Financial Scams and Fraud

How to outsmart scammers:

Tips to avoid scams and protect your pockets

January 2026

Funded in part by the Government of Canada's New Horizons for Seniors Program

Canada

ST. JOHN'S

Introduction

Funded in part by the
Government of Canada's
New Horizons for Seniors Program

Canada

ST. JOHN'S

Definitions

Fraud:

- A general term that covers any form of dishonest behaviour designed to gain something unfairly. It can involve various forms of deception, such as stealing personal information or manipulating someone to give them money or goods.

Scams:

- Scams are a subset of fraud that specifically refer to deceptive schemes used to trick someone into giving up money, personal information, or other valuable assets.

The Impact of Fraud in Canada

As of September 30, 2025:

- **33,854** reports processed
- **23,113** victims of fraud
- **$544 M** lost to fraud

In 2024:

- **51,999** reports processed
- **36,248** victims of fraud
- **$644 M** lost to fraud

Source: Canadian Anti-Fraud Centre 2025

The Impact of Fraud in NL (1/2)

During 2024 in NL:

- **310** reports
- **61** reports per 100,000 population
- **76%** victimized
- **$4.3M** loss

Top 3 Frauds based on number of reports:

- **60** service frauds
- **41** identity frauds
- **34** Investment frauds

Source: 2024 Annual Statistical Report
Canadian Anti-Fraud Centre

The Impact of Fraud in NL (2/2)

Top 3 frauds in NL based on dollar loss:

- Investment: **34 ($3.2M)**
- Romance: **12 (over $2.3K)**
- Job: **20 (over $1.4K)**

Source: 2024 Annual Statistical Report
Canadian Anti-Fraud Centre

Why Seniors?

- Trusting and polite nature
- Often home during the day
- Retirement savings attract scammers
- Less familiar with technology or online security
- Loneliness or social isolation increases vulnerability
- Memory or cognitive decline makes it harder to spot suspicious activity

Types of Scams

Funded in part by the
Government of Canada's
New Horizons for Seniors Program

Canada

ST. JOHN'S

Common Types of Scams

- Internet Fraud
- Grandparent Scams
- Romance Scams
- Investment Scams
- Canada Revenue Agency (CRA) Scams
- Telephone Scams
- Door to door Scams
- Overpayment Scams
- AI (Artificial Intelligence) Scams
- Technology Support Scams

Internet Fraud

Using online platforms and messaging to trick victims into giving personal information, money, or both. It includes phishing, smishing and other digital scams.

- Fake emails and messages
- Pop-up ads with malicious links
- Scammers posing as banks, government, or family
- Fake online stores or prize / lottery offers

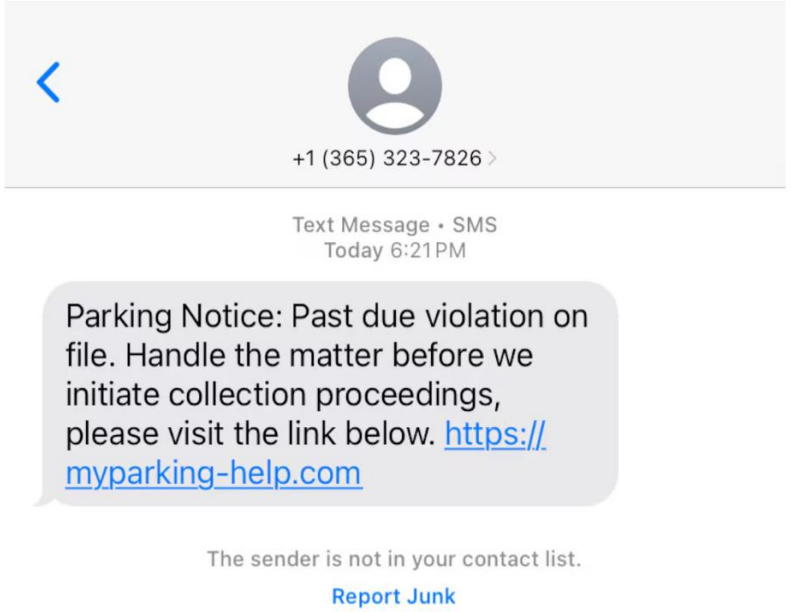
Phishing and Smishing

Phishing:

- Unsolicited e-mails that claim to be from a legitimate organization, e.g., banks, government agencies, asking for personal and/or financial information.

Smishing:

- Like phishing but takes place by text messages to your cell phone or iPhone trying to get login information to online banking or social media.



Video: Phishing Scams

Phishing Example: Trusted Company

1. Email looks legitimate but it’s fake. “L” is a capital "I".
2. Strong wording to sound urgent
3. Logo: pixelated & light color
4. Friendly tone
5. Pressure to respond
6. Links disguised to look official

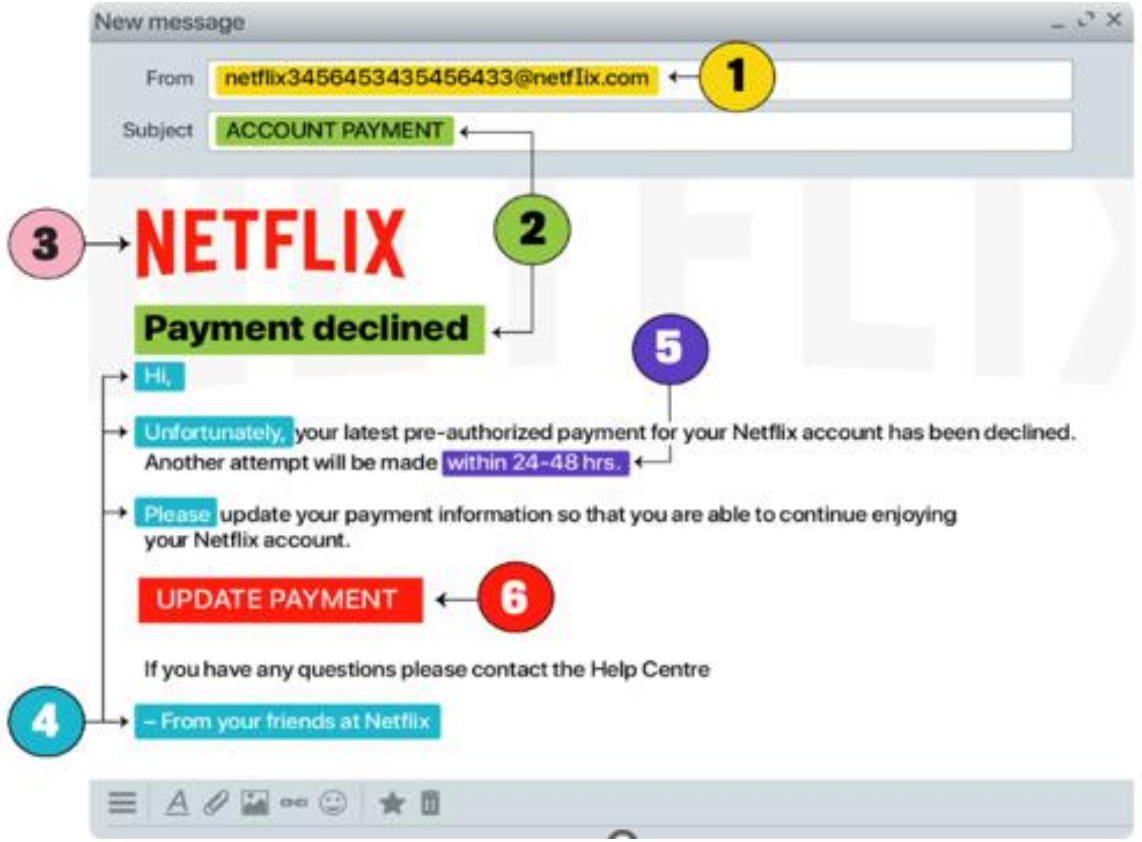


Photo credit: Government of Canada

Phishing Example: Vendor Impersonation

1. Uses official logo to trick you
2. Different character - **α** - in the email domain
3. Pushing you to take action
4. Friendly or apologetic tone
5. Prize offer for cooperation
6. Professional signature to seem legitimate

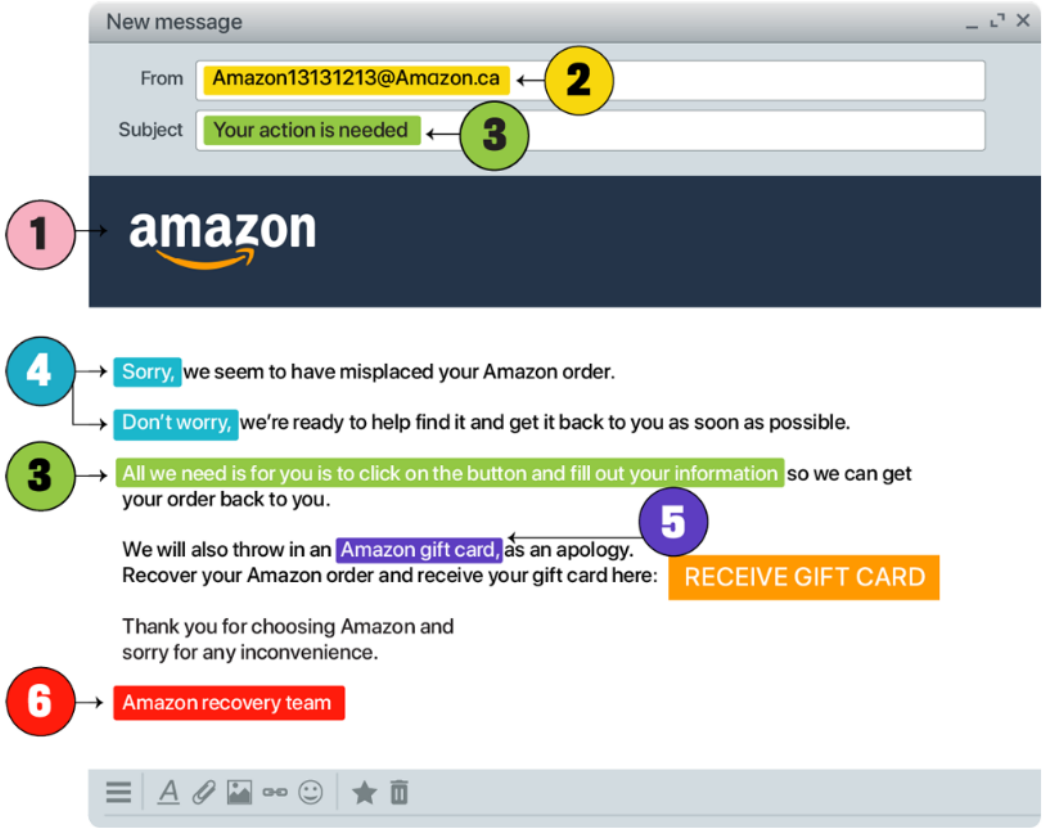


Photo credit: Government of Canada

Grandparent Scams (1/3)

Scammers call seniors, pretending to be a grandchild or official, claiming the grandchild is in trouble and urgently needs money for bail, hospital bills, or emergencies.

Video: Emergency Scams

Photo credit: Keeper Security

Grandparent Scams (2/3)

Warning Signs

- Unexpected call from someone claiming to be family.
- They need money quickly (for an accident, bail or emergencies)
- The caller asks for secrecy and immediate action.
- They pressure you for money via wire transfer, e-transfer, or cash pickup.

Grandparent Scams (3/3)

Protection Tips

- Slow down and verify (never act impulsively).
- Ask questions only the real family member would know.
- End the call and call your grandchild / family member to confirm.
- Never send money or give personal information to strangers.
- Use code words with your family as proof of identity.

Romance Scams

- Typically, the victim and scammer meet on a social media / dating site.
- The scammer will then try to develop a relationship with the victim.
- May spend several months making the victim feel they are in a romantic relationship.

Video: Romance Scams

Photo credit: Edmonton Police Services

Romance Scams are on the Rise

- Especially if you are a single woman over 40 or a widow or a widower
- With a social media account and/or dating profile
- Take advantage of your ‘loneliness’
- Tell you what you want to hear
- Find out about your personal life
- Ask you to send money

Romance Scams: Warning Signs (1/2)

- Your new friend moves too fast.
- Your love interest asks you to send money, or for payments in gift cards, cryptocurrency or through a wire transfer.
- Does your new friend have an online profile? Look for inconsistencies between what they post, and what they tell you.

Romance Scams: Warning Signs (2/2)

- If you receive a message from your friend and they use the wrong name, that may be a red flag.
- Scammers will claim that they live close to you but that they’re working overseas. They do this so that they have many reasons to ask for you for money. Be on your guard.
- If you receive a cheque or another form of payment from someone you've met online, and they ask you to cash it and send a portion of the funds back to them - don't do it.

Investment Scams

Scammers offer fake investment opportunities promising high returns with little or no risk. The use of cryptocurrency (digital currency, such as Bitcoin) is common in investment scams.

Common Warning Signs

- Pressure to “act fast” or risk missing out.
- Requests to keep the opportunity secret.
- Unsolicited calls, emails, or messages about investment opportunities.
- Limited or vague information about the company or investment product.

Video: Investment Scams

Canada Revenue Agency (CRA) Scams

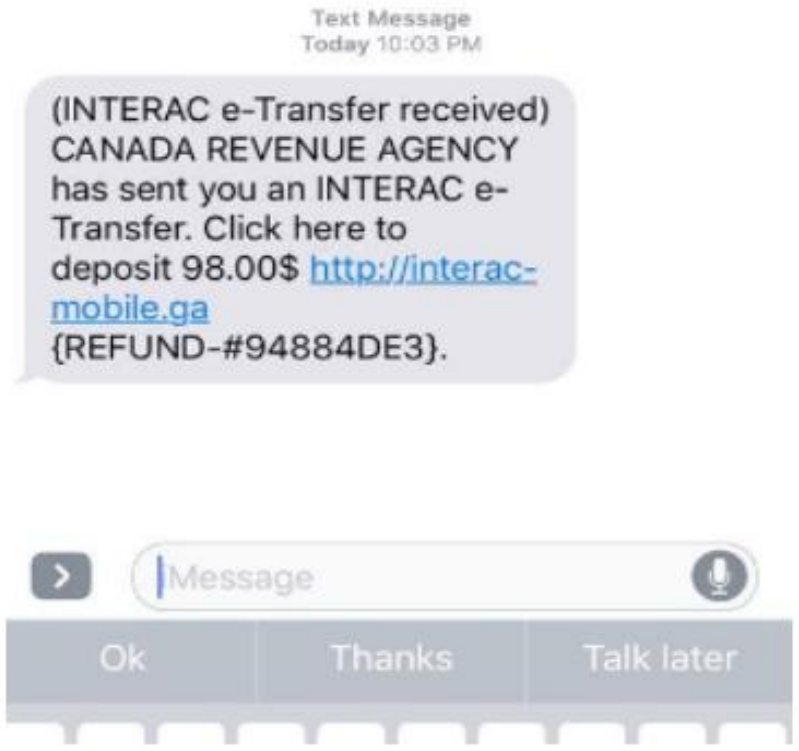
- Scammers pretend to be CRA officials and contact people by phone, text, or email.
- They claim you owe taxes, have a refund, or are under legal threat, demanding money or personal info.

Video: CRA Fraud Prevention

Photo credit: University of Alberta

The CRA Will Never:

- Use aggressive language or threats (arrest, deportation or send police).
- Ask for payment by Bitcoin, gift cards, e-transfer, or wire transfer.
- Use text messages to communicate.
- Ask or provide financial information in an email.
- Provide instructions to click suspicious links or download files.

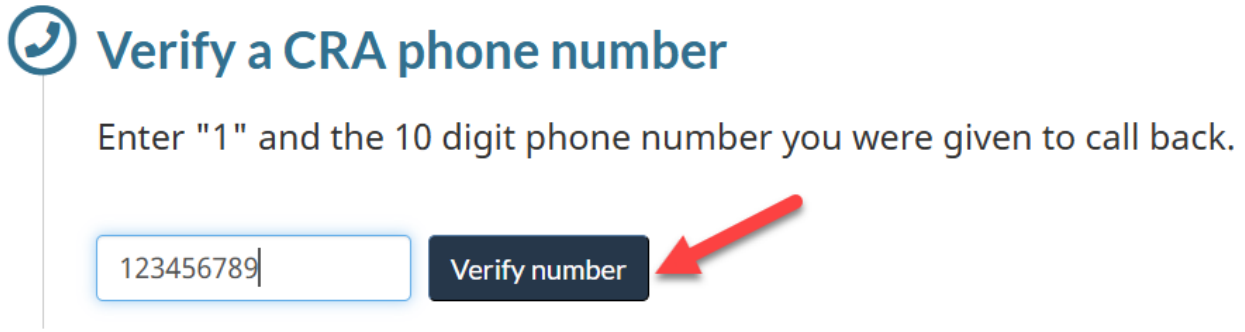


Canada Text Tax Scam

Photo credit: AG Tax

CRA Tool to Verify Phone Numbers

- Call CRA to verify at 1-800-959-8281 or login securely on the official website.
- Go to the link below to verify if it's the CRA calling: https://www.canada.ca/en/revenue-agency/corporate/scams-fraud/verify-cra-contact.html
- Enter the number in the field box and click "verify number."



Telephone Scams / Vishing

Phone scams, also known as **vishing** or telephone fraud, are fraudulent calls designed to trick individuals into giving away money or personal information.

- 1-900 calls
- Banking calls
- Credit card scams
- Income tax scams
- Emergency or “grandparent” scams
- Canada Post delivery fail scams

Door to Door Scams

Scammers posing as salespeople or representatives of legitimate businesses to pressure homeowners into making unwanted purchases or entering into unfavourable contracts:

- Home maintenance
- Repairs and renovations
- Service providers

Overpayment Scams (1/2)

These scams trick you into refunding money to a scammer who has overpaid you with a bogus cheque or a stolen credit card for an item you're selling. **How they work:**

- You place an online ad for an item such as furniture and receive an offer for the item from a "buyer"/scammer, usually by email.
- The scammer sends a cheque or money order larger than the asking price (e.g., your item is $1,500 but the scammer sends a cheque for $3,000). Sometimes, scammers may pay with stolen credit cards or online banking credentials.

Overpayment Scams (2/2)

- The scammer says the extra funds are for shipping costs or customs fees and must be sent to a third party. You deposit the cheque / money order and transfer the extra funds to the third party.
- Once the cheque / money order is processed, you learn that it was fraudulent. You will not get the money promised by the “buyer” and sent some of your own money to the third-party account – which is owned by the scammer.
- In other cases, the “buyer” might claim they have sent a larger cheque by accident, but the outcome is the same. Once you send back the “extra” funds, you discover the cheque was fake.

Protect Yourself from Overpayment Scams

- Beware of buyers who send more money than you are asking for.
- Instead of a cheque or money order, request a certified cheque.
- If you receive a cheque or money order for an amount that is more than agreed, refuse the payment and send it back to the buyer.
- Treat a money order like a cheque; these funds are not the same as cash and must be cleared and settled the same way that a cheque clears and settles.
- Make sure you wait until the cheque, e-transfer, wire transfer or money order is fully cleared and validated by your financial institution.

Artificial Intelligence (AI) Scams

- AI (technology that allows computers to think and learn like humans) scams use fake voices, images, or videos, that look and sound real to trick people online, in texts, or by phone.
- “Deepfake” videos or audio of celebrities or loved ones asking for money.
- Emails, texts, or ads with perfect grammar, real photos, and convincing stories - sometimes with your name or personal details.
- Phony investment or job offers, prizes, urgent requests to “verify” accounts, or warnings about fake emergencies.

Video: AI Generated Scams

Technology Support Scams

- You receive an urgent call, email, or pop-up claiming there is a problem with your bank account, taxes, or computer.
- You are told your computer has a virus and asked to download software or give remote access.
- They may claim that your bank account has been compromised and ask for personal information, such as a password, credit card, bank account, or Social Insurance Number to “secure” it.
- The message threatens legal action, account suspension, or financial loss if you don’t act quickly.

Other Examples of Frauds and Scams

- Bank impersonation scam
- Gift card scam
- Bank fraud calls
- Fake charity appeals
- Fake merchant scam
- Fine print scam
- Warranty, insurance and debt consolidation scams
- Website password requests scam

Reporting Scams

Canada

ST. JOHN'S

Why is Reporting Low?

The Canadian Anti-Fraud Centre estimates that **less than 5%** of fraud victims report their experiences. Why?

- Embarrassment or shame
- Fear of losing independence or being judged
- Believe nothing can be done after the scam
- Worry about upsetting family or friends
- Don’t know where or how to report

Why Reporting Matters

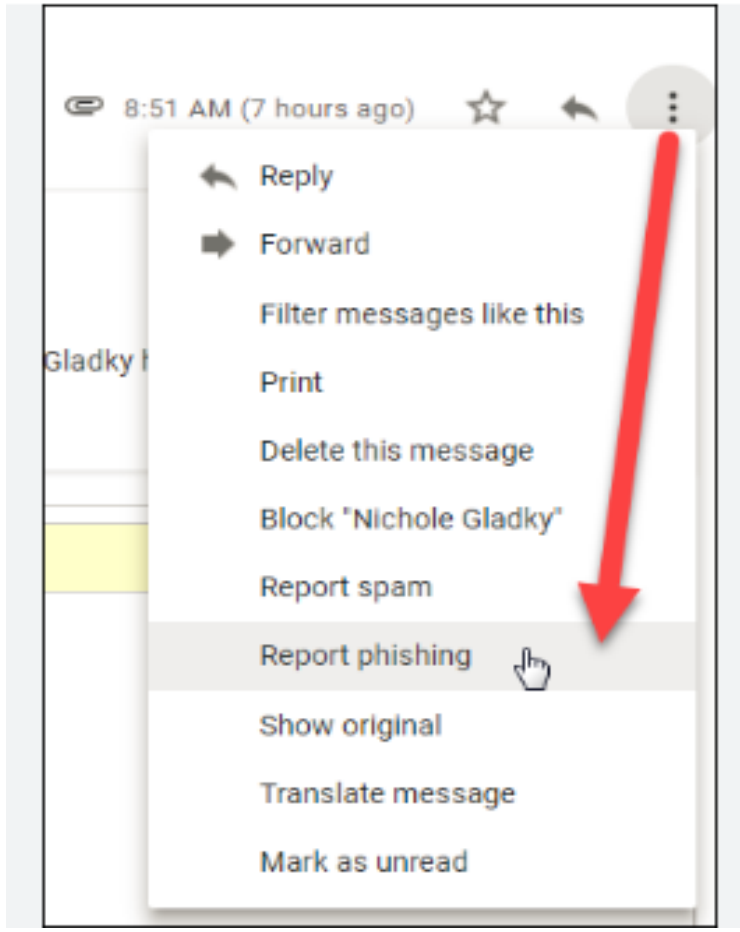
By reporting a scam, you provide law enforcement with the information they need to stop fraudsters and help prevent others from becoming victims.

What Should Be Reported?

- All suspected scams: online and phone fraud, phishing, financial fraud, identity theft, fake investments, and government impersonation.
- Any unsolicited request for personal info, money, or account access.

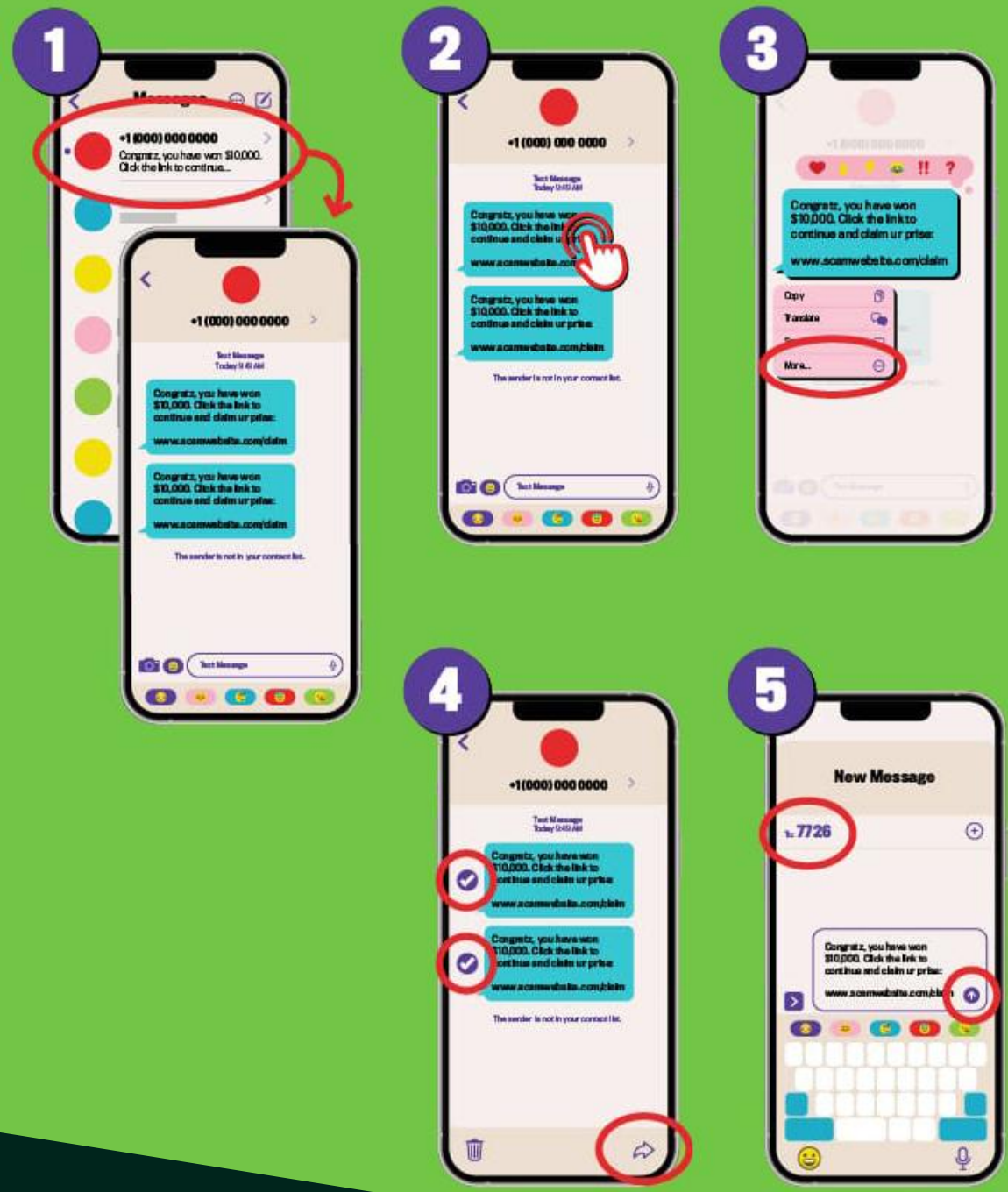
How to Report Phishing in Gmail

- To report a phishing email in Google Gmail on a computer, open the email, click the three vertical dots (More) next to the Reply button, and then select "Report phishing" from the drop-down menu.
- For the mobile Gmail app, open the email, tap the three vertical dots in the top-right corner, and then select "Report phishing".



How to Report Smishing on iPhone

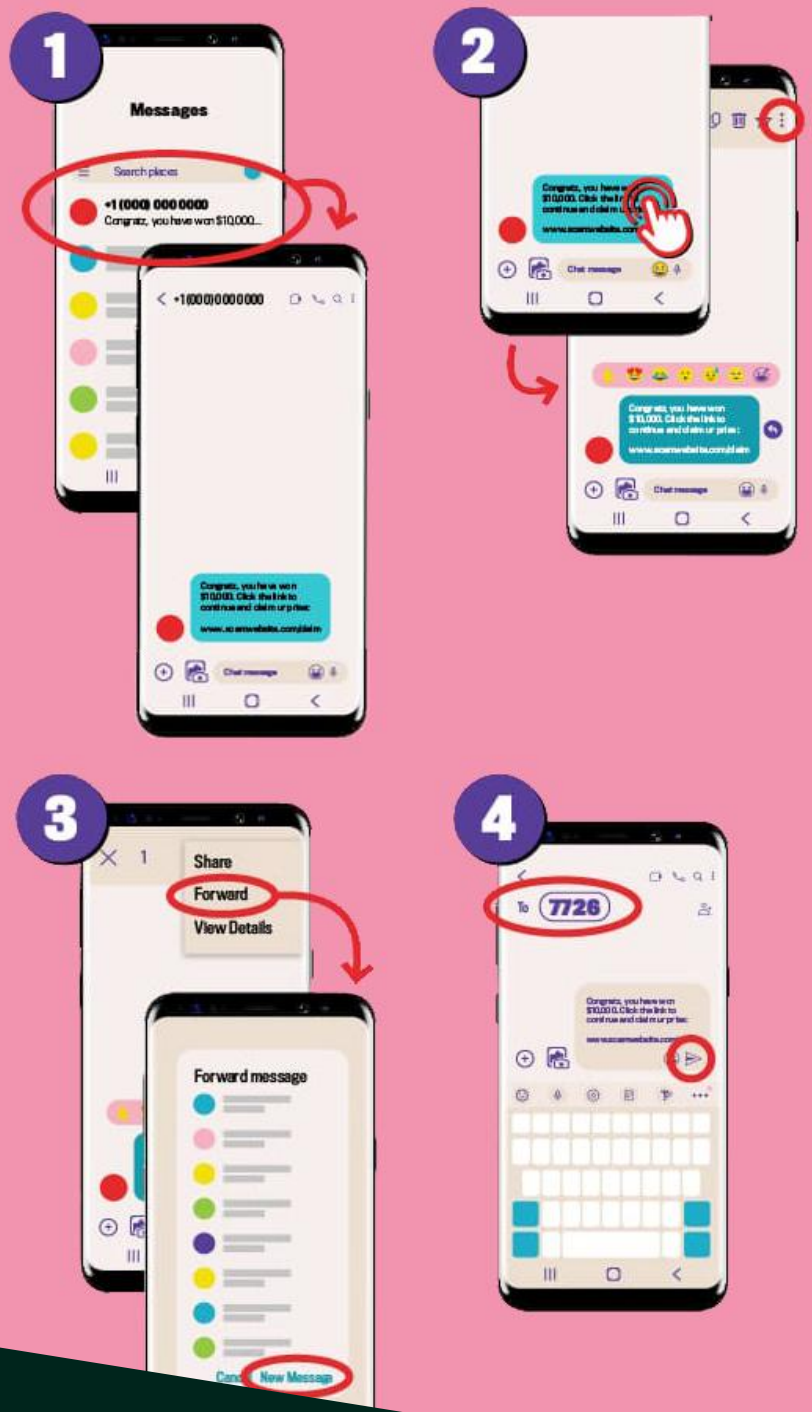
- Open the suspicious text in your Messages app.
- Press and hold the message.
- On iPhones, tap “More…” and select the messages for forwarding, tap the arrow icon (bottom right),
- Type 7726 in the “To:” field and send.



Canada ST. JOHN'S

How to Report Smishing on Android Phone

- Open the suspicious text in your Messages app.
- Press and hold the message.
- On Android phones, select “Forward” from the menu and start a new message
- Type 7726 in the “To:” field and send.



Canada ST. JOHN'S

If You've Been Scammed

Report all frauds and scams to your local police as well as the Canadian Anti-Fraud Centre.

Royal Newfoundland Constabulary (RNC):

- 1-709-729-8000
- Deaf / Hard of Hearing TTY: 1-800-363-4334

Canadian Anti-Fraud Centre:

- 1-888-495-8501
- Monday to Friday, from 9:00 am to 4:45 pm (Eastern time)

Protection Tips

Funded in part by the
Government of Canada's
New Horizons for Seniors Program

Canada

ST. JOHN'S

Protection Tips – Personal Information

- Protect your personal information.
- Keep all personal and financial documents in a secure place (e.g., in a safe, locked drawer, or a locked room).
- Do not carry your birth certificate, passport or Social Insurance Number (SIN #) unless you need them.
- Safely dispose of old bills and statements. Shredding is best.
- Never give out credit card, bank account, or personal information unless you know the organization or business, or if you made contact.

Protection Tips - Finances

- Do business with companies you know and trust.
- Regularly check your bills and bank statements.
- Avoid sensitive transactions like online banking using public Wi-Fi.
- Do not sign an agreement or contract to buy anything without giving yourself time to think it over.
- Before hiring someone ask for proof of identity and at least three (3) references.
- Be suspicious if someone you don’t know asks you to send them money, or to return money they “accidentally” sent you.

Protection Tips – Online (1/2)

- Protect your computer with anti-virus software.
- Do not click on pop-ups or respond to e-mails sent by people you don’t know.
- Only download apps and files from trusted official sources (e.g., Apple App store, Google Play store).
- Report suspicious e-mails and delete them as they can carry viruses. Let family and friends know.
- Use websites with "https" - not "http" - in their addresses when inputting bank or credit info. “s” in https means secure.

Protection Tips – Online (2/2)

- Log out of all accounts, especially on shared or public computers.
- Don't open emails from people or organizations you don't know.
- Don't accept friend requests from people you don't know and don't share private information (e.g. home address) on social media.
- Don’t believe everything you read online.
- Remember: it is unlikely that someone will declare their undying love to you after only a few e-mails, phone calls or pictures.

Password Protection

Weak passwords are made up of common words, numbers, names, birthdays or keyboard patterns. Examples include:

- 1234
- qwerty
- Jennifer1
- Password
- 0000

Best Practices for Password Protection (1/2)

- Use long, strong, and unique passwords; minimum 12-16 characters.
- Use passphrases, combine random words, numbers, and symbols (e.g., Coffee@Midnight#9528!).
- Never reuse passwords across multiple accounts to prevent one breach from affecting others.
- Avoid writing passwords down, use a reputable password manager to store and generate secure passwords.
- Change passwords quickly if there's a hint of breach or compromise.

Video: How to Create a Strong Password

Best Practices for Password Protection (2/2)

- Pick security questions only you can answer.
- Never use your date of birth or your telephone number digits.
- Never write down your on-line password but if you absolutely have to, have it disguised as something else and the paper kept in a safe out of reach place.
- Set up Alerts on your bank accounts to receive a text message/email when there is activity even if it is your own.

In Summary

Funded in part by the
Government of Canada's
New Horizons for Seniors Program

Canada

ST. JOHN'S

In a Nutshell

- If something seems too good to be true, it probably is.
- An ounce of prevention is worth a pound of cure.
- Check and double check; don’t rush into decisions.
- No legitimate company or government office will demand payment in gift cards or cash.
- Scammers change tactics and new forms of scams emerge; stay cautious, not fearful.
- Asking questions and taking time can prevent fraud
- Recognize, report and stop fraud.

Keeping Safe from Abuse

Tips for looking after your physical and emotional health and well-being:

- Stay involved. Know your rights.
- Stay connected!
- Reach out to others!
- Have fun!
- Stay physically active!
- Get support!

Acknowledgements

Funded in part by the
Government of Canada's
New Horizons for Seniors Program

Canada

ST. JOHN'S

Acknowledgments (1/2)

A very sincere thank you to Leo Bonnell, Seniors NL and Sharron Callahan for sharing resources that helped with the development of this toolkit. Also, to Suzanne Brake- Chair of the Seniors Advisory Committee, Sharron Callahan- Member of Building Safer Communities Steering Committee and Mary Ennis- SeniorsNL for their support in delivery of this presentation.

Acknowledgments (2/2)

We would also like to thank the following organization for engaging with us and providing their input and advice:

- Seniors NL
- Seniors Advisory Committee
- Connections for Seniors
- Digital Seniors NL
- Office of the Seniors' Advocate
- First Light
- YWCA St. John's
- Royal NL Constabulary
- Multicultural Women's Organization of Newfoundland and Labrador
- Public Legal Information Association of Newfoundland and Labrador
- Learning Disabilities Association of Newfoundland and Labrador
- Building Safer Communities Steering Committee
- Mental Health Foundation of Canada

Thank you!

Any Questions?

Funded in part by the
Government of Canada's
New Horizons for Seniors Program

Canada

ST. JOHN'S