VIGIE FRAUDE · CANADA · ÉDITION HEBDOMADAIRE · 24 novembre 2026

Est-ce une fraude?

Un guide en langage clair sur les fraudes qui ciblent les Canadiens en ce moment — sur votre téléphone, dans vos courriels et sur les réseaux sociaux.

Une initiative de : **lennartandersen.xyz**

Si vous venez de cliquer, de payer ou de donner un code

1. **Appelez votre banque** (numéro au dos de la carte) pour arrêter le paiement.
2. **Changez ce mot de passe** et activez la vérification en deux étapes.
3. **Signalez-le** au Centre antifraude du Canada, même si vous n'avez rien perdu.

Qui contacter au Canada

SIGNALEZ-LE

Centre antifraude du Canada

1-888-495-8501

Signalement national de la fraude. Lun. au ven., 10 h à 16 h 45 (HE). En ligne en tout temps : antifraudcentre.ca.

SIGNALEZ-LE

Texto frauduleux

Transférez au 7726

7726 = « SPAM » sur le clavier. Gratuit chez tous les fournisseurs canadiens, qui bloquent l'expéditeur. Puis supprimez-le.

APPELEZ

Votre police locale

Ligne non urgente

Perte d'argent, menaces ou chantage en ligne : faites une déclaration. Urgence : 911.

PROTÉGEZ VOTRE IDENTITÉ

Equifax et TransUnion

Agences d'évaluation du crédit

Vous avez donné votre NAS, permis ou passeport? Faites inscrire une alerte à la fraude auprès des deux agences.

Six règles pour vous protéger en ligne

- **Un texto inattendu avec un lien est une fraude jusqu'à preuve du contraire.** Postes Canada, l'ARC, les péages, votre banque — allez vous-même dans leur application ou sur leur site, jamais par le lien.
- **Ne partagez jamais un code.** Un code à usage unique est la clé de votre compte. Personne de légitime ne vous demandera de le lire.
- **Les rendements garantis sont un mensonge.** La cryptomonnaie appuyée par des vedettes, les « robots de trading IA » et les tuyaux d'amis d'amis font perdre le plus d'argent au Canada.
- **Activez les mises à jour automatiques** sur votre téléphone, votre ordinateur et votre navigateur. La plupart des piratages exploitent des failles déjà corrigées.
- **Utilisez la vérification en deux étapes et un gestionnaire de mots de passe** (ou des clés d'accès) pour vos courriels et vos services bancaires — votre courriel sert à réinitialiser tous vos autres comptes.
- **Cartes-cadeaux, cryptomonnaie et virements télégraphiques sont des paiements de fraudeurs.** Aucune vraie entreprise, aucun gouvernement ni employeur ne les exigera.

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).

Les fraudes qui coûtent de l'argent aux Canadiens

Texto de livraison, de péage ou d'impôt « impayé »

Un texto annonce qu'un colis est retenu, qu'un péage autoroutier est en souffrance ou qu'un remboursement de l'ARC vous attend. Le lien mène à une copie parfaite du vrai site, qui vous demande votre carte.

> **Signe révélateur :** Un petit montant, un délai serré et un lien. Les vrais organismes ne perçoivent pas de paiements par texto.

Fraudes de placement et de cryptomonnaie

Une publicité montre un Canadien célèbre — souvent une vidéo hypertruquée — qui vante une plateforme. Un « conseiller » sympathique vous montre vos profits qui grimpent sur un tableau de bord, puis vous demande d'investir davantage.

> **Signe révélateur :** Impossible de retirer votre argent sans payer d'abord des « frais » ou une « taxe ». Vérifiez toute entreprise sur autorites-valeurs-mobilieres.ca (« Sont-ils inscrits? »).

Emploi en ligne « à tâches »

Un recruteur vous écrit sur WhatsApp ou Telegram : gagnez de l'argent en évaluant des produits ou en aimant des vidéos. De petits paiements arrivent au début — puis vous devez déposer de l'argent pour débloquer de plus grosses tâches.

> **Signe révélateur :** Un emploi qui exige que vous payiez, généralement en cryptomonnaie. Un vrai emploi vous paie.

Fraudes sur Marketplace et de location

Une aubaine sur Facebook Marketplace ou Kijiji — une voiture, des billets de spectacle, un appartement — mais le vendeur est « à l'extérieur » et exige d'abord un dépôt par virement Interac.

> **Signe révélateur :** Vous ne pouvez pas voir l'article ou le logement en personne avant de payer. Ne versez jamais de dépôt sans avoir vu.

Prise de contrôle de compte et faux soutien

Un texto ou un appel d'« alerte de sécurité » de votre banque, d'Amazon ou de votre fournisseur de téléphonie affirme que votre compte est compromis et vous demande de confirmer un code ou de déplacer de l'argent.

> **Signe révélateur :** On vous demande un code que vous venez de recevoir. Ce code, c'est eux qui se connectent à votre place.

Sextorsion et chantage

Une personne rencontrée en ligne — ou un inconnu qui prétend avoir piraté votre caméra — menace de diffuser des images intimes si vous ne payez pas. Les adolescents sont particulièrement ciblés.

> **Signe révélateur :** Une pression immédiate pour payer. Ne payez pas, cessez de répondre, conservez les messages et signalez-le à la police — pour les jeunes, aussi à cyberaide.ca.

Mettez-les à jour maintenant — des pirates les exploitent ce mois-ci

Failles de produits grand public activement exploitées par des pirates, ajoutées au cours des 30 derniers jours à la liste des vulnérabilités exploitées connues (KEV) de la CISA des États-Unis (cisa.gov/kev). Données au 24 novembre 2026.

Si vous utilisez	Comment faire la mise à jour	Signalé le
Microsoft Office CVE-2026-124194	Ouvrez une application Office → Fichier → Compte → Options de mise à jour → Mettre à jour.	2026-11-10
Google Chrome CVE-2026-125350	Menu (⋮) → Aide → À propos de Google Chrome, puis cliquez sur Relancer.	2026-11-10
iPhone, iPad et Mac CVE-2024-27834	Réglages → Général → Mise à jour logicielle (Mac : Réglages Système → Général → Mise à jour de logiciels).	2026-11-04

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. Section en direct générée automatiquement le 24 novembre 2026 à partir de sources publiques; elle ne présente que les failles de produits grand public courants.