SCAM WATCH · CANADA · WEEKLY EDITION · November 24, 2026

Is This a Scam?

A plain-language guide to the scams hitting Canadians right now — on your phone, your inbox and your feed.

Brought to you by: **lennartandersen.xyz**

If you just clicked, paid, or gave out a code

1. **Call your bank** on the number on the back of your card. Ask them to stop or reverse the payment — minutes matter.
2. **Change that password** from a different device, and turn on two-step verification. If you reused it elsewhere, change it there too.
3. **Report it** to the Canadian Anti-Fraud Centre — even if you lost nothing. Your report helps stop the next person.

Who to contact in Canada

REPORT IT

Canadian Anti-Fraud Centre

1-888-495-8501

National fraud reporting centre. Mon–Fri, 10am–4:45pm Eastern. Report online any time at antifraudcentre.ca.

REPORT IT

Scam text message

Forward to 7726

7726 spells SPAM. Free on every Canadian carrier — they use it to block the sender. Then delete the text.

CALL NOW

Your local police

Non-emergency line

If you lost money or are being threatened or blackmailed online, file a police report. Emergency: 911.

PROTECT YOUR ID

Equifax & TransUnion

Credit bureaus

If you gave out your SIN, driver's licence or passport, place a fraud alert with both credit bureaus.

Six rules that protect you online

- **A surprise text with a link is a scam until proven otherwise.** Canada Post, CRA, highway tolls, your bank — go to their app or website yourself, never through the link.
- **Never share a code.** A one-time code sent to you is the key to your account. Nobody legitimate will ever ask you to read it back.
- **Guaranteed returns are a lie.** Celebrity-backed crypto, "AI trading bots," and friends-of-friends tips are the biggest money-losers in Canada.
- **Turn on automatic updates** on your phone, computer and browser. Most hacks use flaws that already have a fix.
- **Use two-step verification and a password manager** (or passkeys) on email and banking — your email resets every other account.
- **Gift cards, crypto and wire transfers are scam payments.** No real company, government or employer will ever demand them.

The scams Canadians are losing money to

Delivery, toll or tax "unpaid" text

A text says a parcel is held, a highway toll is overdue, or a CRA refund is waiting. A link leads to a perfect copy of the real site asking for your card.

> **Giveaway:** A small amount, a tight deadline, and a link. Real agencies don't collect payments by text.

Marketplace and rental scams

A great deal on Facebook Marketplace or Kijiji — a car, concert tickets, an apartment — but the seller is "away" and needs a deposit by e-Transfer first.

> **Giveaway:** You can't see the item or the unit in person before paying. Never pay a deposit sight unseen.

Investment and crypto scams

An ad shows a famous Canadian — often a deepfake video — praising a platform. A friendly "advisor" shows you growing profits on a dashboard, then asks you to add more.

> **Giveaway:** You can't withdraw without paying a "fee" or "tax" first. Check any firm at aretheyregistered.ca.

Account takeover & fake support

A "security alert" text or call from your bank, Amazon or your phone company says your account is compromised and asks you to confirm a code or move money.

> **Giveaway:** They ask for a code you just received. That code is them logging in as you.

Online "task" job

A recruiter messages you on WhatsApp or Telegram: earn money rating products or liking videos. Small payouts arrive at first — then you must deposit to unlock bigger tasks.

> **Giveaway:** A job that requires you to pay in, usually in crypto. Real jobs pay you.

Sextortion and blackmail

Someone you met online — or a stranger claiming to have hacked your camera — threatens to share intimate images unless you pay. Teens are heavily targeted.

> **Giveaway:** Instant pressure to pay. Don't pay, stop replying, keep the messages and report to police — for youth, also cybertip.ca.

Update these now — attackers are using them this month

Flaws in common consumer products that attackers are actively exploiting, added in the last 30 days to the U.S. CISA Known Exploited Vulnerabilities list (cisa.gov/kev). Data as of November 24, 2026.

If you use	How to update	Flagged
Microsoft Office CVE-2026-124194	Open any Office app → File → Account → Update Options → Update Now.	2026-11-10
Google Chrome CVE-2026-125350	Menu (⋮) → Help → About Google Chrome, then click Relaunch.	2026-11-10
iPhone, iPad & Mac CVE-2024-27834	Settings → General → Software Update (Mac: System Settings → General → Software Update).	2026-11-04

The number on your screen can be faked

Scammers can make any number show up on your phone — even the real number of your bank, the police or the CRA. This is called **spoofing**. If a call asks for money, codes or personal details, **hang up and call back** on the number on your card or the official website.

Blocking scam callers on your own phone

- **Android:** Phone app → Settings → *Caller ID & spam* → turn on spam filtering (Samsung: *Caller ID and spam protection*). Pixel phones also have *Call Screen*, which answers unknown callers for you.
- **iPhone:** Settings → Phone (newer iOS: Settings → Apps → Phone) → *Silence Unknown Callers* sends numbers not in your contacts to voicemail.
- **Single numbers:** block them from your recent-calls list. It helps a little, but scammers change numbers all the time.
- **Your phone company:** most offer free spam-call filtering in their app or account settings — ask them.
- **Scam texts:** forward them to **7726** (SPAM). Your carrier uses the reports to block scam links.

This is general information, not legal, financial or police advice. Phone numbers were checked against the organizations' own websites (last checked November 2026), but numbers and procedures change — always confirm a number through the official website before you rely on

it. In an emergency, always call 911. Live section generated automatically on November 24, 2026 from public feeds; it lists only flaws in widely used consumer products.