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

Scams and Security Alerts for Your Business

A plain-language guide for Canadian small businesses — the fraud that drains accounts, and the bugs attackers are using right now.

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

If you think you've just been hit

1. **Call your bank's fraud line now.** A wire or e-Transfer can sometimes be recalled — but only within hours.
2. **Don't reply to the email.** Phone the person or supplier on a number you already had on file.
3. **Unplug, don't wipe.** Disconnect an infected computer from the network but leave it on — evidence helps recovery and insurance.

Who to contact in Canada

REPORT IT

Canadian Anti-Fraud Centre

1-888-495-8501

Report fraud against your business. Mon–Fri, 10am–4:45pm Eastern, or online at antifraudcentre.ca.

REPORT IT

Canadian Centre for Cyber Security

cyber.gc.ca

Report a cyber incident (ransomware, hacked email, data breach) online via "Report a cyber incident".

CALL NOW

Your bank's business fraud line

Number on your card

First call after any suspicious payment. Ask for a recall and a fraud hold on the account.

CALL NOW

Your local police

Non-emergency line

File a report for any loss — insurers and banks usually require the file number.

Six rules that stop most business fraud

- **Verify every bank-detail change by phone.** New account for a supplier? Call them on the number you already had — never the one in the email.
- **Two people approve payments.** Any new payee or large transfer needs a second person's sign-off. Urgent requests get no exceptions.
- **Turn on two-step verification** for email, banking, payroll and accounting. Hacked email is behind most business fraud.
- **Patch internet-facing software within days,** not months — website, VPN, firewall, email server. See the live list overleaf.
- **Keep backups offline and test them.** If ransomware hits, a tested backup is the difference between a bad day and closing down.
- **No one pays in gift cards.** A "boss" texting staff to buy gift cards for a client is a scam, every time.

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.

Patch now — bugs attackers are exploiting this month

Added in the last 30 days to the U.S. CISA Known Exploited Vulnerabilities list (cisa.gov/kev) — attackers are using these in the wild. If your business, web host or IT provider runs any of these, update now. Data as of November 24, 2026.

Software	Vulnerability IDs	Flagged
Broadcom VMware vCenter	CVE-2026-123890	2026-11-20
Cisco Expressway Series	CVE-2026-76466	2026-11-20
Synology DiskStation Manager (DSM) RANSOMWARE	CVE-2024-10441	2026-11-18
Microsoft Office	CVE-2026-124194	2026-11-10
Cisco BroadWorks	CVE-2026-20320	2026-11-10
Barracuda Networks Multiple Products	CVE-2026-111560	2026-11-10
Barracuda Email Security Gateway (ESG)	CVE-2026-116606	2026-11-10
Google Chromium	CVE-2026-125350	2026-11-10
SonicWall SonicOS SSLVPN	CVE-2026-19868	2026-11-06
Apple Multiple Products	CVE-2024-27834	2026-11-04
WordPress Core	CVE-2026-119977	2026-11-03
Ivanti Connect Secure	CVE-2026-118527, CVE-2026-111357	2026-10-30
Secure Firewall ASA Software and Cisco Secure FTD Software	CVE-2026-76418	2026-10-29
Broadcom VMware ESX	CVE-2026-41709	2026-10-28
Adobe Commerce and Magento	CVE-2026-48356	2026-10-27

Don't run your own servers? Forward this page to your web host or IT provider and ask: "Are we affected, and is it patched?"

Latest Canadian Cyber Centre alerts

Alerts (AL) — the serious ones

- **AL26-029** 2026-11-17 — Critical vulnerability impacting Oracle Java - CVE-2026-114938
- **AL26-028** 2026-10-28 — Ongoing Help Desk Voice Phishing Campaign Targeting Canadian Organizations
- **AL26-027** 2026-10-28 — Critical vulnerability impacting Google Brotli – CVE-2026-111497
- **AL26-026** 2026-10-27 — Critical vulnerabilities impacting PHP - CVE-2026-109618 and CVE-2026-109619 - Update 2

Advisories (AV)

- **AV26-1204** 2026-11-24 — Erlang security advisory
- **AV26-1186** 2026-11-24 — Drupal security advisory – Update 1
- **AV26-1203** 2026-11-24 — VMware security advisory
- **AV26-1202** 2026-11-24 — Tanium security advisory
- **AV26-1201** 2026-11-24 — Google security advisory
- **AV26-1200** 2026-11-24 — n8n security advisory

Full details: cyber.gc.ca → Alerts and advisories.

Linux servers — critical bugs attackers are exploiting

The 10 Linux kernel and Linux-distribution flaws most recently added to the CISA list. Most websites, cloud servers, VPS and NAS boxes run Linux. Kernel fixes only take effect after a **reboot** — ask your host or IT provider: "Is the kernel updated, and has the server been restarted?"

Software	CVE	Flagged	Software	CVE	Flagged
OpenBSD OpenSSH	CVE-2026-123158	2026-11-09	**Linux Kernel**	CVE-2026-53362	2026-08-27
Linux Kernel	CVE-2026-46300	2026-10-28	**Red Hat Libuser**	CVE-2015-3246	2026-08-26
Linux Kernel	CVE-2025-39964	2026-09-18	**Red Hat Automatic Bug Reporting Tool**	CVE-2015-5287	2026-08-26
Linux Kernel	CVE-2026-53266	2026-09-18	**Linux Kernel**	CVE-2022-0995	2026-08-26
Linux Kernel	CVE-2025-39682	2026-09-18	**Linux Kernel**	CVE-2022-0492	2026-06-02

The scams that hit Canadian businesses

Supplier "new bank details" email

A real supplier's email — or a near-identical address — says their banking has changed and the next invoice should go to a new account. Often sent from a genuinely hacked mailbox.

> **Giveaway:** Any change of payment details by email. Call the supplier on a known number before paying.

Fake government or CRA business call

A caller says your business number is under audit, GST/HST is overdue, or a licence will be suspended unless you pay today.

> **Giveaway:** The CRA never demands immediate payment by gift card, crypto or e-Transfer. Check your My Business Account yourself.

CEO or boss impersonation

A message "from the owner" — sometimes a cloned voice on the phone — asks finance to make an urgent, confidential payment or buy gift cards for a client.

> **Giveaway:** Secrecy plus urgency plus "I can't talk right now." Confirm in person or by calling back.

Fake invoices and directory listings

Bills for domain renewals, "trademark registry" fees, online directory listings or office supplies you never ordered — hoping someone in accounts just pays them.

> **Giveaway:** A vendor you've never used, or fine print saying you "agreed" on a phone call.

Ransomware from one click

A staff member opens a fake invoice, shipping notice or shared document. Days later every file is encrypted and a ransom note appears.

> **Giveaway:** Unexpected attachments and "sign in to view this document" pages. Report, don't click.

Fake tech support and "your account is locked"

A call or pop-up claims to be Microsoft or your IT provider and asks staff to install remote-access software or approve a login prompt.

> **Giveaway:** An unexpected approval request on your phone. If you didn't just log in, deny it and tell IT.

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 sections generated automatically on November 24, 2026 from the CISA KEV catalog and the Canadian Centre for Cyber Security feed; they are not an assessment of your systems.