Client protection playbook

Common types of scams you should be aware of and how to protect yourself

Book 3 of 3

Table of contents

Message from Keith Gordon

Executive Vice President & Chief Security Officer,
Canadian Imperial Bank of Commerce (CIBC)

Technology plays a big role in our everyday lives - from checking our bank account balances online to streaming our favourite movies. With the advancement of technology, it brings about extraordinary benefits to our lives and shapes the world we live in. At CIBC, we continuously embrace new technology and security features that help make your ambitions a reality by protecting your money and information.

With technology evolving, so are the strategic tactics of fraudsters. According to the Canadian Anti-Fraud Centre and the Federal Trade Commission, North Americans lost just over $6 billion to fraud last year. Since the pandemic began, the global volume of online transactions has increased significantly, and while that's been convenient for consumers and essential for businesses, it's also created an ideal environment for fraud to escalate. Fraudsters are constantly trying to find new ways to scam people out of money and obtain their personal and banking information. At CIBC, we work around the clock to stop fraudsters and keep our clients safe.

Cyber security impacts everyone and cyber security threats represent one of the most significant risks that financial institutions face today and require constant vigilance and improvement to stay ahead in the current environment. As such, CIBC regards information & cyber security as a core capability. The protection of our systems and information is one of our strategic objectives and is part of our organizational DNA. We're constantly improving how clients can bank safely and securely - but the first line of defense starts with you.

Increasing your fraud knowledge decreases your chances of falling for a scam. Knowing how to prevent, identify and respond to fraud is essential for your defense against fraud. As fraud comes in many different forms, it's important to understand different tactics fraudsters use to try to trick people. Use this playbook as a guide to enhance your fraud knowledge, as you'll learn how to identify common types of scams and tips to protect yourself, so you'll know a scam when you see one.

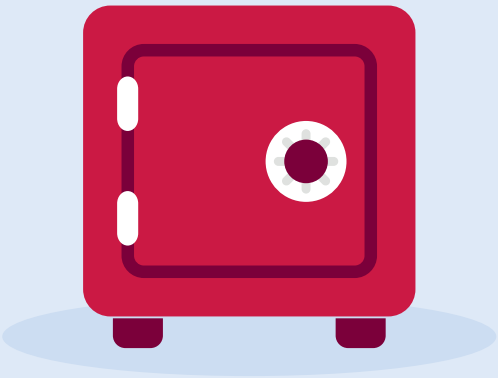
Let's work together and keep everyone safe.

Keith Gordon

Background information on scams

With the ongoing enhancements to technology, social media, and e-commerce, personal and banking information is at risk of being stolen every day. 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.



so·cial en·gi·neer·ing
/ˈsōSHəl ˌenjəˈni(ə)riNG/

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.

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.

Here are three key characteristics of social engineering techniques:

Using fear as a motivator by sending threatening emails, phone calls or texts to scare you into revealing information or conducting transactions.

Urgent and unexpected requests for personal or business information through written communications, such as email or text messages.

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 send money 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. Beware of requests to transfer money electronically.

Suspicious and unsolicited emails, text messages or telephone calls

Be skeptical of calls, emails or text messages from individuals or entities claiming you owe taxes, your accounts have been suspended or compromised, your package delivery has been missed, you have unauthorized charges on your credit card, or that you are being offered a job that offers high pay for little to no work. 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, driver's license or bank accounts. Take note of spelling or grammar errors, and email and web addresses and examine whether there are subtle mistakes or differences.

An offer that sounds too good to be true

Promotions, investment opportunities, or sales that sound too good to be true, are likely just that. Fraudsters want you to respond quickly 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.

Buyers want to overpay you

When selling items online, be cautious of buyers who overpay you for an item and request you to send back the difference or ask you to cover the transportation costs, promising to reimburse you after the product is delivered. A fraudster may send you a counterfeit cheque for an amount greater than the price you advertised and ask you to deposit the cheque and wire the excess funds immediately back to them. Once sent to the fraudster, they will cease all communication before the cheque bounces, leaving you on the hook for the deposited and out of the money transferred.

Online best practices:

Keep your money and your information safe by following the best practises below

- Do not share One-Time Verification Codes (OTVC) with anyone.
- Set up *Interac* e-Transfer Autodeposit to ensure funds sent to you are automatically deposited into your bank account.
- Never click on an attached link inside an email to visit a website – type the address into your browser instead.
- Keep your passwords secured offline, or in a reputable password manager.
- Do not respond to or click on pop-up messages claiming your computer is at risk.
- Check monthly banking statements regularly for any unauthorized charges.

How CIBC protects you from identity theft and fraud

CIBC and other legitimate entities will never contact you and ask you directly for your personal or banking information – do not share these details with those claiming to be from legitimate companies.

Enroll in CIBC's MyAlerts on mobile or online banking to monitor suspicious activity on your banking accounts.

Sign up for CIBC's voice verification security feature to bank faster, securely, and protect yourself from fraud. *Must be 13 or over to enroll (Quebec: must be 14 or over).*

Opt-in to CIBC's push notifications on mobile banking to receive One-Time Verification Codes (OTVC) when conducting high-risk transactions.

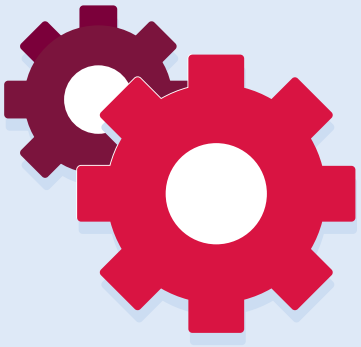
Identity theft

How it works

Identity theft is the act of stealing someone else's identity and personal information. Fraudsters commonly attempt to steal the personal or banking information of their victims through three main methods:

1) **SIM jacking**;
2) **phishing**; and
3) **malware**.

Once the victim's identity is stolen, scammers use it for illegal purposes and conducting financial transactions, a process known as identity fraud.



What it is:	Red flags to look for:
SIM jacking After stealing the victim's personal information using malware or phishing tactics, the fraudster calls their cell phone service provider and poses as the victim to switch the mobile number to a SIM card the fraudster owns	✕ A sudden loss of service connection to your cell phone ✕ A text message from your service provider stating that a request was made to transfer your number to another SIM card
Phishing / Vishing / Smishing Unsolicited contact from fraudsters who pose as government agencies or other institutions requesting payment or personal information, via email (phishing), voice over telephone (vishing), or text messages (smishing)	✕ Requests for money or personal / banking information ✕ Misspelled email addresses or addresses that have an unusual combination of characters and poorly written messages ✕ Urgent demands, with threats for not complying
Malware Short for malicious software, it is designed to gain unauthorized, remote access to a device's files and disable the user's access to them or track the user's keystrokes. Examples of malware include keyloggers, ransomware, adware and spyware	✕ Pop-up windows claiming your computer is at risk, directing you to install antivirus software via a clickable link ✕ Your files have been locked, and you are required to pay a ransom to regain access ✕ You cannot login to frequently used accounts (banking, email, social media, etc.)

Protect yourself from identity theft

1. Identify any red flags

Identity theft is not always easy to spot until after it has already occurred. **Spot the signs of identity theft early** to ensure action can be taken as soon as possible:

- Suspicious and unexpected messages or calls, asking you to conduct financial transactions or provide personal information
- Messages claiming you have won a prize for a contest you never entered, or messages about offers that sound too good to be true
- Threats, fearmongering, or urgency in messages or calls, in an attempt to persuade you to act quickly
- Requests to send funds via wire transfers, gift cards, prepaid cards, Bitcoin and other cryptocurrencies

2. Dig deeper

Closely examine the characteristics of an email or text message you are uncomfortable with, such as the tone and grammar, the subject line, and the email address of the sender. If there are multiple grammatical errors and the email address is an unusual combination of letters and characters, the message may be a fraudulent one. Furthermore, be wary of messages claiming to be from a government agency or the financial institution you bank with, urging you to click a link to confirm personal or transaction details: **if faced with such a message, ignore the message or call your financial institution to confirm.**

3. Slow down. Don't rush.

Fraudsters are demanding and want you to act quickly. Maintain control of any situation by slowing down; think carefully about what is being asked of you and whether it makes sense. Investigate any requests for personal information and verify that it is legitimate before sharing.

4. Be cautious

The best defense against identity theft is to monitor your online presence and be careful about what and how much you share. The more information fraudsters know about you, the more successful they can be at swindling you. Always create unique and difficult passwords for each of your online accounts, install up to date software on your PC to detect and remove malware, and do not respond to unsolicited emails or text messages that ask you to click on a link or provide personal information.

CIBC is committed to keeping you and your banking information safe. To learn more about how you can protect yourself from being a victim of identity theft, visit www.cibc.com/fraud and click on our Protect yourself from identity theft reference guide.

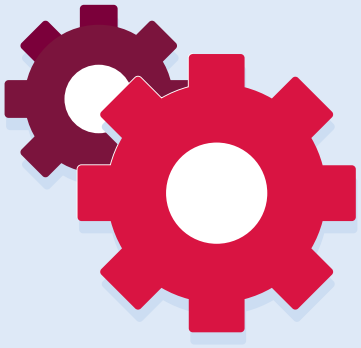
5. Verify with a trusted individual

When in doubt, always reach out! Contact a trusted family member or friend about your situation for a second opinion on messages, calls or other forms of unsolicited contact that you are not sure are legitimate. If you are still unsure, deny any requests for personal information and contact CIBC by calling the number on the back of your card.

Interac e-Transfer interception fraud

How it works

In *Interac* e-Transfer interception fraud, fraudsters are able to intercept an *Interac* e-Transfer that is being sent from one individual's bank account to another by gaining access to the recipient's email address or text messages and correctly answering or obtaining the security answer. The victim will receive an email confirming a successful transfer, but the funds will have been diverted to a bank account that the fraudster controls.



Points of compromise that can lead to an *Interac* e-Transfer being intercepted	
Weak security question and answer	✕
Recipient's contact details are outdated or inaccurate	✕
Answer to the security question is sent via the same method as the *Interac* e-Transfer itself	✕

Indicators of *Interac* e-Transfer fraud	
Intended recipient does not receive the transfer almost immediately	✕
Intended recipient receives an email confirmation of the transfer, but cannot collect the funds	✕

Protect yourself from *Interac* e-Transfer fraud

Do (as the sender):

- Create a unique security question that only you and the recipient can know
- If necessary, only share the answer to your security question with the recipient over a secure method of communication, such as over the phone

Do (as the recipient):

- Register for *Interac* e-Transfer Autodeposit to have money automatically deposited without answering a security question
- Create strong and unique passwords to protect your accounts, including your email and social media accounts

Don't (as the sender):

- Include the answer in the security question
- Share the answer to your security question via email, text or on social media
- Reuse the same security question and answer

Don't (as the recipient):

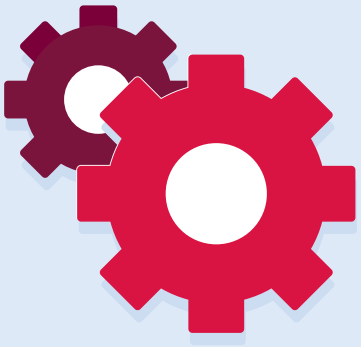
- Create weak account passwords that anyone can easily guess
- Share your passwords with anyone or use the same passwords for all your accounts
- Suggest multiple senders use the same security question and answer

Holiday purchase scams

How it works

Fraudsters take advantage of the increase in consumer spending during the holiday season to impersonate legitimate companies, exploit consumers' charitable attitudes, and lure victims into divulging personal or banking information or sending funds.

The most common holiday purchase scams and how they work are discussed below.



How the scams work

Fake shipping notices	• **Method 1:** Fraudster sends out emails replicating legitimate company shipping notices with an attached link that when clicked on, will download malware or ask for personal or banking information • **Method 2:** Fraudster leaves a "missed delivery" notification on victims' doors with a phone number to call; when victims call, fraudsters will attempt to retrieve personal or banking information
Fake charities	• Fraudster uses email or social media posts to lead victims to the website of a fake charitable organization, using emotional appeals for donations • The fake charity requests donations by payment methods that are untraceable (i.e. wire transfer, pre loaded gift cards, cryptocurrency)
Phony gift cards	• Fraudster sends phishing emails and pop up ads offering free gift cards • Victims click on the email link or ad and may download malware or be tricked into giving their personal or banking information

Offers or deals that sound too good to be true

Offers or deals that sound too good to be true	✕
Requests for personal or banking information	✕
Email or other communications that use poor grammar	✕
Requests for payment via untraceable methods	✕

Protect yourself from holiday purchase scams

1. Identify any red flags

Whether you are expecting package deliveries or are in a giving mood, it is important to distinguish between legitimate and false information. **Ask yourself:**

- Why am I being asked to click on a link by the delivery company in an email? Why would they need my personal information?
- Does the website of this charitable organization seem legitimate? Are there reviews of the charity online?
- Am I receiving unsolicited communications for offers I did not sign up for?

2. Dig deeper

Closely examine the contents of an email, social media post or text message and identify whether it seems suspicious. In particular, look at the grammar, the email address of the sender, the overall presence of the social media account, and whether the account was recently created. If you received a missed delivery notice, check the order status of the packages you are expecting using the tracking link provided by the company that you purchased from.

3. Slow down. Don't rush.

Take time to think carefully about what is being asked of you, and whether it makes sense or sounds too good to be true. Fraudsters will often try to get you to act quickly to their requests by changing topics frequently during a conversation, or by pressuring or instilling fear in you. Do not fall for their tactics; take control of the situation by taking time to think about the information presented to you.

4. Be cautious

- If you have received communications claiming you won gift card prizes for a giveaway or contest you did not enter, it is likely a scam.
- Be wary of emails or websites that claim to be from a reputable delivery company (i.e. UPS, Canada Post, DHL). Closely examine the email addresses and elements of the website that seem suspicious.
- If it sounds too good to be true, it probably is! Many fraudulent lenders lure victims by offering "can't miss" opportunities, in exchange for your personal information or money. If you feel suspicious of an offer, it's best to reject it altogether.

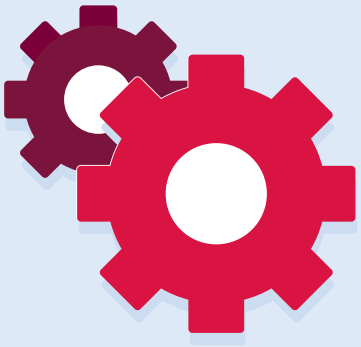
5. Verify with a trusted individual

When in doubt, always reach out! Contact a trusted family member or friend about your situation for a second opinion on the communications or offers presented to you, and whether they are familiar with the name or reputation of the charitable organization you are interested in donating to. If you remain unconvinced or suspicious, do not proceed with donating and ignore all communications.

Vacation and property rental scams

How it works

Vacation and rental property scams involve fraudsters advertising a cottage, apartment, or house for rent on marketplace websites where hosts and properties are not vetted. They do this by taking pictures and descriptions from authentic real estate listings and change the contact information, or fabricate a listing using pictures from a Google search.



Once the victim responds to the ad and contacts the fraudster, they are asked for a security deposit or upfront payment via *Interac* e-Transfer or prepaid gift cards and the fraudster immediately stops all communication thereafter. The victim becomes aware that the property does not exist at the address provided, or the true owner of the property is unaware of the fraudulent listing.

Common marketplace websites fraudsters advertise on:	Craigslist	Kijiji	Facebook Marketplace
Red flags to look for			
Requests for a security deposit or upfront payment via *Interac* e-Transfer or prepaid gift card, without invoices or receipts provided	✕	✕	✕
Requests for credit or debit card numbers and other personal information, or claims by the lister that they cannot meet at the property described	✕	✕	✕
Being rushed or pressured into making an upfront payment as soon as possible, with claims that the offer is the best in the market	✕	✕	✕
Listings with prices that are far below the market price of comparable listings, or that sound too good to be true	✕	✕	✕

Protect yourself from vacation and property rental scams

1. Identify any red flags

When searching for rental listings, it is important to verify whether the offer is legitimate before proceeding further.
Ask yourself:

- Does the property truly exist at the address provided? What does a Google Maps search show me?
- Does the rental price seem too good to be true? What is the price of comparable or nearby listings?
- Is the lister being evasive? Are they denying requests to meet in person?
- Am I being rushed to proceed with the offer? Am I being asked for personal or banking information?

2. Dig deeper

Verify the property exists at the address advertised by doing a quick Google search or seeing the property in person. Search the address on other rental listing websites – and, if an advertisement is found, validate whether the contact information on those listings match the listing you are considering. After performing your due diligence, ask yourself whether you still feel comfortable with the listing or the lister.

3. Slow down. Don't rush.

Take time to think carefully about what is being asked of you, and whether it makes sense or sounds too good to be true. Fraudsters will often try to get you to act quickly to their requests by changing topics frequently during a conversation, or by pressuring or instilling fear in you. Do not fall for their tactics; take control of the situation by taking time to think about the information presented to you.

4. Be cautious

- If you received requests for personal or banking information (i.e. credit or debit card number, SIN, etc.) when interacting with a lister, you may be speaking with a fraudster.
- Be wary of individuals who deny your requests to meet in person or at the property described in the listing.
- If it sounds too good to be true, it probably is! Many fraudulent rental property listers make claims of best in the market deals and urge you to act quickly due to high demand. If you feel suspicious of an offer, it's best to reject it altogether.
- Always request a paper trail in the form of invoices or receipts when making payments for a rental listing, and book vacation rentals with a credit or debit card through reputable listing websites (Airbnb, Vbro) due to the consumer protection benefits provided.

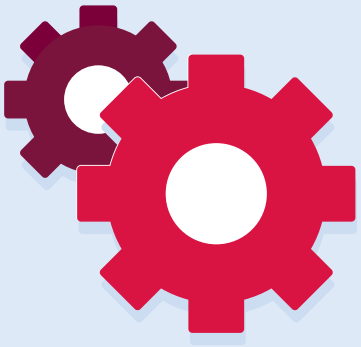
5. Verify with a trusted individual

When in doubt, always reach out! Contact a trusted family member or friend about your situation for a second opinion on messages, calls, or other forms of contact that you are not sure are legitimate. If possible, book vacation rentals or rental properties where relatives or friends have previously stayed.

Lottery and prize scams

How it works

Fraudsters use lottery and prize scams to get money or your personal and banking information. The victim receives an unexpected call, text, email or letter claiming they've won a prize, but are asked to pay a fee to claim the winnings. Typically the victim won't remember entering to win, and that's because chances are they didn't. Once the fee is paid, the victim expects to receive the prize but it never arrives.



To claim the prize, fraudsters may ask the victim to pay a fee for one of the following reasons:

✕ Bank fees	✕ Insurance	✕ Taxes

Red flags to look for

You have to pay a fee to receive the prize. Real prizes do not require winners to pay a fee.	✕
You don't recall entering a draw or contest.	✕
You have to give your financial information to claim the prize.	✕
You're advised to respond quickly to claim the prize or risk missing out.	✕

Protect yourself from lottery and prize scams

1. Identify any red flags

Winning prizes can be exciting, but only when they're real. Before claiming the prize, **ask yourself:**

- Did I enter for the chance to win this prize? How do they have my contact information?
- Claiming a prize should be free - why am I being asked to pay a fee?
- If I won this prize, why am I being pressured to claim the winnings?
- Why am I being asked to provide my financial information?

2. Dig deeper

Gather as much information as you can to verify the legitimacy of the prize. If you received a written communication claiming you've won, check to see who they're claiming to be, look at their email address, and check for spelling or grammatical errors. If you received a phone call, make sure you ask who they are and get as many details as you can. Once you have more information about the contest, research it online to confirm the truth. If they're claiming to be a reputable company, contact them directly using their online contact information.

3. Slow down. Don't rush.

If the prize is real, then you shouldn't be in a hurry to claim it. Take the time to understand what is being asked of you. If you can't recall entering the draw or contest, then it's likely a scam. If you're required to pay a fee or asked to provide your financial information, then it's a scam.

4. Be cautious

Like all scams, the fraudster's intention is to steal from you – whether it be your money, personal and financial information, or both. Fraudsters will use your emotions against you in order to get you to act quickly. As you're excited you've won a prize, the fraudster wants you to quickly do as they say to claim the prize. Don't let them fool you into giving away your money and identity.

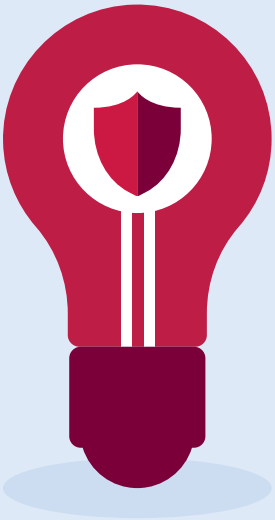
5. Verify with a trusted individual

When in doubt, always reach out! Contact a trusted family member or friend for a second opinion on your situation. If you're still questioning whether the situation is legitimate after doing your own research and getting a second opinion, then trust your instincts and don't follow through with claiming the prize.

Know your fraud, before it knows you

We would like to remind you that you must immediately report any actual or suspected fraud and unauthorized activity on your accounts and debit and credit cards, the loss or theft or cards, and if your card details or PINs are compromised. You must immediately replace your debit card or credit card and change your PINs and banking passwords.

To learn more about resources available to you or how CIBC can help if you are a victim of fraud, please refer to the information below or visit **cibc.com/fraud**.



Stay in the know, wherever you go

Stay on top of your purchases, credit card activity or other transactions that seem out of place with CIBC Alerts via the mobile banking app. By setting up custom alerts tailored to you, we notify you in real-time by text, email or phone if a transaction seems unusual. If it is fraud, we will connect you to a fraud specialist.

Interested in signing up or learning more? Visit our **CIBC Alerts page**.

How CIBC can help

Please contact CIBC at **1 800 872-2422** or email us at **fraud@cibc.com** immediately if you believe you have been a victim of fraud, your accounts have been compromised, or your identity has been stolen.

If you receive fraudulent emails and text messages or would like to report fake websites posing as CIBC, please email us at **fraud@cibc.com** describing the fraudulent incident and attach or include any fraudulent emails or website links you encountered for analysis.

Additional resources

To report fraud, contact the Canadian Anti-Fraud Centre at **1 888 495-8501**, or visit **AntiFraudCentre.ca**.

For the Better Business Bureau (BBB)'s Scam Tracker and Scam Tips, visit:
BBB.org/ScamTracker or **BBB.org/ScamTips**

For more fraud tips, visit:

Competition Bureau Canada	**CompetitionBureau.gc.ca**
Royal Canadian Mounted Police	**RCMP-GRC.gc.ca**