VIGIE FRAUDE · CANADA · PETITES ENTREPRISES · ÉDITION HEBDOMADAIRE · 24 novembre 2026

Fraudes et alertes de sécurité pour votre entreprise

Un guide en langage clair pour les petites entreprises canadiennes — les fraudes qui vident les comptes, et les failles que les pirates exploitent en ce moment.

Une initiative de : **lennartandersen.xyz**

Si vous pensez venir d'être victime

1. **Appelez immédiatement la ligne antifraude de votre banque.** Un virement télégraphique ou Interac peut parfois être rappelé — mais seulement dans les heures qui suivent.
2. **Ne répondez pas au courriel.** Téléphonez à la personne ou au fournisseur à un numéro que vous aviez déjà en dossier.
3. **Débranchez, n'effacez rien.** Déconnectez l'ordinateur infecté du réseau, mais laissez-le allumé — les preuves aident à la récupération et aux assurances.

Qui contacter au Canada

SIGNALEZ-LE

Centre antifraude du Canada

1-888-495-8501

Signalez une fraude visant votre entreprise. Du lundi au vendredi, de 10 h à 16 h 45 (heure de l'Est), ou en ligne : antifraudcentre.ca.

SIGNALEZ-LE

Centre canadien pour la cybersécurité

cyber.gc.ca

Signalez un cyberincident (rançongiciel, courriel piraté, atteinte aux données) en ligne avec le formulaire « Signaler un incident ».

APPELEZ

Ligne antifraude de votre banque

Numéro sur votre carte

Premier appel après tout paiement suspect. Demandez un rappel du paiement et un gel du compte pour fraude.

APPELEZ

Votre police locale

Ligne non urgente

Faites une déclaration pour toute perte — les assureurs et les banques exigent généralement le numéro de dossier.

Six règles qui stoppent la plupart des fraudes

- **Vérifiez par téléphone tout changement de coordonnées bancaires.** Nouveau compte pour un fournisseur? Appelez-le au numéro que vous aviez déjà — jamais à celui du courriel.
- **Deux personnes approuvent les paiements.** Tout nouveau bénéficiaire ou gros virement exige l'approbation d'une deuxième personne. Aucune exception pour les demandes urgentes.
- **Activez la vérification en deux étapes** pour les courriels, les services bancaires, la paie et la comptabilité. Un courriel piraté est à l'origine de la plupart des fraudes.
- **Corrigez les logiciels exposés à Internet en quelques jours,** pas en quelques mois — site Web, RPV, pare-feu, serveur de courriel. Voir la liste en direct au verso.
- **Gardez des sauvegardes hors ligne et testez-les.** En cas de rançongiciel, une sauvegarde testée fait la différence entre une mauvaise journée et la fermeture.
- **Personne ne paie en cartes-cadeaux.** Un « patron » qui texte un employé pour acheter des cartes-cadeaux pour un client, c'est une fraude, chaque fois.

Le numéro affiché peut être truqué

Un fraudeur peut afficher le vrai numéro de votre banque, de la police ou de l'ARC (**usurpation de numéro**). On vous demande de l'argent ou des codes? **Raccrochez et rappelez** au numéro de votre carte.

Bloquer les appels frauduleux sur votre téléphone

- **Android :** Téléphone → Paramètres → *Identification de l'appelant et spam* → activez le filtrage.
- **iPhone :** Réglages → Téléphone (ou Apps → Téléphone) → *Inconnus en silence*.
- **Numéros précis :** bloquez-les depuis les appels récents.
- **Votre fournisseur :** demandez son filtrage gratuit des appels indésirables.
- **Textos frauduleux :** transférez-les au **7726** (SPAM).

Corrigez maintenant — failles exploitées par des pirates ce mois-ci

Ajoutées au cours des 30 derniers jours à la liste des vulnérabilités exploitées connues (KEV) de la CISA (cisa.gov/kev) des États-Unis — des pirates les utilisent activement. Si votre entreprise, votre hébergeur Web ou votre fournisseur TI utilise l'un de ces logiciels, mettez-le à jour maintenant. Données au 24 novembre 2026.

Logiciel	Identifiants de vulnérabilité	Signalé le
Broadcom VMware vCenter	CVE-2026-123890	2026-11-20
Cisco Expressway Series	CVE-2026-76466	2026-11-20
Synology DiskStation Manager (DSM) RANÇONGICIEL	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

Vous ne gérez pas vos propres serveurs? Transmettez cette page à votre hébergeur Web ou à votre fournisseur TI et demandez : « Sommes-nous touchés, et le correctif est-il appliqué? »

Dernières alertes du Centre canadien pour la cybersécurité

Alertes (AL) — les plus graves

- **AL26-029** 2026-11-17 — Vulnérabilité critique affectant Oracle Java - CVE-2026-114938
- **AL26-028** 2026-10-28 — Campagne continue d'hameçonnage vocal lié au soutien technique ciblant des organisations canadiennes
- **AL26-027** 2026-10-28 — Vulnérabilité critique touchant Google Brotli – CVE-2026-111497
- **AL26-026** 2026-10-27 — Vulnérabilités critiques touchant PHP – CVE-2026-109618 et CVE-2026-109619 - Mise à jour 2

Avis (AV)

- **AV26-1204** 2026-11-24 — Bulletin de sécurité Erlang
- **AV26-1186** 2026-11-24 — Bulletin de sécurité Drupal – Mise à jour 1
- **AV26-1203** 2026-11-24 — Bulletin de sécurité VMware
- **AV26-1202** 2026-11-24 — Bulletin de sécurité Tanium
- **AV26-1201** 2026-11-24 — Bulletin de sécurité Google
- **AV26-1200** 2026-11-24 — Bulletin de sécurité n8n

Détails complets : cyber.gc.ca → Alertes et avis.

Serveurs Linux — failles critiques exploitées par les pirates

Les 10 failles du noyau Linux et des distributions Linux ajoutées le plus récemment à la liste de la CISA. La plupart des sites Web, serveurs infonuagiques, VPS et NAS fonctionnent sous Linux. Les correctifs du noyau ne s'appliquent qu'après un **redémarrage** — demandez à votre hébergeur ou fournisseur TI : « Le noyau est-il à jour, et le serveur a-t-il été redémarré? »

Logiciel	CVE	Signalé	Logiciel	CVE	Signalé
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

Les fraudes qui frappent les entreprises canadiennes

Courriel de « nouvelles coordonnées bancaires »

Le courriel d'un vrai fournisseur — ou d'une adresse presque identique — annonce que ses coordonnées bancaires ont changé et que la prochaine facture doit être payée dans un nouveau compte. Souvent envoyé d'une boîte de courriel réellement piratée.

> **Signe révélateur :** Tout changement de coordonnées de paiement par courriel. Appelez le fournisseur à un numéro connu avant de payer.

Usurpation de l'identité du PDG ou du patron

Un message « du propriétaire » — parfois une voix clonée au téléphone — demande à la comptabilité d'effectuer un paiement urgent et confidentiel ou d'acheter des cartes-cadeaux pour un client.

> **Signe révélateur :** Secret, urgence et « je ne peux pas parler en ce moment ». Confirmez en personne ou en rappelant.

Un rançongiciel en un seul clic

Un employé ouvre une fausse facture, un avis d'expédition ou un document partagé. Quelques jours plus tard, tous les fichiers sont chiffrés et une demande de rançon apparaît.

> **Signe révélateur :** Des pièces jointes inattendues et des pages « connectez-vous pour voir ce document ». Signalez, ne cliquez pas.

Faux appel du gouvernement ou de l'ARC

Un interlocuteur affirme que votre numéro d'entreprise fait l'objet d'une vérification, que la TPS/TVH est en retard ou qu'un permis sera suspendu si vous ne payez pas aujourd'hui.

> **Signe révélateur :** L'ARC n'exige jamais de paiement immédiat par carte-cadeau, cryptomonnaie ou virement Interac. Vérifiez vous-même dans Mon dossier d'entreprise.

Fausses factures et inscriptions à des répertoires

Des factures pour un renouvellement de nom de domaine, des frais de « registre des marques », une inscription à un répertoire en ligne ou des fournitures de bureau jamais commandées — en espérant que quelqu'un à la comptabilité les paie.

> **Signe révélateur :** Un fournisseur avec qui vous n'avez jamais fait affaire, ou des petits caractères affirmant que vous avez « accepté » au téléphone.

Faux soutien technique et « votre compte est verrouillé »

Un appel ou une fenêtre se présente comme Microsoft ou votre fournisseur TI et demande à un employé d'installer un logiciel d'accès à distance ou d'approuver une demande de connexion.

> **Signe révélateur :** Une demande d'approbation inattendue sur votre téléphone. Si vous ne venez pas de vous connecter, refusez-la et avisez les TI.

Ce document fournit de l'information générale et ne constitue pas un avis juridique, financier ou policier. Les numéros de téléphone ont été vérifiés sur les sites officiels des organismes (dernière vérification : novembre 2026), mais les numéros et les procédures changent — confirmez toujours un numéro sur le site officiel avant de vous y fier. En cas d'urgence, composez toujours le 911. Sections en direct générées automatiquement le 24 novembre 2026 à partir du catalogue KEV de la CISA et du flux du Centre canadien pour la cybersécurité; elles ne constituent pas une évaluation de vos systèmes.