



Aware*and* **Safe**

BE AWARE. STAY SAFE.

SAFE IN THE AGE OF AI

The Senior's Guide to Outsmarting Scams

FREE SAMPLE · CHAPTER 1

The Six Scams That Come for Seniors

From "The Senior's Guide to Outsmarting Scams" — read the full first chapter free.

The Six Scams That Come for Seniors

Scammers are not creative. That's the first thing to understand, and it's good news. There are only a handful of scripts they run, and once you know the scripts, you'll recognise them the way you recognise a telemarketer's opening line — before they've finished the first sentence.

What follows are the six scams reported most often against seniors in Canada and the United States. The details change. The shape doesn't.

1. The bank calls — but it isn't the bank

The phone rings, and the caller says they're from your bank's fraud department. There's been suspicious activity on your account. They know your name. They may know the last few digits of your card. They sound professional, calm, and concerned. They need you to "verify" your identity — your full card number, your PIN, the code that just arrived by text — so they can "protect" your money.

Here is the rule that defeats this scam every time: **your bank will never ask you for your PIN, your full password, or a security code over the phone.** Not to verify you. Not to

protect you. Not ever. A real bank employee who needs to reach you will ask you to call back on the number printed on your bank card, or to visit a branch. Anyone who pressures you to stay on the line and give them codes is not from your bank, no matter what the call display says.

About that call display: scammers can fake it. The technology is called "spoofing," and it lets them make any name and number appear on your screen — including your bank's real number. So "the bank's number showed up" proves nothing. The only proof that counts is a call *you* placed, to a number *you* looked up yourself.

2. The grandchild in trouble

This one deserves its own chapter — Chapter 2 is entirely about it — but it belongs on this list because it's the scam seniors report most often. A young voice calls, crying or whispering. "Grandma? It's me. I'm in trouble." A car accident. An arrest. A hospital in another city. They need money wired right away, and please don't tell Mom and Dad.

The classic version relied on the caller sounding vaguely like a grandchild and on your love doing the rest. The new version, powered by artificial intelligence, can sound *exactly* like your grandchild. We'll take this apart properly in the next chapter. For now, remember the shape: an emergency, a demand for secrecy, and a demand for money sent in a way you can't reverse.

3. The new romance

This one usually starts on Facebook, on a dating site, or sometimes through a wrong-number text that turns friendly. Someone charming appears. They're attentive. They remember details. They may send photos — handsome or beautiful, always a little too polished. Over weeks or months, a relationship grows. Then comes the crisis: a medical bill, a business emergency, a plane ticket to finally meet you. They can't use their own bank account "for reasons." Could you wire the money, or buy gift cards?

Romance scams are cruel in a specific way: they exploit loneliness and then weaponise the victim's own hope. The person on the other end is not who the photos show. The photos are stolen. The crisis is invented. And the money, once sent, funds an organised operation that runs this same script on dozens of people simultaneously.

Two rules protect you. First, **never send money to someone you haven't met in person**, no matter how long you've been talking and no matter how real it feels. Second, tell someone in your life about the relationship early — a friend, a child, a neighbour. Scammers depend on secrecy. Sunlight ends them.

4. Your computer has a virus

A message pops up on your screen — sometimes with alarming red text and a loud warning sound — saying your computer is infected and you must call a number immediately. Or the phone rings and someone from

"Microsoft" or "your internet company" says they've detected a problem. They're helpful. They'll fix it for you. They just need remote access to your computer — "so I can see what you see" — and your credit card for the repair fee.

No legitimate technology company calls you out of the blue about your computer. Not Microsoft, not Apple, not your internet provider. Ever. The pop-up is fake; it's an advertisement designed to look like a warning. The caller is a criminal. If you grant remote access, they can install real malicious software, steal your files and passwords, and lock you out of your own machine.

If a scary warning appears on your screen, do this: turn the computer off, wait a minute, and turn it back on. If the warning is gone, it was fake. If something still seems wrong, take the computer to a local shop you know, or ask a family member for help. Never call the number on the warning.

5. You've won a prize

"You've won a lottery!" "A cruise!" "A government grant for seniors!" The prize is always exciting and always just out of reach — there's a "processing fee," or "taxes" to pay first, or you need to provide your bank details "so we can deposit your winnings."

Real lotteries don't work this way. You cannot win a lottery you never entered. Governments don't award grants by cold-calling. And no legitimate prize in the history of prizes has ever required the winner to pay money to receive it. The "fee" is the entire scam; there is no prize.

There's a nastier cousin of this one aimed specifically at seniors: the "government benefit" call. Someone claims to be from a pension office or tax agency, saying you're owed money or that your benefits will be cut off unless you "confirm" your banking details. Government agencies in Canada — the CRA, Service Canada, Old Age Security — do not demand banking details or payments by phone, and they do not threaten arrest. If you're unsure about anything related to your benefits, call the agency yourself using the number on their official website or on a letter you received in the mail.

6. The friendly contractor

A knock at the door. Someone noticed your roof, your driveway, your eavestroughs while "working in the neighbourhood." They can fix it today, cheap, cash only. Or they start a small job and discover — surprise — much bigger problems that need immediate, expensive work.

Legitimate contractors don't solicit door to door, don't demand cash up front, and don't pressure you to decide today. Get three written quotes for any significant work. Never pay in full before the job is done. And be especially wary of anyone who shows up right after a storm — that's when the travelling repair crews come through, and not all of them intend to finish what they start.

The thread that connects them all

Look at the six scripts again and you'll see the same machinery underneath: **contact out of nowhere, a story that creates urgency or strong emotion, a request for money or**

information, and pressure to act before you can think or check. Artificial intelligence has made the stories more convincing — better voices, better letters, better websites — but it hasn't changed the machinery. That's why the defence in Chapter 3 works against all of them.

KEY TAKEAWAYS

1. **There are only a handful of scam scripts.** Learn the six in this chapter and you'll recognise new versions on sight — the details change, the shape doesn't.
2. **Your bank will never ask for your PIN, password, or security code by phone.** Anyone who does is a scammer, regardless of what your call display shows.
3. **Never send money to someone you haven't met in person,** no matter how long the online relationship or how urgent the crisis sounds.
4. **No real tech company calls about your computer.** A scary pop-up is an ad; turn the computer off and on again, and never call the number on the warning.
5. **You can't win a prize you didn't enter, and real prizes never charge fees.** Government agencies don't demand payments or banking details by phone either.

Enjoyed this chapter?

This was Chapter 1 of *The Senior's Guide to Outsmarting Scams*, part of the *Safe in the Age of AI* series by Aware and Safe. The complete handbook includes every chapter, all the checklists, and the companion resources — available now in the edition that suits you.

Ebook + Audiobook Bundle

\$8.99

Everything together — the best value.

<https://awareandsafe.com/product/seniors-guide-to-outsmarting-scams-ebook-audiobook-bundle/>

Ebook

\$6.99

Premium PDF — read on any device.

<https://awareandsafe.com/product/seniors-guide-to-outsmarting-scams-ebook/>

Audiobook

\$4.99

Full MP3 narration + companion PDF.