FRAUDES ET ESCROQUERIES LIÉES AUX CRYPTO-ACTIFS

RESTEZ VIGILANT(E) ET PROTÉGEZ-VOUS

La croissance rapide des crypto-actifs et leurs caractéristiques spécifiques (accessibilité mondiale, rapidité, anonymat et souvent irréversibilité des transactions) font de vous une cible privilégiée pour les cybercriminels. Les fraudeurs et les escrocs utilisent des techniques sophistiquées pour vous leurrer, telles que les « pyramides de Ponzi », les fausses opportunités d'investissement, les offres « gratuites » sur les médias sociaux et les messages trompeurs. Ils recourent également à des escroqueries sentimentales ou des adresses quasi identiques à des adresses légitimes (« look-alike addresses ») pour avoir accès à votre portefeuille. Ils vous contactent souvent via les médias sociaux, des applications de messagerie, des courriels ou des appels téléphoniques inattendus qui semblent légitimes. Vous pouvez faire face à des risques tels que la perte financière, l'usurpation d'identité et une détresse émotionnelle.

Soyez prudent et suivez ces conseils clés pour rester en sécurité :

Restez attentif(ve) aux éventuelles fraudes et escroqueries dans le domaine des crypto-actifs :
Pour en savoir plus sur les différents types de fraudes et d'escroqueries (voir pages 5, 6, 7 et 8);

Repérez les signes d'alerte :
Apprenez à reconnaître les comportements, messages ou offres suspects (voir page 2);

Protégez-vous et protégez vos actifs :
Sécurisez vos informations personnelles (voir page 3);

Sachez quoi faire si vous êtes victime d'une fraude ou d'une escroquerie
(voir page 4).

Signaux d'alerte

Une promesse qui semble trop belle pour être vraie

Une offre non sollicitée

Un rendement rapide et élevé garanti

Urgence à agir (par exemple, des offres limitées dans le temps qui vous poussent à agir immédiatement)

Une demande de paiement via des méthodes impossibles à tracer (par exemple, crypto-actifs, cartes-cadeaux, virements bancaires ou cartes de débit prépayées)

Une invitation à cliquer sur un lien, à scanner un QR code ou à télécharger une application

Une demande d'envoi ou de partage de vos clés privées et de vos phrases de récupération secrètes (liste de mots pour accéder et récupérer votre portefeuille de crypto-actifs)

Une URL suspecte ou incorrecte

Un logo légèrement modifié, un site Internet qui imite celui d'une véritable entreprise ou paraissant professionnel, mais dépourvu de coordonnées de contact vérifiées, d'informations relatives à l'enregistrement de l'entreprise, d'historique ou de présence vérifiable

Une plateforme d'échange inconnue

Une pièce jointe suspecte, en particulier des fichiers Office .exe, .scr, .zip ou avec macros activé (.docm, .xlsm)

Étapes pour vous protéger

1 Prenez le temps de réfléchir avant d'agir :

Ne vous précipitez pas pour investir, partager des informations ou cliquer sur des liens : les escrocs créent délibérément un sentiment d'urgence. En cas de doutes, même minimes, n'agissez pas, n'investissez pas et vérifiez soigneusement la source.

2 Vérifiez attentivement la source :

- Vérifiez toujours l'origine des messages, des appels, des courriels et des liens, même s'ils semblent officiels, semblent provenir d'un ami ou d'un membre de votre famille, ou même d'une personnalité publique. Recherchez les fautes d'orthographe, les URL étranges ou l'absence d'indicateurs de sécurité. Par exemple, vérifiez que le lien du site Internet contient bien un « s » à « HTTPS » pour vous assurer que le site Internet est sécurisé, et vérifiez qu'aucune lettre n'a été ajoutée ou ne manque dans le nom de l'entreprise.
- N'ouvrez pas les liens envoyés dans des messages non sollicités, installez uniquement des applications officielles via des boutiques d'applications fiables et ne scannez pas de QR codes inconnus.
- Même si une offre semble officielle, comparez-la toujours avec les informations publiées sur le site Internet de l'entreprise ou vérifiez que le compte de médias sociaux est certifié (par exemple avec le badge officiel).
- Utilisez des coordonnées vérifiées pour contacter directement l'entreprise ou la personne de contact et ne vous fiez jamais aux coordonnées fournies par le présumé fraudeur (par exemple, recherchez le nom de l'entreprise de manière indépendante, consultez des annuaires professionnels reconnus). Les escrocs peuvent prétendre être autorisés ou imiter le site Internet d'une société autorisée. Vous pouvez vérifier si un fournisseur de crypto-actifs est agréé dans l'UE en consultant le registre de l'ESMA (↖). Vous pouvez également consulter le site Internet de la CSSF pour savoir si des avertissements ou des listes noires ont été émis ou la liste I-SCAN de l'OICV (iosco.org/i-scan/).

3 Ne partagez jamais de mots de passe, vos clés privées ou de phrases de récupération secrète (*seed phrases*) :

Toute personne y ayant accès peut prendre le contrôle de vos actifs. Les entreprises légitimes ne vous demanderont jamais vos mots de passe ou vos codes de sécurité par courriel, SMS ou téléphone.

4 Sécurisez vos appareils et vos clés privées :

Utilisez des mots de passe forts et uniques pour chacun de vos comptes en crypto-actifs, gardez votre mot de passe secret et évitez de réutiliser les mêmes informations d'identification sur différentes plateformes. Activez l'authentification multifacteur dans la mesure du possible. Vous pouvez obtenir quelques conseils sur les mots de passe sous ↖. Gardez votre logiciel et votre protection antivirus à jour et activés.

5 Soyez prudent(e) avec les offres d'investissement inattendues :

Méfiez-vous des investissements qui promettent d'énormes rendements. Si cela semble trop beau pour être vrai, c'est probablement le cas.

6 Réfléchissez avant de partager des informations sur les réseaux sociaux :

Les groupes de discussion, les forums, les publications sur les réseaux sociaux et les photos peuvent fournir des informations précieuses pour les fraudeurs. Divulguer trop de détails sur vous ou sur vos investissements peut faire de vous une cible facile.

Que faire lorsque vous êtes victime d'une fraude ou d'une escroquerie

Arrêtez immédiatement les transactions :

Bloquez toute nouvelle transaction vers des comptes suspects afin d'éviter des pertes supplémentaires. Cessez tout contact avec les escrocs : ignorez leurs appels et leurs courriels et bloquez l'expéditeur.

Modifiez vos mots de passe sur tous vos appareils et applications/sites Internet.

Les fraudeurs achètent des mots de passe divulgués en ligne et les essaient sur plusieurs comptes. Changer un seul mot de passe ne suffit pas : changez-les tous afin que les fraudeurs ne puissent pas les réutiliser.

Déconnectez-vous et révoquez l'accès :

Révoquez les autorisations suspectes dans votre contrat numérique qui s'exécutent automatiquement sur la blockchain (contrat intelligent – *smart contract*) pour empêcher les escrocs de dépenser vos jetons sans votre consentement. De nombreux portefeuilles et explorateurs de blockchain offrent des outils qui vous permettent de voir quels contrats intelligents disposent au moment présent d'un accès pour dépenser vos jetons. Pour ce faire, vous pouvez :

- utiliser un outil fiable de vérification d'autorisation, qui vérifie si un utilisateur ou une adresse blockchain est autorisé à exécuter une opération ;
- revoir la liste des autorisations, et
- utiliser le bouton « Révoquer » directement depuis la plateforme.

Déplacez vos fonds :

Si votre portefeuille est compromis, transférez immédiatement vos actifs restants vers un nouveau portefeuille sécurisé.

Contactez votre fournisseur de crypto-actifs :

Informez votre fournisseur de crypto-actifs dès que possible en utilisant les canaux de contact officiels, afin d'examiner les solutions disponibles. Même si, dans la plupart des cas, une transaction blockchain ne peut être annulée, le fournisseur pourrait tout de même geler le compte de l'escroc (s'il se trouve sur sa plateforme) et mettre l'adresse du portefeuille sur liste noire.

Signalez l'incident et alertez votre entourage :

Signalez l'incident à la police et, si pertinent, à la CSSF (www.cssf.lu) informez votre entourage (par exemple, vos amis et votre famille) afin de sensibiliser le public. Ces actions sont la meilleure façon de vous protéger et de protéger les autres.

Méfiez-vous de la fraude de type « *recovery room* » :

Le fraudeur peut vous contacter en sachant que vous avez déjà été victime d'une escroquerie, prétendant être une autorité publique (par exemple, la police, l'autorité fiscale ou financière, etc.) et vous proposant de récupérer votre argent perdu moyennant des frais. C'est souvent une nouvelle tentative de vous arnaquer. Rappelez-vous : le fait d'avoir été victime d'une arnaque une fois ne vous empêche pas d'être victime d'une nouvelle arnaque.

Voir l'avertissement des autorités européennes communes de surveillance pour en savoir plus sur les risques liés aux crypto-actifs (↖) et la fiche d'information intitulée « Les crypto-actifs expliqués : Ce que MiCA signifie pour vous en tant que consommateur » (↖).

Autorité bancaire européenne, Autorité européenne des assurances et des pensions professionnelles, Autorité européenne des marchés financiers, 2025

Luxembourg: Office des publications de l'Union européenne, 2025

PDF ISBN 978-92-9407-228-3 doi:10.2853/4216609 DZ-01-25-117-FR-N

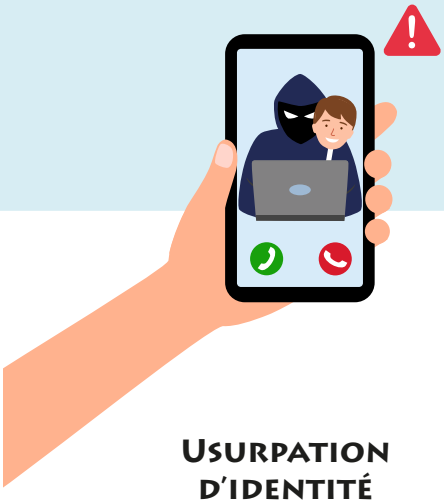
TYPES DE FRAUDES LIÉES AUX CRYPTO-ACTIFS

« *Pump-dump* » et « *Rug pull* » (technique de la bouilloire et escroqueries de sortie)

Vous voyez une publicité (annonce) sur les réseaux sociaux ou un site Internet faisant la promotion d'une « opportunité d'investissement à durée limitée » dans des crypto-actifs, recommandant d'investir dans un nouveau jeton ou un projet de crypto-actifs. Après avoir exprimé votre intérêt, vous êtes contacté(e) et redirigé(e) vers une plateforme d'échange de crypto-actifs ou un canal de messagerie (par exemple Telegram, Viber ou WhatsApp). Un contact apparemment crédible promet des gains rapides ou des rendements élevés si vous investissez rapidement. On vous encourage à investir un petit montant, puis on vous met la pression pour investir davantage.

Que pourrait-il se passer :

Vous découvrez que le jeton dans lequel vous avez investi n'a aucune valeur et que la personne avec laquelle vous avez été en contact cesse de répondre. Lorsque vous essayez de retirer votre argent, le site Internet n'existe plus et l'entreprise est injoignable. Les escrocs ont artificiellement gonflé ou surestimé un crypto-actif à faible valeur pour en augmenter la valeur (pump), puis ont vendu leurs actifs (dump), provoquant un effondrement du cours et des pertes pour les investisseurs. Dans d'autres cas, ils pourraient fermer le projet et disparaître avec les fonds (rug pull).



Usurpation d'identité

Après avoir posté une question sur une plate-forme de réseaux sociaux ou un site Internet au sujet d'un problème de portefeuille de crypto-actifs, vous recevez un message direct inattendu (DM) ou un courriel de quelqu'un se faisant passer pour un interlocuteur de confiance (par exemple, une plateforme d'échange de crypto-actifs, un fournisseur de portefeuille, un support informatique ou même un ami). La personne demande votre phrase de récupération secrète (c'est-à-dire une séquence de mots qui sert de sauvegarde centrale pour accéder à votre portefeuille numérique), vos mots de passe ou vos clés privées (un code cryptographique généré automatiquement qui prouve la propriété des actifs numériques).

Ce qui pourrait arriver :

Une fois que vous partagez votre phrase de récupération secrète, vos mots de passe ou vos clés privées, l'escroc les utilise pour voler vos crypto-actifs ou d'autres fonds. Gardez à l'esprit que la perte de clés privées entraîne la perte définitive et irréversible d'accès à vos crypto-actifs et de la propriété de vos crypto-actifs. Contrairement aux transactions bancaires, un transfert cryptographique est irréversible : une fois que vos fonds ont disparu, il est presque impossible de le récupérer.

Hameçonnage (*phishing*)

Vous recevez un message inattendu par courriel, téléphone, pop-up ou sur les réseaux sociaux, prétendant provenir d'un prestaire de services sur crypto-actifs bien connu. Le message vous invite à vous connecter ou à télécharger une nouvelle application. Vous pouvez également recevoir un courriel qui semble provenir de votre application de portefeuille de crypto-actifs, vous exhortant à résoudre un prétendu problème de sécurité en cliquant sur un lien provenant d'une source non officielle ou en mettant à jour l'application.

Ce qui pourrait arriver :

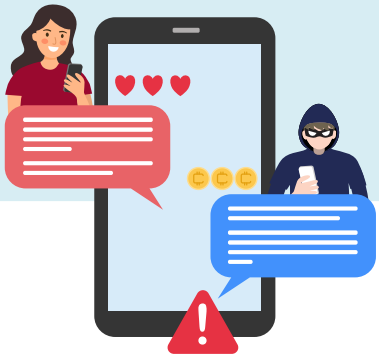
En cliquant sur le lien, en téléchargeant l'application ou en scannant un QR code, vous installez un logiciel malveillant qui permet à l'escroc d'accéder à vos informations et de les utiliser pour voler vos crypto-actifs ou vos fonds.

Arnaque aux faux cadeaux (*giveaway scam*)

Vous tombez sur une annonce sur les réseaux sociaux affirmant qu'une entreprise donne des crypto-actifs après un petit investissement initial en crypto-actifs. Il s'agit notamment d'une vidéo ou d'un message présentant des photos d'une célébrité ou d'une marque – généralement fausses ou obtenues sans autorisation – promettant de « doubler la valeur de vos crypto-actifs » si vous envoyez d'abord de l'argent. Le logo, la mise en page, les témoignages et le style utilisé semblent professionnels et officiels, tout comme le site Internet vers lequel vous êtes redirigé(e).

Ce qui pourrait arriver :

Après avoir envoyé vos crypto-actifs, vous ne recevez rien en retour et perdez l'argent envoyé. Le cadeau était faux, et le message ou le livestream usurpant l'identité de célébrités ou d'entreprises a été conçu pour vous tromper.



Escroquerie sentimentale avec investissement (*romance investment scam*)

Vous avez été contacté(e) sur les réseaux sociaux, des applications de rencontre ou par téléphone/SMS par une personne que vous n'avez jamais rencontrée dans la vie réelle. Cette personne peut engager des conversations fréquentes, personnelles et romantiques, gagnant ainsi progressivement votre confiance en utilisant de faux profils. Peu à peu, elle oriente la conversation vers des opportunités financières, prétendant réaliser d'importants gains grâce à des investissements dans des crypto-actifs et vous encourageant à investir à votre tour avec des promesses de rendements élevés et de faibles risques. Elle vous guide pas à pas dans la création d'un compte et le versement d'un petit dépôt initial pour rendre le stratagème plus crédible.

Les escrocs créent de faux profils en ligne et utilisent des images volées ou générées par l'intelligence artificielle pour vous approcher.

Ce qui pourrait arriver :

L'escroc extrait autant d'argent que possible, puis coupe tout contact et disparaît. Le site Internet ou l'application d'investissement frauduleux est mis hors ligne, vous laissant sans aucun accès aux prétendus investissements. Dans certains cas, les escrocs peuvent utiliser les informations obtenues au cours de l'escroquerie pour cibler vos proches ou voler votre identité, ce qui peut avoir des conséquences financières ou juridiques pour vous (par exemple, le fraudeur peut ouvrir des portefeuilles volés à votre nom et vous pourriez être tenu(e) responsable des dettes ou d'activités illégales sous votre nom jusqu'à preuve du contraire).

Pyramide de Ponzi

Vous êtes invité(e) à participer à un projet qui promet des rendements élevés et réguliers grâce à des investissements en crypto-actifs, souvent appuyés par de faux témoignages ou des histoires de réussites inventées. Le schéma peut être présenté comme une opportunité de marketing à plusieurs niveaux, où vous gagnez des récompenses non seulement de votre propre investissement, mais aussi en recrutant d'autres participants. Les premiers investisseurs semblent recevoir des paiements, encourageant davantage de personnes à adhérer et à promouvoir ce schéma.

En réalité, il n'y a pas de véritable affaire ni de profit générés. L'argent provient uniquement de la contribution des nouveaux investisseurs qui est utilisée pour rémunérer les organisateurs du régime et les premiers participants de ce régime.

Ce qui pourrait arriver :

Une fois que les nouveaux investissements ralentissent, le système s'effondre et vous, comme la plupart des participants, perdez votre argent. Les organisateurs disparaissent, ne laissant aucun moyen de récupérer des fonds. La structure à plusieurs niveaux contribue à la propagation rapide de l'escroquerie, car les victimes deviennent, malgré elles, des promoteurs.

Une adresse ressemblante contaminant votre portefeuille

Après avoir effectué une transaction en crypto-actifs, vous remarquez une nouvelle adresse apparaissant dans l'historique de votre portefeuille. Cette adresse ressemble à une adresse avec laquelle vous avez déjà interagi. Les escrocs peuvent faire apparaître de fausses adresses de portefeuille dans votre historique de transactions en vous envoyant une petite quantité de crypto-actifs à partir d'une adresse similaire à celle de votre portefeuille. Vous finissez par stocker, dans l'activité récente de votre portefeuille ou dans les suggestions automatiques, la fausse adresse créée par l'escroc. Les escrocs créent délibérément ces adresses similaires en changeant seulement quelques caractères, souvent au milieu de l'adresse, pour que cela passe inaperçu.

Ce qui pourrait arriver :

Lorsque vous essayez d'envoyer des crypto-actifs et vous copiez par erreur la mauvaise adresse à partir de l'historique de votre portefeuille, vous envoyez sans le savoir des fonds au portefeuille de l'escroc. Étant donné que les transactions en crypto-actifs sont souvent irréversibles, vos fonds sont perdus dans la plupart des cas de manière définitive. Cette escroquerie repose sur la tromperie visuelle et l'erreur de l'utilisateur, exploitant l'habitude de copier-coller des adresses de portefeuille sans les vérifier attentivement.