



CANADIAN ANTI-FRAUD CENTRE CENTRE ANTIFRAUDE DU CANADA

Fraude liée aux portefeuilles
de cryptomonnaies

05-08-2026

FRAUD: RECOGNIZE, REJECT, REPORT IT LA FRAUDE: IDENTIFIEZ-LA, SIGNALEZ-LA, ENRAYEZ-LA

Le Centre antifraude du Canada (CAFC) souhaite mettre en garde les Canadiens contre les fraudes ciblant les personnes qui possèdent ou utilisent des portefeuilles de cryptomonnaies. Les fraudeurs peuvent tenter d'accéder à un portefeuille, de voler de la cryptomonnaie ou d'inciter les victimes à partager des renseignements personnels.

Les transactions en cryptomonnaie sont difficiles à inverser. Une fois la cryptomonnaie envoyée ou volée, il peut être difficile ou impossible de la récupérer. Les personnes qui ont déjà perdu de la cryptomonnaie peuvent également être ciblées à nouveau par des fraudeurs qui prétendent pouvoir récupérer les fonds.

Fraude par portefeuille de cryptomonnaie et phrases de récupération

Un portefeuille de cryptomonnaie est utilisé pour accéder à la cryptomonnaie et la gérer. Certains portefeuilles sont des applications sur un téléphone ou un ordinateur. D'autres sont des appareils physiques.

De nombreux portefeuilles de cryptomonnaies utilisent une liste de 12 ou 24 mots secrets. C'est ce qu'on appelle une phrase de récupération ou une phrase de récupération. Il fonctionne comme une clé maîtresse et peut être utilisé pour restaurer le portefeuille et contrôler la crypto-monnaie à l'intérieur. Toute personne qui obtient la phrase de récupération peut être en mesure d'accéder au portefeuille et de transférer la crypto-monnaie. Ils n'ont peut-être pas besoin du téléphone, de l'ordinateur ou du portefeuille physique de la victime.

Les fraudeurs peuvent tenter d'obtenir ces renseignements au moyen de faux sites Web, de courriels, de messages textes, d'appels téléphoniques, de lettres, de codes QR ou de logiciels malveillants. Ils peuvent prétendre qu'il y a un problème avec le portefeuille et qu'une action immédiate est nécessaire.

Une phrase de récupération ne doit jamais être partagée. Un service de police, un organisme gouvernemental, une institution financière, un fournisseur de portefeuille ou un service de soutien légitime ne vous demandera pas de l'envoyer par courriel, message texte, médias sociaux, formulaire en ligne ou lettre.

Fraude de récupération

Les personnes ayant perdu des cryptomonnaies peuvent être à nouveau ciblées par le biais d'une fraude à la récupération.

Dans ce type de fraude, un escroc prétend pouvoir retrouver, débloquer ou restituer des cryptomonnaies volées. Il peut se faire passer pour :

- un agent de police ou un fonctionnaire



Royal Canadian
Mounted Police

Gendarmerie royale
du Canada



Compétition Bureau
Canada

Bureau de la concurrence
Canada



Ontario Provincial Police

Canada

- un avocat ou un enquêteur
- un expert en cryptomonnaies
- un employé d'un portefeuille ou d'une plateforme d'échange
- un représentant d'une société de récupération
- une victime prétendant savoir comment récupérer les fonds

Les fraudeurs peuvent contacter les victimes par téléphone, e-mail, SMS, réseaux sociaux ou courrier postal.

Ils peuvent déjà disposer de certaines informations sur la victime, telles que le montant perdu, le type de cryptomonnaie concerné ou l'adresse publique d'un portefeuille. Ils peuvent utiliser ces détails pour paraître légitimes et demander à la victime les informations qui leur manquent.

Ils peuvent demander des informations personnelles, des pièces d'identité, des détails financiers, des informations sur le portefeuille ou un paiement anticipé. Le fait de disposer de certaines informations correctes ne prouve pas que la personne ou l'organisation soit légitime.

Signes avant-coureurs

Méfiez-vous de toute personne qui :

- Vous contacte spontanément au sujet de vos cryptomonnaies ou de votre portefeuille
- Prétend que votre portefeuille a été piraté, bloqué ou mis en danger
- Affirme avoir retrouvé vos cryptomonnaies volées
- Promet ou garantit que les fonds perdus peuvent être récupérés
- Vous demande votre phrase de récupération, votre clé privée, votre mot de passe, votre code NIP ou votre code de sécurité
- Vous demande de confirmer des informations personnelles ou financières
- Vous envoie un lien ou un code QR et vous demande de connecter ou de vérifier votre portefeuille
- Vous demande de transférer des cryptomonnaies vers un portefeuille « sûr », « sécurisé » ou « protégé »
- Vous demande d'installer un logiciel ou de lui fournir un accès à distance à votre appareil
- Exige le paiement préalable de frais de récupération, de frais juridiques, fiscaux, d'assurance ou de traitement
- Vous met la pression pour que vous agissiez rapidement ou que vous gardiez l'affaire secrète
- Vous conseille de ne pas contacter la police, votre établissement financier ou les membres de votre famille

Comment vous protéger

- Ne communiquez jamais votre phrase de récupération ni votre clé privée.
- Conservez votre phrase de récupération dans un endroit privé et sécurisé.
- Ne la stockez pas dans un e-mail, un compte cloud, un document en ligne ou une photo.
- Utilisez des mots de passe forts et uniques.
- Activez l'authentification multifactorielle lorsqu'elle est disponible.
- Maintenez à jour vos portefeuilles matériels, vos applications, vos téléphones et vos ordinateurs.
- Téléchargez les logiciels et les mises à jour uniquement à partir de sources officielles.
- Vérifiez les adresses des sites web avant de saisir des informations.

- Ne cliquez pas sur les liens, n'ouvrez pas les pièces jointes et ne scannez pas les codes QR contenus dans des messages inattendus.
- Ne permettez pas à une personne inconnue d'accéder à distance à votre appareil.
- Ne transférez jamais de cryptomonnaie vers un portefeuille fourni par une personne qui vous contacte.
- Ne payez personne qui vous promet de récupérer des cryptomonnaies perdues.
- Ne communiquez pas d'informations personnelles, financières ou relatives à votre portefeuille par le biais de correspondances inattendues.
- Recherchez vous-même les coordonnées officielles d'une organisation et contactez-la directement.
- Prenez le temps de vérifier toutes les demandes avant d'agir.

Si vous croyez avoir été la cible de fraude ou de cybercriminalité, signalez-le à votre service de police local. Il est aussi possible de faire un signalement en ligne sur le site Web [Signaler la cybercriminalité et la fraude](#) ou par téléphone au 1-888-495-8501.