cryptocurrency as a form of payment because the funds become hard to trace.

Investment schemes
Fraudsters try to lure you in with fake cryptocurrency investment opportunities. The fraudster says this is a once-in-a-lifetime prospect, limited time deal, a guaranteed high return or no risk opportunity. The fraudster will make you believe your investment is doing well, but you'll never receive your money back.

Phishing
Fraudsters use phishing to get your digital wallet private key and steal your cryptocurrencies. They send mass emails in hopes that you click on the attached link and share your personal and banking details.

Warning signs:
- Promises of free money
- Vague details about where your investment funds are going
- Someone you don't know shares a cryptocurrency investment opportunity that's too good to be true
- You're advised that a cryptocurrency investment would have no risk and a guaranteed high return
- A celebrity or social media influencer promotes a cryptocurrency investment opportunity
- Misspelled words and grammatical errors in any communication you receive, such as an unsolicited email or social media post.

Tips to stay safe:
- If you're told to pay with cryptocurrency, it's most likely a scam. Credible institutions won't force you to pay with cryptocurrency.
- Don't click on any links or attachments from suspicious emails, text messages or social media.
- Don't feel pressured to invest quickly. Take your time to understand where your money is going.
- If you have cryptocurrency stored in a digital wallet, protect the private key and don't give it out to anyone.

Timeshare Resale scams

Fraudsters will call or email pretending to be a reseller or real estate agent looking to gain business by helping you sell your timeshare. They will make false claims, such as having a buyer lined up and ready to make a deal or will guarantee that they can sell quickly with a high profit margin. The fraudster may seem professional and provide fake documents that look legitimate, and will ask you to provide your credit card information or pay upfront fees by wire transfer. The fraudster will take your money and the deal will never close.

Warning signs:
- You're unexpectedly contacted by telephone or email and are offered to sell your timeshare
- They promise your timeshare will sell quickly with a high profit margin
- You're asked to pay for various fees before selling your timeshare, including maintenance fees and taxes.

Tips to stay safe:
- Confirm the reseller or real estate agent is licensed and legitimate by researching them online, viewing their website, and reading client reviews. You can also ask the reseller to provide their proof of licensing and ask for references from satisfied clients.
- Do not pay upfront fees. Use a reseller that offers to receive the selling fee after the timeshare has been sold.
- Carefully read the contract and ensure it matches with what you've been told before signing.

Bank Impersonator scams

Fraudsters call their victims and pretend to be a bank representative investigating an ongoing fraud case that has been committed by a banking centre employee. The fraudster asks the victim for their participation in the undercover case in order to catch the employee. The victim is advised not to tell anyone else about the investigation due to its confidentiality and avoiding "tipping off" the suspicious employee. In some cases, victims are promised a form of compensation for their participation. To participate in the investigation, fraudsters pretend to deposit money into the victim's bank account, often through fraudulent cheques, making victims believe the funds are real. The victim is advised to use those funds to send a wire transfer or purchase gift cards and provide the card information back to the fraudster in order to help with the case.

Warning signs:

- You're asked not to tell anyone about the investigation
- You're asked to provide your one-time verification code
- The bank investigator asks for your personal information, bank account information or online banking password
- You receive funds in your account as part of the investigation
- You're asked to purchase gift cards and provide the card information to the investigator or wire transfer a large sum of money.

Tips to stay safe:

- CIBC will never ask you to provide your online banking password, PIN, one-time verification codes or to withdraw money from your account. Never share your passwords and verification codes with anyone.
- CIBC or a law enforcement organization, such as the RCMP, will never ask you to assist with an undercover fraud investigation
- Do not always trust your caller ID. Fraudsters may use call spoofing software that makes it seem like the call is coming from a legitimate CIBC phone number.
- If you receive a call claiming to be from CIBC and it seems suspicious, hang up and contact CIBC using the phone number listed on the back of your bank card.

What can I do if I'm a victim?

Follow the steps below immediately to avoid further losses and being a repeat victim:

Review all of your CIBC products to identify any unauthorized activity. If there's suspicious activity in your Wood Gundy account, contact your investment advisor or call Client Relations at 1 800 387-2979.

Additional steps:

- Contact credit reporting agencies to request a fraud alert be placed on your file. This will notify companies not to issue credit to anyone applying under your name without verification.
- Install reputable antivirus software on your computer and run full scans regularly to remove any viruses.
- Change passwords, including your online banking password and email address passwords on a clean device (i.e. a device free of malicious software).
- Check email and telephone message forwarding and redirection settings to ensure there are no rules set that were not made by you.