# ■■ Stay Safe Online

How to Spot Scams & Protect Yourself on Your Phone & Computer

A Sage Tutoring Guide · sage-tutoring.ca

You don't need to be a tech expert to stay safe. Scammers count on people feeling confused or embarrassed — but once you know their tricks, they lose their power. This guide will walk you through the most common scams targeting seniors today, and exactly what to do when something feels 0ff.

## The Golden Rule of Online Safety

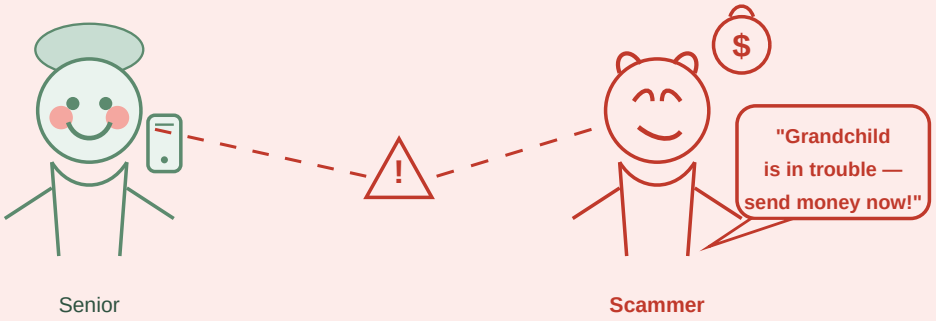
**■ If something feels wrong — it probably is. You are always allowed to hang up, close the window, or say "I need to think about it". No real company or government agency will ever pressure you to act immediately.**

**What's inside this guide:**

- ■ **7 common scams explained**
  With simple illustrations so you can spot them instantly.
- ■ **Universal warning signs**
  The red flags every scammer relies on — and how to catch them.
- ■ **What to do if targeted**
  A clear 5-step plan so you always know what to do next.
- ■ **Daily safety habits**
  Three simple things that keep you protected every day.
- ■ **Quick reference card**
  Cut it out and keep it by your phone for easy reference.

# The 7 Most Common Scams Targeting Seniors

## 1. The Grandchild Scam




**How it works:** You get a call from someone claiming to be your grandchild (or a lawyer/police officer). They say your grandchild is in trouble — arrested, in an accident, or hurt — and needs money wired urgently. They beg you not to tell other family members.

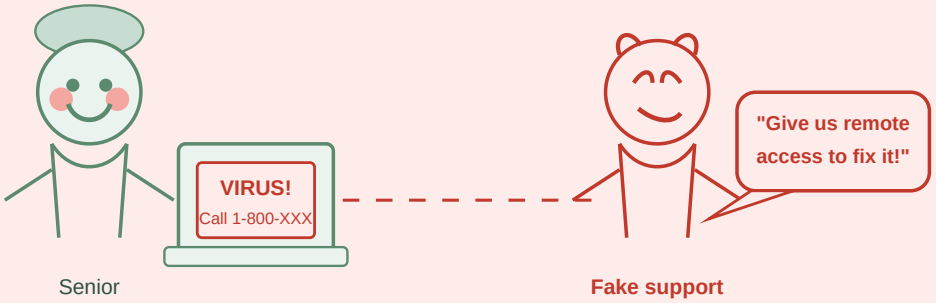
**What to do:**

✔ Hang up and call your grandchild directly on the number you already have.

✔ Call another family member to verify.

✔ Never wire money or buy gift cards based on a phone call.

## 2. The Fake Tech Support




**How it works:** A scary message appears on your screen saying your computer has a virus. It shows a phone number to call 'Microsoft' or 'Apple' immediately. If you call, they ask for remote access to your computer — and then steal your personal information or charge you hundreds of dollars for fake repairs.

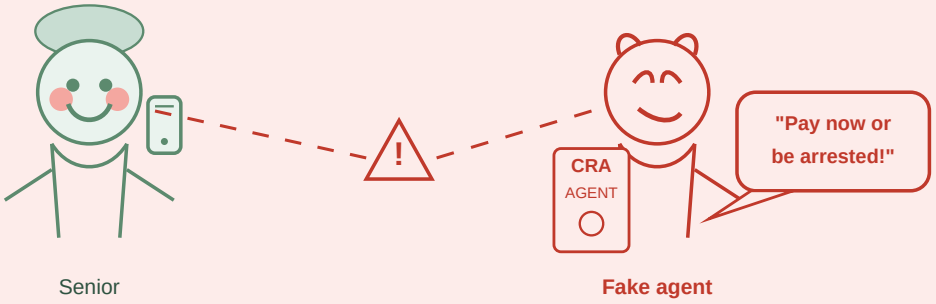
**What to do:**

✔ Do NOT call the number. Close the window (or restart your computer).

✔ Real Microsoft and Apple will NEVER call you or send pop-up warnings with phone numbers.

✔ If you're unsure, call Sage Tutoring — we can check your computer safely.

## 3. The Government Impersonator




**How it works:** Someone calls claiming to be from the CRA (Canada Revenue Agency), Service Canada, or even the police. They say you owe back taxes or have missed a benefit payment — and that you'll be arrested unless you pay immediately by gift card or wire transfer.

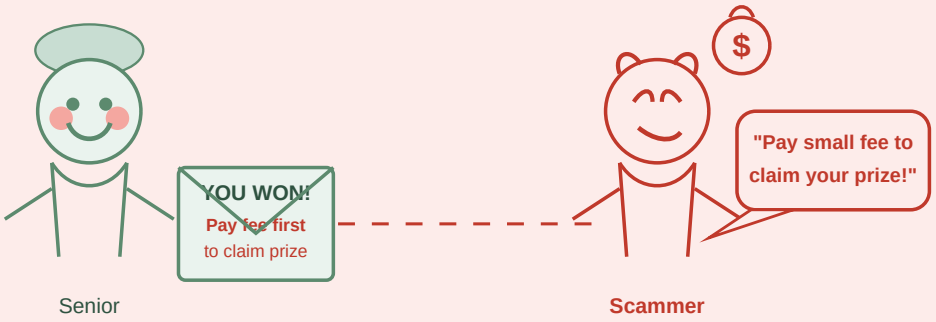
**What to do:**

✔ The CRA will NEVER demand immediate payment by gift card, Bitcoin, or wire transfer.

✔ Hang up. Then call CRA directly at 1-800-959-8281 to check if there's a real issue.

✔ Never give your SIN (Social Insurance Number) to someone who called you.

## 4. The Fake Lottery or Prize




**How it works:** You receive an email, letter, or call saying you've won a prize or lottery — but you need to pay a small fee upfront to claim your winnings. Once you pay, the 'prize' never arrives, and you may be asked for more and more money.

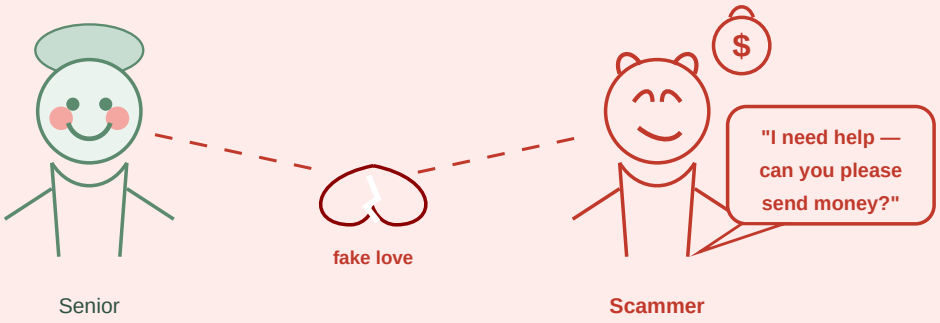
**What to do:**

✔ You cannot win a lottery you didn't enter.

✔ Never pay a fee to claim a prize. Legitimate prizes are free to collect.

✔ Delete the email or letter. Do not respond.

## 5. The Romance Scam




**How it works:** Someone reaches out on Facebook, email, or a dating site. They seem kind and interested in you. After weeks of messages, they share a sob story — an emergency, a business deal gone wrong — and ask for money. They may never ask for it directly at first, building trust over months.

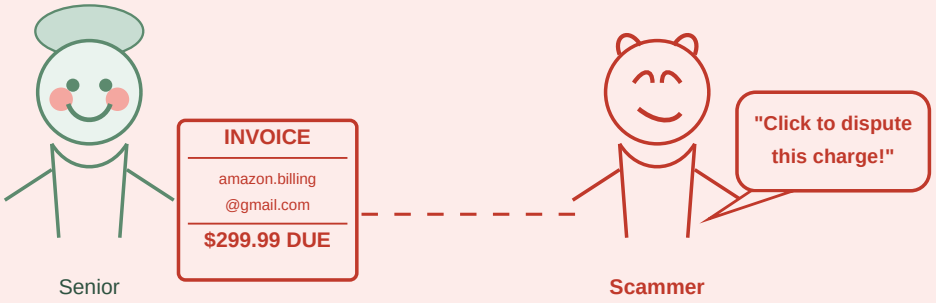
**What to do:**

✔ Be cautious of anyone online who seems 'too perfect' and has never met you in person.

✔ Never send money to someone you haven't met face-to-face.

✔ Talk to a trusted family member or friend before sending money to anyone online.

## 6. The Fake Invoice Email




**How it works:** You receive an email that looks like an official invoice or bill — from a company like Amazon, PayPal, Norton, or even your bank. It says you owe money for a purchase or subscription and asks you to click a link or call a number to dispute it. The link takes you to a fake website designed to steal your credit card or banking details.

**What to do:**

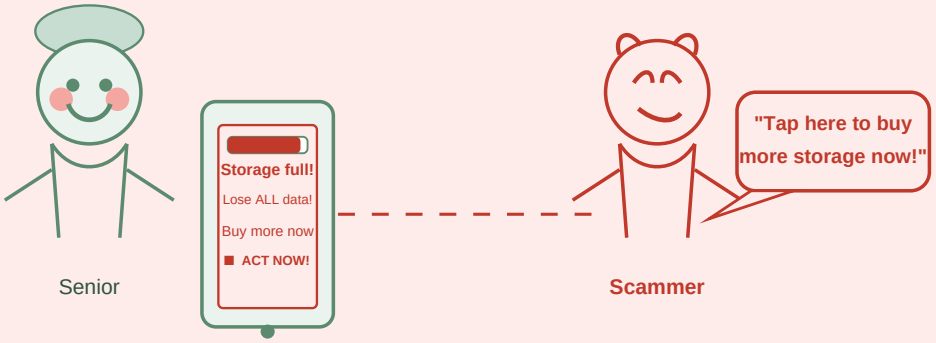
✔ Don't click any links in the email. Go directly to the company's real website by typing it yourself.

✔ Call the company using a number from their official website — NOT the number in the email.

✔ If you didn't make a purchase, it's almost certainly a scam. Delete the email.

✔ Check the sender's email address carefully — scammers use addresses like amazon-billing**@gmail.com** instead of **@amazon.com**.

## 7. The Fake Storage Warning




**How it works:** An email arrives warning that your storage is full — for your email, Google account, or iCloud — and that you'll lose all your photos, emails, and data unless you purchase more storage immediately. The email looks very official, with real-looking logos. Clicking the link takes you to a fake payment page to steal your information.

**What to do:**

✔ Don't panic and don't click the link. Real storage warnings appear inside the app itself, not by email.

✔ To check your actual storage, go directly to your Settings app on your phone or computer.

✔ Google and Apple will NEVER threaten to delete everything without warning — they give plenty of notice.

✔ If you're unsure whether your storage is really full, ask a family member or contact Sage Tutoring.

## Universal Warning Signs

No matter what form a scam takes, watch for these red flags:

- **They want you to act RIGHT NOW**
  Urgency and panic are a scammer's best tools. Real situations allow you time to think and verify.
- **They ask for gift cards or wire transfers**
  These cannot be reversed. No legitimate business, government, or family member needs you to pay this way.
- **They tell you to keep it secret**
  Anyone who says 'don't tell your family' is trying to isolate you. Always loop in someone you trust.
- **They know some personal details**
  Scammers often buy data. Knowing your name or city doesn't mean they're legitimate.
- **The offer seems too good to be true**
  Free vacations, surprise inheritances, miracle cures — if it sounds unbelievable, it is.
- **You feel confused or pressured**
  Confusion is a scam tactic. It's always okay to say 'I need time' and hang up.

## What To Do If You're Targeted

| | |
|---|---|
| Step 1 | **Stop and breathe**<br>Don't rush. Scammers want you to panic. Take a breath and remind yourself: you are in control. |
| Step 2 | **Hang up or close the window**<br>You owe nothing to a stranger. You can end a call or close a pop-up at any time, no explanation needed. |
| Step 3 | **Don't send any money or information**<br>Once money is sent by gift card or wire, it's nearly impossible to recover. When in doubt, don't send. |
| Step 4 | **Tell someone you trust**<br>Call a family member, friend, or neighbour. A fresh set of eyes helps — and you won't be judged. |

**Step 5**

**Report it**

Report to the Canadian Anti-Fraud Centre at 1-888-495-8501 or antifraudcentre.ca. Your report helps protect others.

## 3 Simple Habits to Stay Safe Every Day

### Use strong passwords

Use a different password for email, banking, and social media. A good password is at least 10 characters with a mix of letters and numbers. Consider writing them in a small notebook kept at home (not on your phone).

### Keep your devices updated

When your phone or computer says there's an update available, say yes! Updates fix security holes that scammers try to sneak through.

### When in doubt, ask

There's no such thing as a silly question when it comes to your safety. Ask a family member, or reach out to Sage Tutoring — that's exactly what we're here for.

## Quick Reference Card

*Cut this out and keep it by your phone:*

| ■ DO | ■ DON'T |
| --- | --- |
| ▪ Hang up on suspicious calls | ▪ Wire money to strangers |
| ▪ Verify by calling back on a known number | ▪ Buy gift cards as 'payment' |
| ▪ Tell a family member if something feels off | ▪ Give remote access to your computer |
| ▪ Take your time — real things can wait | ▪ Share passwords or SIN over the phone |
| ▪ Report scams to 1-888-495-8501 | ▪ Feel embarrassed — anyone can be targeted |

Need help? I'm Thuraya, the founder of Sage Tutoring. I offer patient, one-on-one tech support for seniors—at your pace, with zero pressure. Whether you want to stay safe online or simply learn your device better, I'm here to help.

**Book a free consultation at sage-tutoring.ca**
Email: thurayatutoring@gmail.com