How to Spot a Fraudulent Email

Be suspicious; check for these clues

- Address of sender: unknown or a risky extension. Never open files with an extension of .exe (executable file), .scr
- Subject Line: enticing you to open it? Generic or strange wording or misspelling.
- Text: poor English, spelling, capitalization, or punctuation. Is it unprofessional?

However, with Artificial Intelligence, current day phishing emails are much more professional. Never click on 'Reply' to any suspicious email. Robots send out millions of scam messages. Replying simply reveals that you are a real site, and they'll come after you.

QR Codes can be encoded with malware. A malicious sticker may be placed over the original sticker.

If Hacked:

Your mouse may become disabled. Your screen may go blank or turn red with text and maybe even a voice warning you: "Do not to turn off your computer; phone this number."

Turn off your computer by holding down the power button for a few seconds until you hear the computer turn off. Unplugging a laptop doesn't work; the battery will keep it on for four more hours! Pulling out your internet cable cuts you off from the internet: that's good too. Wait a minute or two, then turn it back on. If your computer is still disabled, bring in the professionals. If it turns on properly, run your virus protection software to clean your computer's memory. Notify your banks, credit cards; change your passwords.

Safeguards and Resources

Backup every week to an external hard drive or a large memory stick or to a site in the cloud.

Useful Contacts:

Local Police: Fraud Department:
613-549-4660
OPP: 1-888-310-1122.
Phonebusters: 1-888-495-8501
Canadian Anti-Fraud Centre,
www.antifraudcentre-centreantifraude.ca

In the case of loss of identity:
TransUnion Canada
1-800-663-9980
Equifax
1-800-465-7166
consumer.relations@equifax.com

Ask your Insurance Agent about a rider which helps you recover from Identity Theft.

Rotary Contact: Paul Van Nest,
Chair, Fraud Awareness Committee
rotarykingston@gmail.com

Version: April 2026

FRAUD AWARENESS HANDOUT

Based on Our Rotary Club's In-Person or Online Seminar

(This pamphlet is NOT intended to stand alone.)

Presented by the

Rotary Club of Kingston

FRAUD AWARENESS by Rotary Club of Kingston

Scammers think that seniors are particularly vulnerable because they think they may be more easily confused or frightened. Many seniors have money and find it hard to hang up on a telephone call or terminate an email conversation. Newly widowed seniors are perceived as more vulnerable to romance scams, even to predatory cohabittation or marriage. There is a 1 in 7 chance that a fraud or scam may be perpetrated by a family member.

Protect your identity:
Maintain a hard-copy list of your SIN, driver's license, bank cards, credit cards, passport, birth certificate, and internet passwords. Hide it. Shred all your personal papers. Guard your birthdate and your mother's maiden name. Many homeowner's insurance policies help you recover your identity if it is stolen. A rider might offer additional coverage.

Fraud/Scams In Person:
It might be a sales pitch at the door or shoulder surfing at a bank machine, or when paying with a charge card. Learn to touch-type your code while covering the keypad with your other hand. Every GPS or smartphone has a 'Home' setting: choose a nearby public building, not your home address. Otherwise, if you lose your device, it will take the finder or thief right to your home.

Fraud/Scams on the Telephone:
Fraudsters can easily set call display to look like a local call; don't rely on call display to tell the truth. Canada Revenue Agency and banks will not ask for any information over the phone. Scammers may say that they are probing an unauthorized payment or that a system reset is required. Hang up! Or they might pretend to be a family member, but they don't know the name of your cat. Establish a "family password". They may claim to be tracking an unusual credit card expenditure. If they are legitimate, they will be able to see the expenditure just prior so ask them. They'll hang up. Another ruse: "I see that your computer is not working properly." No, they can't know that; hang up! And don't press 1 when asked to, nor phone an 809 or 900 number ever: you may be paying for their long-distance calls.

Paying by gift cards or bitcoin is untraceable; don't do it. Or you may be lured to buy a sample for a few dollars, but in 14 days, a large sum may be deducted from your credit card, monthly. Using Artificial Intelligence and a voice synthesizer, they only need a few sentences to sound just like you. They then phone your family asking for money sounding just like you. Remember the family password? Never phone a number they give you. Instead look up the business number on the internet or telephone number on the back of your card. Only then will you'll know who you are really talking to. Whenever you hang up, wait five minutes before using your phone; they may be still on the line.

Fraud/Scams on the Computer:
A website may not be what it seems. It is easy to create an official-looking site. The danger on websites or emails is clicking on a button or link. If you hover your mouse over a link, the pointer becomes a hand and will display the real destination address (URL). Make sure this is an official site. A padlock icon at the beginning of the address and/or http**s**//… are generally safe sites. Be wary of the country extension on a site name, the 2 characters after the period: .ca is Canada, .ru is Russia. Check for poor grammar and spelling, and extra numbers and letters.

'Phishing' emails entice you to reveal a bank account number or a password. It may be an invitation to help someone move money from a foreign country or to become a friend who may romance you, eventually ending with a plea to send money for a plane ticket or for an ailing parent. And they are always in a hurry. Best not to speak with them at all. They may be recording your voice.