CIBC

# Client protection playbook

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

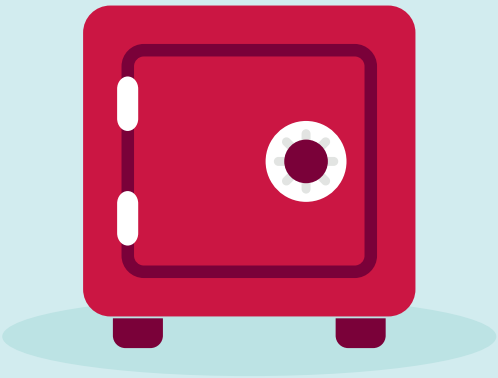
Book 1 of 3

## Table of contents

# 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 using a digital payment platform like Zelle®, prepaid gift cards or 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 Security 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 check for an amount greater than the price you advertised and ask you to deposit the check and wire the excess funds immediately back to them. Once sent to the fraudster, they will cease all communication before the check 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 practices below

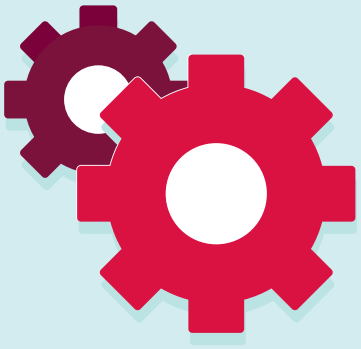
- Enroll your email or U.S. mobile number through your mobile banking app or with the Zelle® app if your bank or credit union doesn't offer Zelle®.
- Never click on an attached link inside an email to visit a website. Type the address into your browser instead.
- Keep your passwords secured offline, 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.

# Romance scams

## How it works

In a romance scam, fraudsters create fake profiles on popular dating or social media sites, posing as companionship seekers targeting victims who are looking for a relationship.

The fraudster maintains frequent contact with the victim through online communication, professing their love early in the relationship. As the relationship progresses and trust is built, the fraudster begins to share fabricated stories of hardship, requesting financial assistance from the victim with promises to pay back the funds.



| Elements of a fraudulent social media profile | |
|---|---|
| Profile has a limited number of photos and only displays part of the individual's face | ✕ |
| Individual puts little to no details on their profile, or their interests are suspiciously identical to yours | ✕ |
| Account or profile is newly established | ✕ |
| Bio or profile has poor grammar | ✕ |

| Red flags to look for | |
|---|---|
| They profess their love to you quickly or ask you to marry them, making the relationship move fast | ✕ |
| They ask you for financial aid by sharing a compelling story as the reason for their request, and become aggressive if you say no | ✕ |
| They provide excuses for not being able to meet in person, such as being on a business trip, deployed overseas or visiting family | ✕ |
| They ask you to send money using payment methods that are hard to reverse, such as wire transfers, prepaid gift cards or cryptocurrency | ✕ |

# Protect yourself from romance scams

## 1. Identify any red flags

Check for inconsistencies in your online interest's stories and elements of their social media or dating profile that do not make sense. **Ask yourself:**

- Does something about their profile seem too good to be true? Is there a lack of details or photos of themselves?
- Is the relationship moving too fast? Are they professing their love or using pet names (i.e., "babe" "sweetheart") earlier than expected?
- Do they consistently provide excuses for not meeting in person?
- Do their messages sound like something that could be copied and pasted and shared with other people? Do the messages have grammatical errors in them?
- Are they asking for money when I have not met them in person yet?

## 2. Dig deeper

Perform your own search of the individual's profile and examine their online presence across other social media platforms. Identify any discrepancies between the identity they portray and what you see:

- Examine how many pictures they have of themselves or with others on their social media profile.
- Determine whether the photos used look like something that can be found from a stock photo site or appropriated from a social media influencer's page.
- Check whether they use at least one other platform. Is their profile bare? Do they have little to no connections?

## 3. Slow down. Don't rush.

Protect your emotions and your money by approaching relationships slowly. Although the internet can be a great way to meet others and even develop a relationship, it's important to verify whether new friends or romantic partners are who they say they are. Stay cautiously optimistic and do not be afraid to investigate further if your companion's stories do not make sense.

## 4. Be cautious

Schedule a phone or video chat with your romantic interest early on in the relationship: If they reject the request, they may be a fraudster. Do not send explicit photos or videos of yourself, especially if you have never met them in person. This may be used as extortion against you.

Lastly, never give out your financial information or send money to someone you have never met; if you are asked for financial assistance, reject their request or simply cease all communication with the individual.

## 5. Verify with a trusted individual

When in doubt, always reach out! If you are still unsure about your romantic partner or believe you may be a victim of a romance scam, reach out to a trusted family member or friend for a second opinion about your situation.

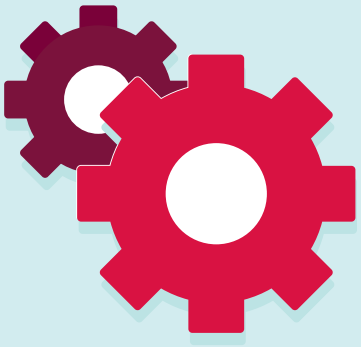
They may be able to provide a more objective view and identify red flags that you did not see.

# Investment scams

## How it works

In investment scams, fraudsters try to persuade victims to purchase fake financial products or services such as stocks, foreign currency or cryptocurrencies. They typically promise high returns for a low risk on their investment and urge their victims to act quickly on this "once-in-a-lifetime" offer.

In most investment schemes, the victim is encouraged to pay money or an advance fee upfront for significantly more profit. Once fraudsters receive that money, they are never heard from again.



| Common financial investments advertised by fraudsters: | Stocks | Offshore accounts | Crypto-currencies | Foreign exchange trading |
|---|---|---|---|---|
| **Red flags to look for** | | | | |
| Paying a "finder's fee" or upfront payment in advance. | ✕ | ✕ | ✕ | ✕ |
| You are guaranteed a high return on your investment at little to no risk. | ✕ | ✕ | ✕ | ✕ |
| Urgency or aggressive sales tactics employed by the fraudster, claiming the offer expires quickly. | ✕ | ✕ | ✕ | ✕ |

# Protect yourself from investment scams

## 1. Identify any red flags

When making investments, it is important to identify your risk tolerance and whether the investment opportunity is legitimate. **Ask yourself:**

- Am I being pressured to act quickly based on claims of a "once-in-a-lifetime" opportunity?
- Is the seller promising significant returns or profits at a low investment risk? Do they claim that everyone is investing in these securities?
- Is the seller claiming they have inside information or received a "hot tip" about a certain investment and wants me to profit from this information?
- Am I being offered freebies by the seller in an attempt to convince me to invest?

## 2. Dig deeper

Verify the authenticity of the seller by researching whether they are a registered investment manager or have a professional designation, such as the Chartered Investment Manager (CIM) designation or the Chartered Financial Analyst (CFA) designation. Dive deeper into the seller's investment management background and their track record of success, and do not be afraid to probe them on their experience or why the offer is sound. Fraudsters often emphasize in their pitches that everyone is investing in it, without explaining the investment itself and why it is promising.

## 3. Slow down. Don't rush.

Take time to think carefully about the investment offer, and whether it makes sense or sounds too good to be true. Fraudsters will often try to get you to act quickly by changing topics frequently during a conversation, 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

- Be skeptical of investment pitches that promise high returns or profits for low risk. Every investment involves risk and never guarantees profits.
- Do not be pressured to act quickly. If you are told that an offer is for a limited time only, consider it a red flag.
- If it sounds too good to be true, it probably is! If you feel suspicious of an investment pitch, it's best to reject it altogether.

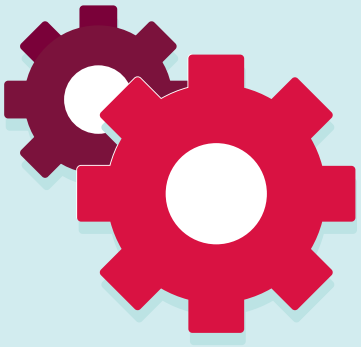
## 5. Verify with a trusted individual

When in doubt, always reach out! Contact a trusted family member or friend about your situation for a second opinion on the investment offer presented to you, and whether they are familiar with the name or reputation of the investment broker. If you remain unconvinced or uneasy about the terms of the offer, reject the offer and stop all communication with the person who contacted you.

# Buy and sell scams

## How it works

In buy scams, victims are tricked by the fraudster into paying for a product or service that does not exist, or is never delivered. Buy scams commonly involve online shopping scenarios, where fraudsters pretend to be legitimate online sellers by creating fake websites or fake advertisements on a genuine marketplace site. They advertise products they do not intend to deliver, and will often ask victims to purchase an item using digital payments, wire transfer or prepaid gift cards. Once payment is received, the fraudster stops all communication with victims.



In sell scams, the fraudster poses as an interested buyer and makes claims to a legitimate seller that they have overpaid the advertised amount for the product(s), requesting the seller to send the difference back via a money transfer. They may even send a fabricated payment receipt to support their claim. A variation of the selling scam involves the fraudster mailing a counterfeit check to the seller worth more than the selling price and taking off with the seller's money transfer before the check can bounce back.

| Common online channels of buy and sell scams | eBay | Facebook Market | Craigslist | Fake websites |
|---|---|---|---|---|
| **Red flags to look for as a buyer** | | | | |
| An unreasonably low price compared to similar offers on the market | ✕ | ✕ | ✕ | ✕ |
| Seller is quick to request payment through a different platform than the one they advertised the product on | ✕ | ✕ | ✕ | ✕ |
| Seller asks for a portion of the advertised price to be paid upfront via money transfer to "reserve" the product | ✕ | ✕ | ✕ | ✕ |
| **Red flags to look for as a seller** | | | | |
| You receive a check for an amount greater than the amount you advertised your product for | ✕ | ✕ | ✕ | ✕ |
| You are asked to pay the difference of an overpaid amount using unconventional methods (i.e., money transfer, prepaid gift card) | ✕ | ✕ | ✕ | ✕ |

# Protect yourself from buying and selling scams

## 1. Identify any red flags

Before making purchases or agreeing to a purchase online, it is important to understand all elements of the offer and verify whether they are legitimate. **Ask yourself:**

- Does the offer advertise an unreasonably low-priced product compared to similar offers on the market? Does the seller's profile appear generic or recently created, or has little previous activity?
- Is the seller asking for payment with prepaid gift cards, money transfer or cryptocurrency? Have they immediately ceased all communication once I have paid for the item?
- Has the buyer sent me falsified or altered receipts, claiming that they have paid or overpaid for the product?
- Is the buyer asking me to pay upfront for transportation costs, promising to reimburse me after delivering the product?

## 2. Dig deeper

**As a buyer**, conduct a reverse image search on Google for photos of the item you are buying. If you find exact pictures of the item that already exist on other legitimate ads or that seem like stock photos, it may be a scam. Consider putting the purchase on hold until you can meet the seller in person to inspect the product, or ask the seller for a video call.

**As a seller**, carefully inspect messages that claim the item has already been paid for. If the buyer has written a check, check your bank account to ensure the funds have cleared before delivering the product.

## 3. Slow down. Don't rush.

Take time to think carefully about what is being asked of you and whether it makes sense. Fraudsters will often try to get you to respond 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

- Be wary of buyers claiming they have overpaid and requesting reimbursement of the difference.
- If the buyer or seller is not willing to meet in person or have a video call to inspect the product before proceeding with the sale, it is best to not proceed.
- **As a buyer**, carefully examine receipts or invoices sent to you and verify whether the information matches the details of the seller's contact information.
- **As a seller**, do not deliver the product until the buyer's funds have cleared and you see them deposited in your bank account.
- Do not agree to cover transportation costs for the buyer, under their promise of reimbursing you after delivery of the product.

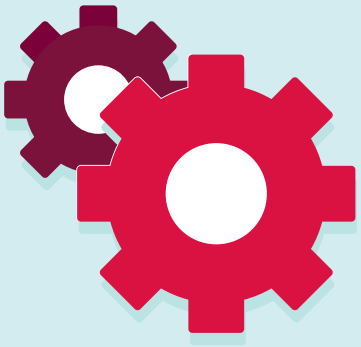
## 5. Verify with a trusted individual

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 make sense. If you remain unconvinced or suspicious, do not proceed with the sale.

# Job scams

## How it works

In a job scam, fraudsters often lure job seekers with a fake opportunity by **promising a high income for little to no effort or experience**—an opportunity that's too good to be true. After a short and simple interview with the fraudster, victims are immediately granted the job and asked for banking information for "direct deposit" purposes. Victims may also be required to pay for job services, training materials and software to another entity using digital payments (i.e., Zelle®, gift cards, etc.).



Many online job sites such as Craigslist, Indeed, Monster, ZipRecruiter and Facebook groups are preferred channels for fraudsters to advertise fake job postings. **Fraudsters may also contact victims directly** by gathering information that they share about themselves via Facebook or LinkedIn, claiming that they found their resume online.

### Common job titles used by fraudsters

| | | | |
|---|---|---|---|
| Cryptocurrency operator | ✕ | Work-from-home roles | ✕ |
| Mystery shopper | ✕ | Administrative/personal assistant | ✕ |
| Caregiver | ✕ | Accounting clerk | ✕ |
| Entry-level jobs | ✕ | | |

### Red flags to look for

| | |
|---|---|
| You are offered a job you did not apply for, or receive unsolicited messages claiming your resume was found online, requesting personal information | ✕ |
| You are promised a high income for little work or no work experience, and salary details are not clearly mentioned (hourly rate/annual) | ✕ |
| The job responsibilities are vague, the employer has little to no online presence, or no contact information is found on the job posting | ✕ |
| After receiving an offer, the employer requests banking information or payment for training, or that you deposit a check on their behalf | ✕ |

# Protect yourself from job scams

## 1. Identify any red flags

While receiving a job offer can be exciting, it is important to verify whether it is legitimate before proceeding further. **Ask yourself:**

- Did I apply for this job? Am I being promised employment after providing personal information on an online form?
- Are the job responsibilities vague? Are the qualifications oversimplified?
- Was the interview process short and not in-depth? Did the employer seem to offer the job too easily?
- Am I being asked to pay for onboarding costs or background checks, send Zelle® transfer payments, or conduct financial transactions on the employer's behalf?

## 2. Dig deeper

Pay close attention to the job description, and whether the job makes promises that sound too good to be true or guarantees a high salary for little work. If you have received unsolicited contact on a job site for an employment opportunity, perform a quick Google search of the company's name plus "scam" and examine what search results appear.

## 3. Slow down. Don't rush.

Take time to think carefully about the content of a job description or offer, and whether it makes sense or sounds too good to be true. If you participated in a virtual interview, reflect on what questions were asked and whether the process was oversimplified or brief. Additionally, if the employer provides you with a list of next steps, rationalize whether they seem reasonable or peculiar (i.e., conducting financial transactions, paying for employer-related costs). If it is the latter, it is likely a scam.

## 4. Be cautious

**Legitimate employers will never:**

- Ask you to pay for training, computer equipment, software costs or background checks
- Provide vague job responsibilities, promise a high salary for little work, or provide obscure salary details
- Request you to provide banking information, your Social Security number, or other personal information immediately after an interview
- Ask you to deposit a check into your bank account, withdraw the funds, then send them via Zelle® to an unknown recipient
- Ask you to purchase prepaid gift cards or cryptocurrency and send them to an unknown recipient

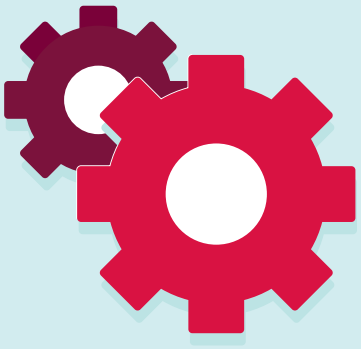
## 5. Verify with a trusted individual

When in doubt, always reach out! Contact a trusted family member or friend about your situation for a second opinion on messages, interviews or other forms of unsolicited contact that you are not sure are legitimate. If you are still suspicious, decline any job offers or requests for personal information and report the incident to the Federal Trade Commission.

# Cryptocurrency scams

## How it works

Fraudsters' main goals in cryptocurrency scams are to obtain access to a victim's digital wallet. Digital wallets are software-based financial accounts that store users' cryptocurrencies, credentials and payment information. Alternatively, fraudsters may attempt to transfer a victim's cryptocurrency directly to their own accounts via social engineering tactics. Several variations of cryptocurrency scams are explained below, but all have the same purpose of stealing personal and banking information and the cryptocurrencies of victims.



## Types of cryptocurrency scams

| | |
|---|---|
| **Romance scams** | Fraudsters use dating apps and websites to lure unsuspecting victims by professing their love early. When trust has been granted, fraudsters ask their victims to transfer their coins or account credentials to take advantage of lucrative cryptocurrency opportunities. |
| **Imposter and giveaway scams** | Fraudsters pose as famous celebrities, business magnates or cryptocurrency influencers who promise victims they will match or multiply the amount of currency sent to them, in what is known as a giveaway scam. |
| **Blackmail and extortion scams** | Fraudsters send blackmail emails to victims claiming they have a record of illicit web pages visited by the user, and threaten to expose them unless they share their digital wallet keys or send cryptocurrency to the fraudsters. |
| **ICO and NFT scams** | Scams involving initial coin offerings (ICOs) and non-fungible tokens (NFTs) have become increasingly prevalent, as investor interest in this space has exploded. Fraudsters launch a fake coin or NFT project, encouraging investors to buy in. After raising enough dollars, they sell the coin or run off and abandon the NFT project, making the investments worthless. |
| **DeFi rug pulls** | Decentralized finance, or DeFi, aims to decentralize finance by removing gatekeepers for financial transactions. DeFi scams closely resemble "rug pull" schemes, in which fraudsters amass investor interest in a project, then take off and abandon the project after stealing a substantial amount of investors' cryptocurrencies. |
| **Cloud mining scams** | Fraudsters convince retail investors to provide upfront capital to rent a continuous stream of cryptocurrency mining power, but never deliver the rewards following the downpayment and cease communication with the victims. |

## Red flags to look for

| | |
|---|---|
| "Guaranteed" returns that are higher than your initial investment | ✕ |
| Giveaways or offers of "free" cryptocurrency, in exchange for personal information or crypto donations | ✕ |
| Heavy use of celebrity and influencer endorsements or testimonials, indicating that they may be fake | ✕ |
| Grandiose claims without specific details, reports or explanations behind them, especially in ICOs and NFT projects | ✕ |

# Protect yourself from cryptocurrency scams

## 1. Identify any red flags

The advent of cryptocurrencies, NFTs and blockchain technology has ushered in a rush of investor enthusiasm and opportunities to exploit the unsuspecting. Before investing in a cryptocurrency or blockchain technology, **ask yourself**:

- Do I fully understand the virtual currency I am investing in? Have the founders provided transparent, in-depth information into the team behind the currency, or is there little information available?
- Is the event I am attending legitimate? Is it promising to give away free cryptocurrency? Are the celebrity or influencer endorsements real?
- Am I being threatened or blackmailed into sending cryptocurrency or revealing my digital wallet credentials?
- Is the project I am interested in investing making big claims without specific details or explanations?

## 2. Dig deeper

Conduct extensive research on the cryptocurrency and digital wallet provider(s) you are interested in before providing any credit card information or wiring money. Identify whether the coin(s) is listed on legitimate cryptocurrency exchange platforms (i.e., Coinbase). Ensure you fully understand the currency you are investing in, the creators of the coin, and explanations of their ICO before deciding to invest. Carefully read agreements with a digital wallet provider or cryptocurrency exchange, as they may not accept responsibility for replacing your money if it is stolen.

## 3. Slow down. Don't rush.

Take time to think carefully about what is being asked of you and whether it makes sense. Fraudsters will often try to get you to respond 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

- Understand the risks involved with investing in a cryptocurrency. Even if you are not being scammed, cryptocurrencies are speculative and volatile. Do not invest money that you cannot afford to lose.
- Do not invest in or trade cryptocurrencies based on advice from celebrities, influencers or someone you have only dealt with online.
- Do not fall for social media posts or endorsements promoting cryptocurrency giveaways.
- Do not share your digital wallet credentials or your "private keys," and store them in a secure place.
- Be very skeptical about any projects or virtual currencies that promise high returns, make large claims or provide no explanations.

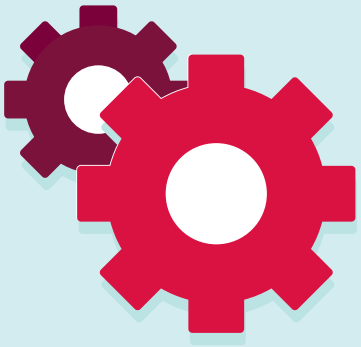
## 5. Verify with a trusted individual

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 make sense. If you remain unconvinced or suspicious, do not proceed with investing in a project or cryptocurrency.

# Emergency scams

## How it works

Emergency scams target parents, grandparents or other family members by scaring them into sending money to help a loved one. A common version of this is the "Grandparent scam," in which fraudsters specifically target a grandparent and impersonate their grandchild.



Fraudsters will call or message claiming to be a family member or friend in trouble. Oftentimes, the caller is with someone claiming to be an authority figure, such as a lawyer, police officer or doctor. The victim is told their family member or friend is in an emergency situation and needs them to send money immediately. Fraudsters will tell the victim that they're the only one that can help, and to not tell anyone about it.

| Common emergency situations | Car accident | Medical emergency | In prison | Trouble getting home from overseas | Legal troubles |
|---|---|---|---|---|---|
| **Red flags to look for** | | | | | |
| You're asked to send money immediately by sending a wire transfer or by paying with gift cards or cryptocurrency | ✕ | ✕ | ✕ | ✕ | ✕ |
| You're asked to keep the emergency situation a secret | ✕ | ✕ | ✕ | ✕ | ✕ |
| You're told you're the only person that can help | ✕ | ✕ | ✕ | ✕ | ✕ |
| There's an authority figure involved, such as a lawyer, police officer or doctor | ✕ | ✕ | ✕ | ✕ | ✕ |

# Protect yourself from emergency scams

## 1. Identify any red flags

You may be eager to help your family member or friend in trouble, but make sure you're not talking to a fraudster before sending your money. **Ask yourself:**

- Why am I the only one that can help?
- Why are they asking me to keep the situation a secret?
- Is this the usual phone number my family member/friend uses to contact me?
- Is an authority figure (e.g., police officer) involved in the situation?
- Are they asking me to send money through wire transfer, gift card or cryptocurrency?

## 2. Dig deeper

Fraudsters gather information about you and your loved ones in order to make this scam seem real. To confirm you're speaking to your actual family member or friend, ask questions that would be difficult for a fraudster to know and answer correctly.

## 3. Slow down. Don't rush.

The situation may seem like an emergency, but resist the urge to act immediately. Fraudsters use fake emergency situations and your emotional connection to your loved ones to get you to send money right away without hesitation. Taking time to confirm that you're speaking to your actual family member or friend in trouble will ensure your money isn't going into the pockets of a fraudster.

## 4. Be cautious

- To confirm if the situation is real, call or message your loved one using the contact information you typically use to reach them.
- Fraudsters will ask you to send money by wire transfer, gift card or cryptocurrency as these payment methods are difficult to trace. If you send money using these untraditional methods, it's difficult or impossible to get your money back.
- Know what information is being shared online about you. Fraudsters use social media as a resource to gather information about you and your loved ones in order to successfully pull off these types of scams.

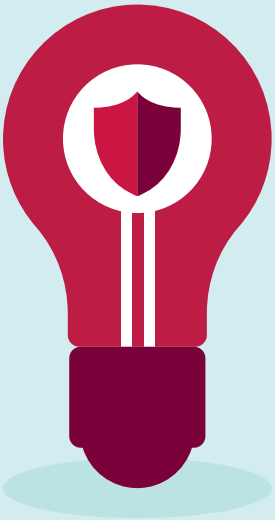
## 5. Verify with a trusted individual

Although you were likely told to keep the situation a secret—don't. Keeping it a secret will only harm you. Share the situation with other family members and friends to get their opinion to see if the emergency situation makes sense.

# 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 of cards, and if your card details or PINs are compromised. Replace your debit card or credit card and change your PINs and banking passwords as soon as possible.

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 **us.cibc.com/FraudPrevention**.



## How CIBC can help

Please contact CIBC at **1-877-448-6500** immediately if you believe you have been a victim of fraud, your accounts have been compromised, or your identity has been stolen.

## Additional resources

To report fraud, visit the Federal Trade Commission at **ReportFraud.ftc.gov**.

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:

| | |
|---|---|
| Bureau of Competition | **ftc.gov/about-ftc/bureaus-offices/bureau-competition** |
| FBI Headquarters | **fbi.gov/contact-us/fbi-headquarters** |