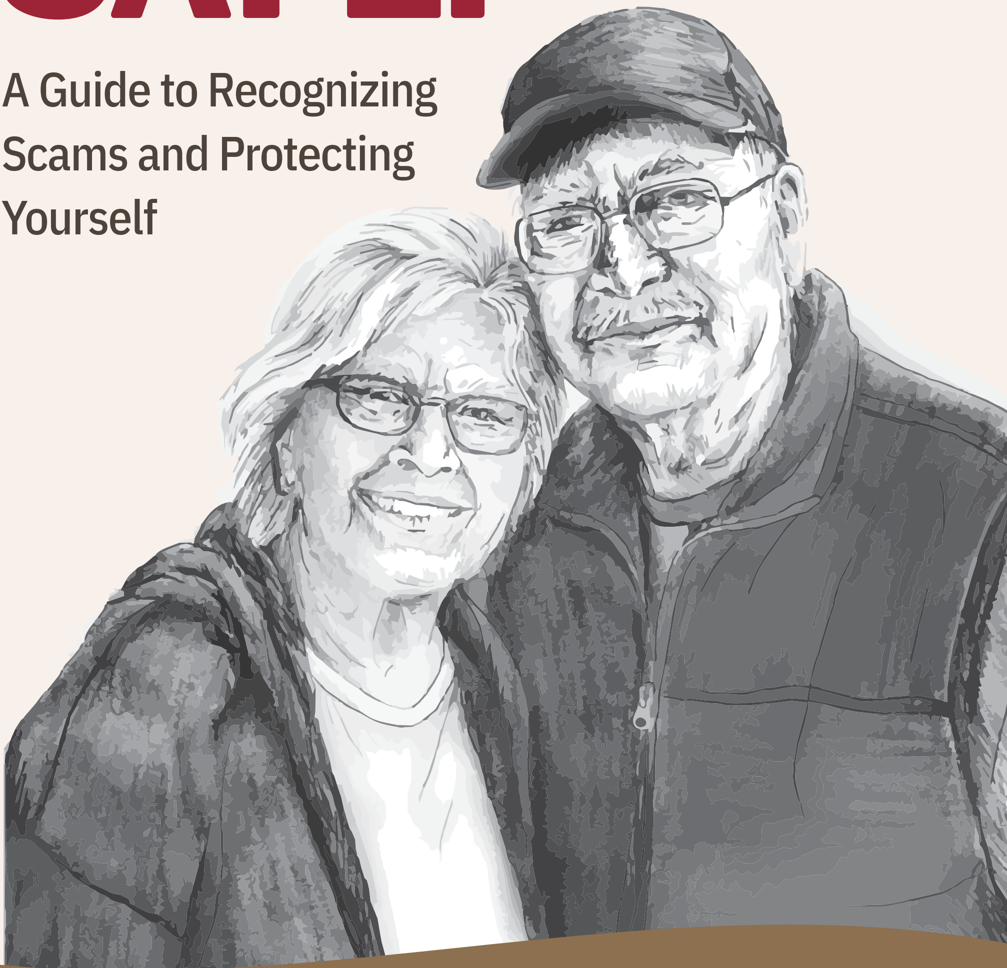
BE SCAM SAFE!

A Guide to Recognizing Scams and Protecting Yourself



STAY INFORMED. STAY PROTECTED. STAY SCAM SAFE!

Northwest Territories
Seniors' Society

Be Scam Safe!

Northwest Territories
Seniors' Society
ESTD. 1983
Seniors Helping Seniors

Box 1044, Yellowknife, NT, X1A2N7
Office: 867-920-7444
Senior Information Line Toll Free: 1-800-661-0878
admin@seniorsnwt.ca
Home - NWT Seniors' Society:
https://nwtseniors.ca/

Table of Contents

Introduction

Scammers actively target seniors. The NWT Seniors Society produced this booklet to inform seniors about scams and how to avoid them.

It's important to be aware of and talk about how some common scams work and what warning signs to look for, so you can disengage before it's too late.

The booklet will include:

- What is scamming? Why is it dangerous?
- Different types of scams.
- How to recognize scams.
- What to do if you suspect a scam.
- What to do to help prevent scams.

Reporting scams to the Canadian Anti-Fraud Centre is very important to help prevent others from being scammed!

Contact the Anti-Fraud Centre to report a scam.
Call toll free: 1-888-495-8501 Mon to Fri, 10am to 4:45pm Eastern time. Closed on holidays.
Report online:
https://reportcyberandfraud.canada.ca/

What is scamming ?

Scamming is when someone tries to trick you into giving them money, personal info, or other things of value. To get you to cooperate, the scammer – the person or entity doing the scam – uses various tactics, such as:

- Threats
- Lies or deceit
- Manipulation
- Building trust and then abusing it

Scamming usually happens through digital devices: smart phone, tablet (e.g. iPad), laptop or desktop computer, or fax machine. Through these devices, scammers make contact through:

- Email
- Social media
- Texts
- Websites
- Online shopping sites
- Ads
- Phone calls
- Faxes

Scamming can also happen over a landline or face-to-face.


12:45
SCAM
SCAM
SCAM

Phishing (email) and Smishing (texts)

Phishing (emails) and smishing (texts) are fake messages that appear to come from a legit, trusted individual / organization. Scammers prompt you to give up personal info – *username, password, credit card number, bank account info* – or click on a link that downloads malware or spyware to your device.

Phishing on social media is the use of fake profiles and malicious links used to steal personal information or gain control of accounts.

Scammers use the data to take over an account, send unauthorized payments, open fake accounts, and create fake identities.

A scammer contacts Jane and claims to be from her bank. There's an issue with her account or credit card, and they need to fix it right away. They ask for her PIN.

A scammer contacts Frank and claims to be with the CRA. They ask for his SIN and other personal info. He owes back taxes and must pay right away to avoid a fine or arrest. Or he has a refund – that he can access when he clicks on the link.

A scammer poses as a medical organization such as Blue Cross or Canada Life. They send a fax, asking for medical and other documents, falsely claiming they are part of a health audit.

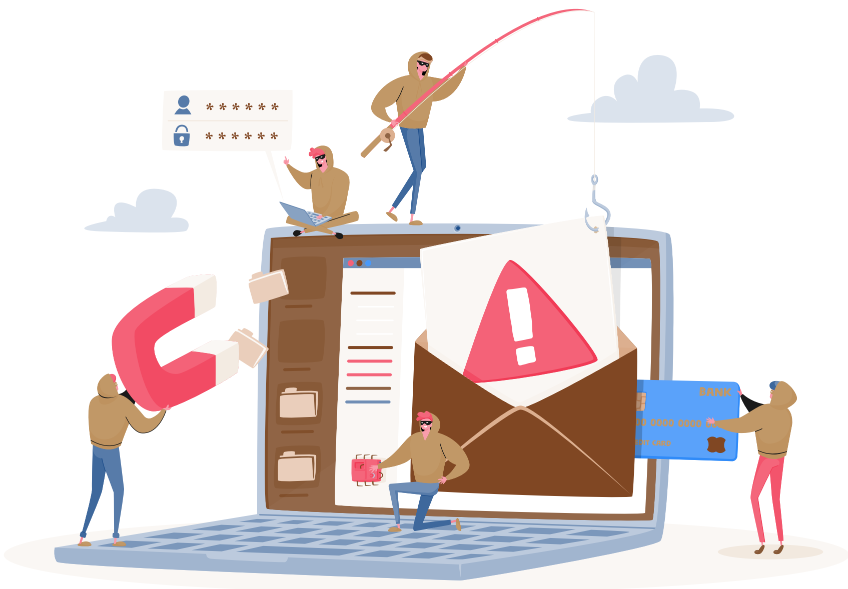
BE AWARE!
Banks and Governments will never ask for personal information, passwords or pin numbers by text or email. They will also never send links for you to click on to provide personal information.

WARNING SIGNS FOR PHISHING / SMISHING

- Threats and urgency – pressure to act quickly / right away.
- Unexpected sender – someone who would never contact you this way. For example, banks, the CRA, and all other federal or territorial departments would NEVER contact you this way.
- Unusual or unknown sender – someone you don't usually hear from, even if you know them.
- Unexpected or odd attachment.
- Too good to be true.
- Links to a suspicious URL (webpage address).
- Email or phone number that doesn't match the organization it's supposed to come from.

IF YOU SUSPECT A SCAM ...

- PAUSE. Take time to think. Do NOT reply or click on any links or provide any personal info.
- VERIFY. Contact the sender directly – call them. Tell them about the message that you suspect a scam.
- Check the URL. You can see it without clicking if you hover the cursor over it. Type it directly into your search engine.
- Delete any suspicious messages and empty the ‘trash’ right away.
- Check your accounts if needed.



Emergency Help

A scammer calls or messages on social media and pretends to be someone in trouble – a grandchild, other family member, or close friend. They need money right away to deal with an emergency / big problem.

GRANDPARENT SCAM

Mabel is a grandmother and close to her grandson Fred. She gets a frantic phone call from 'Fred'. He is totally distressed. He's been in a car accident, arrested, and needs bail money right away. "Please don't tell my mom. She'll be SO upset that I got in trouble again." Mabel sends money to 'Fred' through a wire transfer.

WARNING SIGNS FOR EMERGENCY SCAMS

- Emotional phone call, often late at night.
- Caller may start the call with 'do you know who this is?' looking for a name.
- Claims of an emergency / big problem. Asking for secrecy.
- Unusual payment methods.

IF YOU SUSPECT A SCAM ...

- PAUSE. Do a reality check. Does this make sense?
- VERIFY. Hang up and call the person.
- Ask questions that only that person would know. Use the 'safe' word if your family has one.
- Never use unusual methods to send money.
- End the contact, even if it hurts.

Online Shopping – Buying and Selling

Scammers pretend to be buyers or sellers to steal your money and personal info.

When they are selling, scammers set up a fake website, which imitates a real one. Or they create a fake profile and listings on legit online shopping apps such as Facebook Marketplace. Scammers also post fake ads and fake reviews.

The products and services they offer don't exist. If it's a local ad on Marketplace, they make excuses to not meet the buyer or show them the actual item for sale.

Marie has been doing research online for a new rod and reel for her daughter's birthday. An ad appears that catches her eye. She clicks on it. The site looks legit. The price is great and it's a good brand. Everything checks out. She considers herself wise to scamming. The minute she pays the $200, mysterious charges appear on her credit card. The items she ordered never arrived. No tracking update, no replies, nothing.

When they're buying, scammers try to purchase an item and scam the seller out of the money. They may ask for your help to pay for fake upfront costs (e.g. insurance) and promise to pay you back. Or they may send a fake cheque for an amount higher than the selling price. Then they ask the seller to return the overpayment, often through wire transfer, gift cards or e-transfer. The cheque bounces: you lose the money you sent.

WARNING SIGNS FOR ONLINE BUY AND SELL

- Prices too good to be true.
- Time-limited offer. Pressure to buy right now or the deal ends.
- Payment methods that are hard to trace: wire transfer, cheque, gift card, or cryptocurrency.
- No contact info.
- Webpage address (URL) looks 'off'. E.g. misspelling, extra words or characters, unusual endings, unusual abbreviations, hyphens instead of dots, etc.

IF YOU SUSPECT A SCAM ...

- PAUSE. Take time to think.
- VERIFY. Check the ‘real’ vendor’s website. Google the brand name + ‘scam’ to search for info.
- Only buy online from well-known platforms or trusted sites with secure payment.
- For apps such as Marketplace, only pay when you have the item in hand and pay cash.

Romance (Catfishing)

A scammer adopts a fake online identity to gain a person's affection and trust. They use the illusion of a romantic relationship to steal money and personal info.

Scammers target people through online dating sites, social media, and email. They have many excuses to avoid in-person meetings, video calls, or sending photos.

Romance scams are sometimes called 'catfishing'.

Kelly responds to a dating profile she really likes – 'Jim'. Over time they build a connection – she's emotionally attached. They talk on the phone and use email and text messaging. Then 'Jim' asks for her help – money and plane tickets.

WARNING SIGNS FOR ROMANCE SCAMS

- A profile that's too good to be true.
- Intimacy develops too quickly.
- The person refuses to send a photo or meet in person or via video call. Often say they work / live too far away / in a different country.
- The crisis or 'problem' is clearly made up.
- Asking for money or personal info.

IF YOU SUSPECT A SCAM ...

- PAUSE. Do a reality check. Talk to a trusted friend or family member.
- VERIFY. Search on Google to see if their profile photo is used elsewhere.
- Insist on video calls so you can see the person. Ask them to send a photo.
- Do NOT send money or personal info.
- End the contact, even if it hurts.

Fake Charity

Scammers pose as charities to steal money. They ask for donations via phone, email, or social media. They pretend to be an existing charity, or they may create a fake one. Their info looks realistic and preys on emotions. People donate because they believe they are giving to a good cause.

During the Christmas holiday season, John sends money to a 'charity' that appears to help families in need with toys and food.

Terry Lynn sends money to a 'charity' to help people evacuated during a wildfire or flood. She knows how that feels.

WARNING SIGNS FOR CHARITY SCAM

- Urgency – pressure to respond / pay quickly.
- Unusual payment methods: gift cards, wire transfer, cryptocurrency.
- Unclear about how they plan to use the money.
- Unsolicited contact.

IF YOU SUSPECT A SCAM ...

- PAUSE. Do NOT send money.
- VERIFY. Confirm the organization is legit. Research crowdfunding carefully before donating.
- Donate directly to organizations / causes you support, using secure payment methods.

Tech Support

Scammers use pop-ups, warning messages, or unsolicited contact to get your attention and steal money and / or personal info. They say there's something wrong with your device or that your financial accounts have been hacked or are about to be hacked – and they can fix it.

Ruth receives a call from someone pretending to be tech support from a legit company. "We found a problem with your computer. To fix it we need to download special software; we need your password." Later that day Ruth found someone had accessed all her online bank accounts.

Jimmy clicks on an ad that offers free tech support. He's redirected to a page that asks for his password. A few days later he finds someone has changed his social media accounts, asking his contacts for money.

Bruce is doing his taxes online when a popup warns him of suspicious activity on his computer. He calls the number. "We can fix your computer right away, but we need your password for remote access." A few minutes later Bruce gets notifications of bank transactions he knows nothing about.

Posing as tech support companies, scammers may bring in others to pose as bank or government officials or officials from other legitimate organizations. They say you need to protect your device and encourage you to sign up for a fake subscription – to install software to protect yourself.

WARNING SIGNS FOR TECH SUPPORT SCAMS

- Unsolicited pop-ups or calls.
- Requests for remote access, passwords.
- Claims of expired software, illegal content, or other problems.
- Urgency and threats.
- Unusual, hard-to-trace payment methods.

IF YOU SUSPECT A SCAM ...

- PAUSE. Do NOT click on a link. Do NOT call numbers on warning messages.
- VERIFY. Check the official website for tech support. Try a 'google search' to see if others have had this experience with scammers.
- Ignore unsolicited messages and popups.

- Do NOT allow them to access your device or install software.
- Do NOT share any personal info. E.g. passwords, financial info, etc.

Prize / Lottery

Scammers contact you to tell you that you've won a high-value prize – money, free trip, car, etc. They trick you into handing over personal info and / or money to receive a prize from a competition or lottery that you never entered / that does not exist.

Greg got a private Facebook message claiming he and some others had won $150,000 from Facebook Freedom Lottery. At first, he didn't believe it. It didn't make sense – free money from Facebook; to win a lottery when he didn't buy a ticket. But then he got a message from his cousin saying she also won; that she noticed his name on the winners list – that she got her money.

So Greg started the process to claim his money. He first paid an upfront fee of $250. Then he paid an 'international transfer fee' because the money was in a U.S. bank. Over the next two weeks, Greg paid five more fees. Eventually he contacted his cousin to see how much she paid in fees. She had no idea what he was talking about.

By this time Greg had paid over $1500 in fees and handed over a lot of personal info to the scammers. He lost his money and never got the prize.

WARNING SIGNS FOR PRIZES / LOTTERY SCAMS

- Too good to be true. You never entered a competition.
- Urgency: must act right away or you lose the prize.
- Must pay upfront fees: taxes, shipping, insurance, etc.
- Hard-to-trace payment methods such as wire transfer, gift cards, cryptocurrency.
- Cheque (fake) arrives – scammer asks you to deposit it and send a portion back to cover 'fees'.

IF YOU SUSPECT A SCAM ...

- PAUSE. Do not respond. Consider 'How can I win something when I never entered the competition?
- VERIFY. Look up the organization's website. Try a google search to see if others have had this experience.
- Do NOT send money or personal info.

Investment

Scammers lure people with promises of 'get rich quick', insider info, and exclusive, time-limited offers – to steal money. They often use high-pressure tactics, social media, or celebrity endorsements.

A scammer contacts Sam with options for risk-free investments and high rates of return. To build trust over time, they show 'fake' profits to encourage investment. Sam decides to participate; then needs his money for emergency house repairs. When Sam tries to withdraw his money, they demand fees, claim tax issues, or disappear entirely.

WARNING SIGNS FOR INVESTMENT SCAMS

- Guaranteed, high rates of return. Too good to be true.
- Unsolicited contact.
- Pressure to act quickly – avoid missing out on a 'good thing'.
- Unusual, hard-to-trace payment methods.

IF YOU SUSPECT A SCAM ...

- PAUSE. Consider: is this realistic / a good idea?
- VERIFY. Check that the company is registered.
- Be on the lookout for a 'funds recovery' scam – offers to recover lost money for a fee.

Artificial Intelligence

AI (artificial intelligence)is using computer systems to perform tasks or produce emails, text or phone calls that would normally require a person. It has transformed scamming. Scammers exploit AI to increase their chances of success.

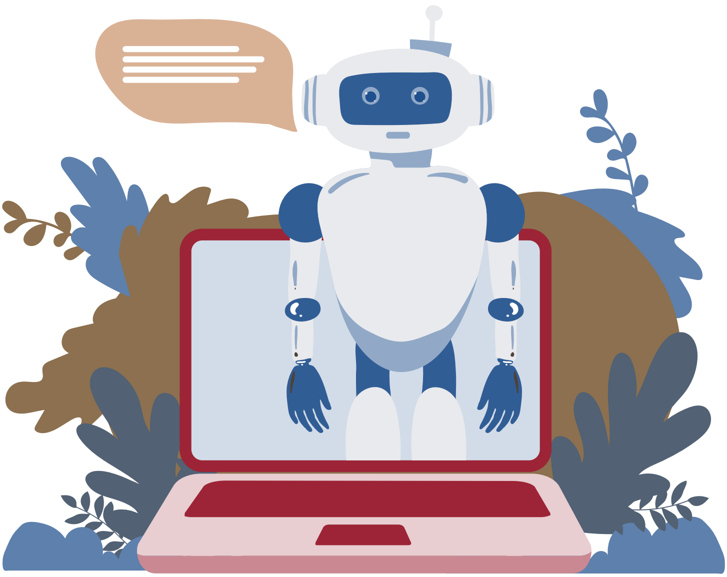
DEEP FAKE AND VOICE CLONING

Scammers use AI to create deep fake videos and images and voice cloning. Scammers use voice cloning to impersonate family, friends, or executives – such as in an emergency scam.

Deepfake videos or images use AI to generate the likeness of a real person. Scammers can use these to impersonate a public figure to promote a fake investment scheme, a family or friend to financial accounts.

Mary sees an ad on Facebook where the Prime Minister of Canada is urging residents to invest $250 into a Federal Government program with the promise of making a huge profit. THIS IS A SCAM!

Scammers use AI to create messages with correct grammar and tailored content. This makes ‘fake’ emails and other messages much harder to detect.



CHATBOTS

Chatbots are a software app or web interface that converses through text or speech.

Scammers use AI-powered chatbots to engage in long-lasting, emotional, and personalized conversations for romance scams via messaging and phone.

FAKE IDENTITY

Using AI, scammers combine real data (e.g. SIN) with fake info to create a 'new identity'. They use this made-up person to open bank accounts, apply for loans, and build credibility over time to maximize gains.

AI PAYMENT OPTIONS

Scammers favour cryptocurrency, digital wallets, money transfer apps, and other instant, non-reversible payment options. These are very hard to trace and make it impossible to recover funds.

FAKE PROFILES

Scammers use social media to create fake profiles or bots (automated apps) to build trust and gather information. They use these tools to impersonate friends, celebrities, or public officials; to trick people into sending money and personal or financial info.

SPOOFING

Spoofing is when the scammer changes the number on the displayed caller ID to make it look like it's from a trusted number, with a local area code – from a legit business, government agency, family member, or friend. Scammers use these apps or bots to disguise their identity and robocall many people at once.

OTHER AI METHODS

SIM card swapping, porting, and call forwarding are all legitimate services. Scammers use them to take over a mobile phone and control accounts. Banks and other entities often use one-time passcodes to authenticate the user. If the scammer has access to the phone, they can intercept the passcode, pose as the person, and start scamming.

Scammers use virtual private networks (VPNs) to hide their internet address. They use botnets to automatically attack a large number of people at the same time. A botnet is a network of internet-connected devices infected with malware.

Fake mobile apps and quick response (QR) codes may use legitimate names or brands. Scammers use these to steal personal info, intercept payments, or install malware to get control of devices and gadgets.

Northwest Territories
Seniors' Society
ESTD. 1983
Seniors Helping Seniors

Government of Canada
Gouvernement du Canada