

READ IT \$!
LEAVE IT!

Protect yourself

Scams and frauds often share many common elements, regardless of which particular story the scammer may be spinning you. Arm yourself and the vulnerable people in your life with preventive tips for dealing with scammers.

Fraud Information and Resources



Don't fall victim to scams and frauds

Even as current scams get reported, fraudsters continue to come up with new ways to try to scam money from anyone: youth, seniors, business people, singles, widows and widowers, animal lovers, people wanting to help after natural disasters, and people buying and selling items online.

ALERT: The Red Deer RCMP, as well as police agencies across the country, have seen a dramatic increase in Grandparent Scams targeting seniors. Learn how to spot a grandparent scam and how to prevent it: [Grandparent scam prevention tips \(pdf\)](https://www.reddeer.ca/city-services/police-rcmp/crime-prevention/Grandparent-Scam.pdf) ([pdf](https://www.reddeer.ca/city-services/police-rcmp/crime-prevention/Grandparent-Scam.pdf)).

The best defence is a good offense

Arm yourself and the vulnerable people in your life with preventive tips for dealing with scammers, regardless of which story they're spinning you.

- Remember, whether the request is from a legitimate company or a scammer, you have the right to ask as many questions as you need to, and take as much time as you need to, in order to decide if they merit your trust.
- Do not give out personal information, over the phone or otherwise, unless you were the one to initiate contact and it is an organization you trust.
- Ask for written information about the person, business or charity.
- Ask for identification and registered charity numbers. Confirm the validity of the information you are given by looking up their phone number and website yourself rather than using the information they offer you.
- Do not send any money or pay a fee to claim a prize.
- Be suspicious if this is a "today only" offer. If it is truly a legitimate deal, it will be there tomorrow.
- Be wary of appeals that tug at your heart strings, especially pleas involving current events.
- Treat your personal information with care; do not leave it lying around for others to take. Shred old bills, statements, credit cards, etc.
- Rely on established businesses or individuals, whose reliability and credibility can be established through a professional organization such as the Better Business Bureau (<http://www.bbb.org/council/consumer-education/>) (BBB) or the Chamber of Commerce (<http://reddeerchamber.com/>).

Have you been the victim of a scam or fraud?

- If you have NOT lost money but suspect you have been targeted, contact the Canadian Anti-Fraud Centre (<http://www.antifraudcentre-centreantifraude.ca/>) 1-888-495-8501 (tel:+1-888-495-8501)
- If you receive a suspicious email soliciting your financial information, advise the bank/agency involved.
- If you are a victim of fraud, call the Police non-emergency line at 403-406-2200 (tel:+1-403-406-2200) and the Canadian Anti-Fraud Centre (<http://www.antifraudcentre-centreantifraude.ca/>) at 1-888-495-8501 (tel:+1-888-495-8501).

Links and Resources

Red Deer RCMP News Releases

(<https://reddeer.ca/city-services/police-rcmp/rcmp-news-releases/>)

RCMP Scams and Frauds

(<http://www.rcmp-grc.gc.ca/scams-fraudes/index-eng.htm>)

Central Alberta Crime Prevention Centre

(<https://www.cacpc.ca/index.html>)

FRAUD EXAMPLES

Taxpayer or Canada Revenue Agency Scams

A scammer claims to be an employee of either the Canada Revenue Agency or Service Canada. They state that you:

- have a compromised SIN number
- have an outstanding case against you
- owe back taxes
- have unpaid balances
- committed a financial crime

They threaten that if you do not speak to them immediately, you'll be arrested, fined or even deported.

The scammers may request payment via money service businesses, pre-paid cards/gift cards (iTunes, Google Play or Steam cards) or Bitcoin.

Law Enforcement Scams

An email or phone call claims to be from a law enforcement agency, such as the RCMP, Interpol or Europol. They will use police logos or other identifiers to appear legitimate. The message could be:

- A fraudulent letter accusing you of criminal charges and asking you to contact them to avoid going to jail
- A message demanding you send money to avoid arrest
- An email with a malicious attachment that they ask you to open

These are all scams. Law enforcement will never demand payment and will not threaten arrest by email or phone. If in doubt, contact the law enforcement agency directly.

Emergency Scams

Emergency scams prey on your fear of a loved one being hurt or in trouble. Scammers claim to be someone you know and tell you they need money immediately.

Scenarios they may use include:

- Needing bail money because they've been arrested
- Being in a car accident
- Trouble returning from a foreign country

Reports are showing a new variation where fraudsters contact you via email or text message, claiming to be a loved one asking for a favour. For this favour, they'll ask you to send money or gift cards.

Fraudsters will

- Claim to be law enforcement officials, lawyers and impersonate the grandchild/family member
- Use urgency and threats to convince you to take out money
- Claim that there is a "gag order" preventing you from speaking about the situation
- If you agree to pay the requested amount (cash or cryptocurrency), fraudsters will arrange to pick up the funds in person or will ask you to send cash in the mail

Variation: Broken phone scam

The CAFC is getting reports about a fraudulent emergency text or social media message. The fraudster might claim to be a family member or loved one saying that their cellphone is broken or has been dropped in water. The fraudster will then provide an alternate phone number to contact them at. The fraudster will proceed to ask for a favor by requesting funds from the victim to repair the broken phone or to pay a bill.

This is a screenshot from a reported emergency scam using the broken phone variation (example in English only).

Variation: Grandparent scams

A senior gets a phone call, typically on their home phone/landline, from a caller claiming to be their grandchild or calling on behalf of their grandchild. They say they need money as soon as possible, whether to pay bail, lawyers fees, hospital fees, ambulance fees, etc. They will say the payment is needed immediately to avoid going to jail or to be released from jail.

Note

These types of scams can target anyone, not just seniors or "grandparents".

How to protect yourself

- If you receive a phone call claiming to be from a family member in an emergency situation, hang up the phone and contact them directly using a phone number you already have – not one provided by the suspected fraudster.
- If the caller claims to be a law enforcement official, hang up and call your local police directly, using a phone number from a reputable source – not one provided by the suspected fraudster

- Be suspicious of telephone calls that require you to immediately act and request money for a family member in distress
- Listen to that inner voice that is screaming at you "This doesn't sound right"
- It is important to know the Canadian Criminal Justice System does not allow for someone to be bailed out of jail with cash or cryptocurrency
- Be careful what you post online
 - Scammers can get details that you shared on social media platforms and dating sites to target you or get names and details about your loved ones
- Don't trust caller ID names and numbers.
 - Scammers use technology to disguise the actual number they are calling from and can make it appear as a trusted phone number, also known as spoofing

Foreign money offers

Also known as **inheritance scams** and **fake business proposals**.

A scammer contacts you asking for help to transfer a large sum of money from one country to another. The requests often appear to come from a lawyer or legal entity.

These requests can include:

- fake inheritance letters
- fake business proposals
- requests for help with an illegal activity (e.g., smuggling gold out of Iraq)

They advise you that you need to pay one or more fees before the money can be released. However, the money doesn't exist and you never receive anything.

These scams are sometimes referred to as Nigerian, 419 or West African fraud.

Tech support

A scammer claims a virus has infected your computer. The communication might happen through:

- Alarming website pop-ups that demand you call a number urgently
- Unsolicited telephone calls (they may claim to be a Microsoft or other well-known computer company employee)

The scammer states that your computer is sending out viruses or has been hacked and must be serviced. They request access to your computer and may run programs or alter settings.

The scammer asks you to pay a fee for fixing your computer via credit card or money transfer. In some cases, the scammer asks you to log into your bank account to transfer funds.

Personal information

A scammer, pretending to be from a business, government agency, a bank, or utility company, urgently asks you to verify your personal information. They may request information such as:

- Your name
- Your address
- Your birth date
- Your account information
- Your Social Insurance Number (SIN)

Once you provide this information, the scammer may use it for identity fraud.

Never provide personal information over the phone, online or through email in response to an [unsolicited request](#).

Relationship and romance

A scammer convinces you to enter a virtual, online relationship so the scammer can gain your trust and affection. This can occur through:

- Email messages
- Fake profiles on social media and dating sites

Eventually, the scammer may ask you:

- for money for travel, a medical emergency or family assistance – making it seem urgent or like an emergency
- to receive money for them – by doing so you might unknowingly be committing a crime
- to join a business venture with them
- to invest in cryptocurrency

Scammers will try to use any means necessary to convince you that their requests are legitimate. The majority of fraud is not committed by amateurs and they will use technology to their advantage.

Variations

Combining romance and investment scams

The CAFC is noticing an increase in a combination of romance and investment scams which are often referred to as "pig butchering". In these scams, you are contacted on dating apps or social media by a fraudster who is attempting to develop a relationship with you to gain your trust. After trust is gained, the fraudster will claim that they have been a successful investor in cryptocurrency and can help you also make money and "get rich" and convince you to invest.

They may even let you cash out some of your investment returns only to get you to invest a larger amount. Suspects will "coach" you on how to invest in their **fraudulent crypto**

currency platforms. Unfortunately, once you request to withdraw their investment, you can't.

Relationship investment fraud phishing

Sometimes referred to as approval phishing. Fraudsters deceive you into granting access to your cryptocurrency accounts by those posing as trusted services. After they coach you on how to acquire cryptocurrency like Ethereum or Tron, they send you a fake request appears to come from the crypto service, asking you to "approve" access to your wallet. By clicking "approve," you unknowingly give control of your funds to the fraudster. The fake requests closely mimic legitimate apps and services, making them look authentic. In some cases, you may receive a transfer request asking you to click on a link to accept and you may unknowingly be providing the "approval" to access your wallet.

Look out for these red flags and be suspicious:

- when someone you haven't met in person professes their love to you
- if the person wants to quickly move to a private or different mode of communication (email, text, Whatsapp, Google Hangouts etc.)
- if they always have an excuse not to meet in person
- if you receive poorly/oddly written messages, sometimes even addressing you by the wrong name
- if the individual claims to live close to you but is working overseas
- if they act distressed or angry to guilt you into sending money
- if the individual discourages you from discussing them or their situation with your friends and family (attempting to isolate you from those who may be suspicious of the relationship)
- if someone offering to "coach" you on crypto investing
- of emails appearing to be from your crypto service provider asking you to click on links
- of get rich quick investment opportunities
- of individuals met on dating sites or social media who attempt to educate and convince you to invest into crypto currency

How to protect yourself

- Don't give out your personal information (name, address, DOB, SIN, banking credentials)
- Don't accept friend requests from people you do not know
- Don't invest your money in platforms provided by people you don't know
- Never send money to someone you haven't met
- Enable Multi-Factor Authentication (MFA) on your accounts
- Beware of fraudsters asking you to open and fund new crypto accounts, they will direct you to send it to wallets they control - Don't!
- If you have granted a suspect access to your crypto account, follow the OPP's [checklist](#) to revoke the token approval

