# FRAUDES ET ARNAQUES LIÉES AUX CRYPTO-ACTIFS

## RESTEZ VIGILANT ET PROTÉGEZ-VOUS

Le développement 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 tactiques sophistiquées pour vous tromper, telles que les « pyramides de Ponzi », les fausses opportunités d'investissement, les offres gratuites sur les réseaux sociaux et les faux messages de sollicitation. Ils utilisent également la technique de l'arnaque aux sentiments ou des fausses adresses de confiance pour vous convaincre d'investir dans leurs produits frauduleux. Ils vous approchent souvent via les réseaux sociaux, par courriels, appels téléphoniques non sollicités ou messages instantanés qui semblent authentiques. Vous risquez alors des pertes financières, le vol d'identité ou de subir de la détresse émotionnelle.

Soyez prudent et suivez ces conseils essentiels pour ne pas tomber dans un piège :

**Restez vigilant face à d'éventuelles fraudes et arnaques (scams) liées aux crypto-actifs :**
Pour en savoir plus sur les différents types de fraudes et d'arnaques (voir pages 5 à 8).

**Reconnaissez les signaux d'alertes :**
apprenez à reconnaître les comportements, messages ou offres suspects (voir page 2).

**Protégez vos données personnelles et vos actifs :**
sécurisez vos équipements et vos informations personnelles (voir page 3).

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

# Les signaux d'alertes

Une promesse trop belle pour être vraie.

Une offre non sollicitée.

Un rendement rapide et élevé garanti.

L'urgence à agir vite (par exemple, offres à durée limitée qui vous pousse à agir immédiatement).

Une demande de paiement via des moyens de paiement irréversibles (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 clés privées ou de *seed phrases* (phrase mnémonique permettant l'accès à ou la recupération de votre portefeuille crypto).


Une plateforme d'échange inconnue.

Un site internet qui mime l'apparence de celui d'une véritable entreprise ou bien qui semble professionnel, mais qui ne contient ni de coordonnées vérifiées, ni d'informations relatives à l'enregistrement de l'entreprise, d'historique ou d'existence vérifiable.

Une adresse (URL) suspecte ou incorrecte, un logo distordu.

Une pièce jointe provenant d'une source inconnue, ou bien dont les fichiers comportent une extension .exe, .scr, .zip ou bien encore un fichier Office ou bureautique pouvant contenir des macros (p. ex. .docm, .xlsm).

# Les précautions pour vous protéger :

**1** **Réfléchissez 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 mineurs, n'investissez pas et vérifiez soigneusement la source avant toute action.

**2** **Vérifiez attentivement la source et l'identité des contacts :**

- Vérifiez toujours la provenance des messages, appels, courriels et liens, même s'ils semblent authentiques, ou paraissent provenir d'un ami, d'un membre de votre famille, ou d'une personnalité publique. Soyez attentifs aux fautes d'orthographe, aux adresses étranges ou aux indicateurs de sécurité manquants (par exemple, vérifiez que le lien vers le site web inclut un « s » dans « http**s** » pour s'assurer que le site web est sécurisé). Vérifiez qu'aucune lettre n'a été ajoutée ou est manquante dans le nom de l'entreprise figurant dans l'adresse ;
- N'ouvrez pas de liens contenus dans des messages non sollicités, n'installez que des applications officielles via des magasins d'applications de confiance et ne scannez pas de QR codes inconnus ;
- Même si une offre semble authentique, vérifiez-la toujours par recoupement avec le site internet de l'entreprise ou assurez-vous que le compte de réseau social utilisé est vérifié (par exemple avec un pictogramme de certification) ;
- Utilisez des coordonnées vérifiées pour contacter directement l'entreprise ou l'individu et ne vous fiez jamais aux coordonnées fournies par le fraudeur présumé (par exemple, recherchez le nom de l'entreprise de manière indépendante, utilisez des annuaires commerciaux vérifiés). Les escrocs peuvent prétendre être autorisés ou bien imiter le site web d'une société autorisée. Vous pouvez vérifier si le fournisseur de crypto-actifs est autorisé dans l'UE en consultant le registre européen de l'AEMF (ESMA) (). Vous pouvez également consulter le site internet des autorités compétentes nationales () pour vérifier si une alerte ou une inscription en liste noire ont été publiées, ou bien encore la liste internationale I-SCAN de l'OICV (IOSCO) (iosco.org/i-scan/).

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

Toute personne y ayant accès peut prendre le contrôle de vos actifs. Une entreprise légitime ne vous demandera jamais vos mots de passe ou codes de sécurité.

**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 au secret vos mots de passe et évitez de réutiliser les mêmes informations d'identification sur différentes plateformes; activez l'authentification forte dans la mesure du possible (recommandations de référence en la matière : ). Gardez votre protection logicielle et antivirus à jour et activée.

**5** **Soyez prudent envers les offres d'investissement non sollicitées :**

Méfiez-vous des investissements qui promettent des rendements très élevés. Si cela semble trop beau pour être vrai, c'est probablement une arnaque.

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

Les informations et les photos que vous postez sur les groupes de discussion, les forums et sur les réseaux sociaux en général peuvent être précieuses pour les escrocs. Dévoiler trop d'informations sur vous-même ou sur vos investissements peut faire de vous une cible plus vulnérable.

# Que faire si vous êtes victime d'une fraude ou d'une arnaque

## Arrêtez immédiatement toute transaction avec le fraudeur :

Bloquez tout virement vers les comptes du fraudeur pour éviter des pertes supplémentaires. Arrêtez tout contact avec les escrocs – ignorez leurs appels et leurs courriels et, si possible, bloquez leurs contacts téléphoniques ou expéditeurs de messagerie.

## Modifiez vos mots de passe sur tous vos appareils, applications et sites internet:

Les fraudeurs achètent des mots de passe compromis et tentent de les utiliser sur tous les comptes où vous auriez pu vous identifier avec votre adresse courriel. Changer un seul mot de passe ne suffit pas ; assurez-vous de tous les changer, afin que les fraudeurs ne puissent pas les réutiliser.

## Déconnectez-vous et révoquez vos accès accordés aux *smart contracts* :

Révoquez les autorisations suspectes accordées aux programmes qui s'exécutent automatiquement sur la blockchain (*smart contracts*) pour empêcher les escrocs de dépenser vos jetons sans votre consentement. De nombreux portefeuilles (*wallets*) et explorateurs de blockchain offrent des outils qui vous permettent de voir quels *smart contracts* ont actuellement un accès vous permettant de dépenser vos jetons. Pour ce faire, vous pouvez :

- utiliser un « vérificateur d'autorisation » de confiance, 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 si une autorisation vous semble suspecte.

## Déplacez vos fonds :

Si votre portefeuille est compromis, transférez immédiatement vos actifs restants dans 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'explorer les différentes options. Même si, dans la plupart des cas, il ne sera pas possible d'annuler la transaction sur la blockchain, le fournisseur pourrait tout de même geler le compte de l'escroc (s'il se trouve sur sa plateforme) et mettre sur liste noire l'adresse de son portefeuille.

## Signalez et alertez :

Signalez l'incident à la police ou à votre autorité nationale de surveillance financière (↖) et informez votre réseau (par exemple, vos amis et votre famille) afin de le sensibiliser. Ces actions sont la meilleure façon de vous protéger et de protéger les autres.

## Méfiez-vous de la fraude au recouvrement de fonds :

Un escroc peut vous approcher en tant que victime d'une précédente escroquerie, prétendant représenter une autorité publique (par exemple, la police, une autorité fiscale ou financière, etc.) et vous propose de récupérer votre argent perdu, moyennant des frais. C'est une tentative pour vous escroquer une nouvelle fois. Rappelez-vous : être arnaqué une fois ne vous empêche pas d'être arnaqué à nouveau !

Prenez connaissance de l'avertissement conjoint des autorités européennes de supervision financière pour en savoir plus sur les risques liés aux crypto-actifs « Avertissement sur les crypto-actifs » (↖) et la fiche d'information intitulée « Crypto-actifs: ce que MiCA signifie pour vous en tant qu'investisseur » (↖)

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

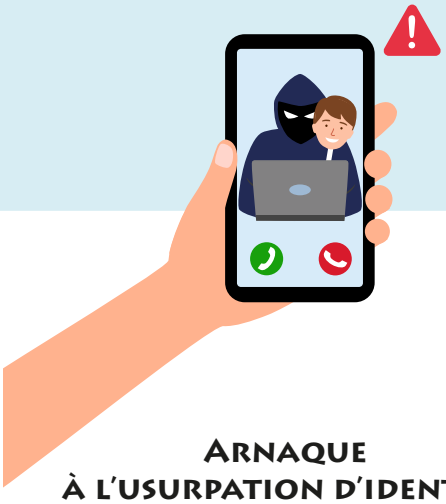
# TYPES D'ARNAQUES LIÉES AUX CRYPTO-ACTIFS

## Techniques « *pump and dump* » ou « *rug pull* »

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 les crypto-actifs, recommandant d'investir dans un nouveau jeton ou projet en crypto-actifs. Après avoir exprimé votre intérêt, vous êtes contacté et redirigé vers une plateforme de crypto-actifs ou un canal de messagerie (par exemple Telegram, Viber ou WhatsApp). Un contact apparemment crédible vous promet des profits rapides ou des rendements élevés si vous investissez rapidement. On vous encourage à investir un petit montant, puis on vous presse pour investir davantage.

***Ce qui pourrait arriver :***

*Vous découvrez que le jeton dans lequel vous avez investi n'a aucune valeur et que la personne avec laquelle vous avez échangé 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 accru le cours d'un crypto-actif de faible valeur pour en augmenter sa valorisation (« pump »), puis ont vendu les actifs en la matière (« dump »), provoquant un krach de la valeur et des pertes pour les investisseurs. Alternativement, ils pourraient cesser le projet et disparaître avec les fonds (« rug pull »).*



## Arnaque à l'usurpation d'identité

Après avoir posté une question sur un réseau social ou un site internet au sujet d'un problème sur un portefeuille de crypto-actifs, vous recevez un message instantané (DM) inattendu ou un courriel d'une personne se faisant passer pour un contact 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 *seed phrase* (c'est-à-dire la séquence de mots permettant la récupération et l'accès à votre portefeuille numérique), vos mots de passe ou vos clés privées (un code cryptographique généré automatiquement qui prouve la propriété et permet de contrôler vos actifs numériques).

***Ce qui pourrait arriver :***

*Une fois que vous partagez votre seed phrase, vos mots de passe ou vos clés privées, l'escroc les utilise pour voler vos crypto-actifs ou d'autres fonds rendus accessibles. Gardez à l'esprit que la perte de clés privées entraîne une perte permanente et irréversible de l'accès et de la propriété de vos crypto-actifs. Contrairement aux transactions bancaires, une fois qu'un transfert de crypto-actifs a été effectué, leur récupération est en général impossible.*

## Phishing

Vous recevez un message inopiné par courriel, téléphone, pop-up ou via les réseaux sociaux, prétendant provenir d'un fournisseur de crypto-actifs reconnu. Le message vous invite à vous connecter sur un site web ou à télécharger une nouvelle application. Vous pouvez également recevoir un courriel qui semble provenir de votre application de portefeuille crypto, vous exhortant à résoudre un soi-disant problème de sécurité (en cliquant sur un lien émanant d'une source non officielle, ou bien en mettant à jour l'application).

***Ce qui pourrait arriver :***

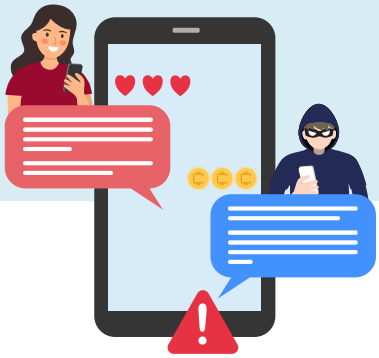
*En cliquant sur le lien, en téléchargeant l'application ou en scannant un QR code, vous installez un logiciel malveillant qui permet à l'escroc d'accéder et d'utiliser les informations pour voler vos crypto-actifs ou vos fonds.*

## Arnaque au cadeau

Vous tombez sur une annonce sur les réseaux sociaux affirmant que des entreprises offrent des crypto-actifs après un petit investissement en crypto-actifs. Il peut s'agir 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 vos crypto-actifs » si vous envoyez de l'argent préalablement. Le logo, la mise en page, les témoignages et le langage utilisés paraissent professionnels et officiels, tout comme le site internet vers lequel vous êtes redirigé.

***Ce qui pourrait arriver :***

*Après avoir transmis vos crypto-actifs, vous ne recevez rien en retour et vous avez perdu les actifs envoyés. La promesse de cadeau était fausse, et le message ou la vidéo usurpant l'identité de célébrités ou d'entreprises avait été conçu pour vous tromper.*



## Arnaque aux sentiments

Vous avez été contacté sur les réseaux sociaux, via une application de rencontres ou par téléphone / message par quelqu'un que vous n'avez jamais rencontré dans la vie réelle. Cette personne s'engage dans des conversations fréquentes, personnelles et romantiques avec vous, partage des histoires et peut même feindre un intérêt sentimental pour gagner votre confiance. Peu à peu, elle oriente la conversation vers des opportunités financières, vantant les énormes bénéfices liés à des investissements dans des crypto-actifs et vous encouragent à investir dans des offres promettant des rendements élevés avec un faible risque. Elle vous guide à travers la création d'un compte et vous montre comment effectuer un petit dépôt initial pour que le système semble réel.

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 retire autant d'argent que possible depuis votre compte, puis coupe toute communication et disparaît. Le site internet ou l'application d'investissement frauduleux est mis hors ligne, vous laissant sans accès aux investissements supposés. Dans certains cas, les escrocs peuvent utiliser les informations obtenues au cours de l'arnaque pour cibler vos amis et votre famille ou pour une future usurpation d'identité qui pourra avoir de lourdes conséquences financières ou juridiques pour vous (par exemple, l'escroc peut vérifier les portefeuilles volés à votre nom et vous pourriez être tenu responsable des dettes ou des délits commis sous votre nom jusqu'à preuve du contraire).*

## Pyramide de Ponzi

Vous êtes invité à participer à un projet qui promet des rendements élevés constants à travers des investissements en crypto-actifs, souvent promus par de faux témoignages. Le projet peut être présenté comme une opportunité à plusieurs niveaux, où vous recevez des revenus non seulement issus de votre propre investissement, mais aussi en recrutant d'autres investisseurs. Les premiers investisseurs reçoivent effectivement une rémunération, encourageant davantage de personnes à adhérer et à promouvoir le projet.

En réalité, il n'y a pas de véritable entreprise ou de profit généré. Les revenus proviennent en fait uniquement de la contribution des nouveaux investisseurs qui sont utilisés pour rémunérer les organisateurs du projet et les premiers participants.

***Ce qui pourrait arriver :***

*Une fois que le flux des investisseurs ralentit, la pyramide s'effondre et vous, comme la plupart des participants, perdez votre argent. Les organisateurs disparaissent, ne laissant aucun moyen de récupérer les fonds détournés. La structure à plusieurs niveaux favorise la propagation rapide de l'arnaque, car les victimes deviennent inconsciemment des promoteurs.*


## Une adresse ressemblante empoisonnant votre portefeuille (address poisoning)

Après avoir effectué une transaction en crypto-actifs, vous remarquez qu'une nouvelle adresse émerge dans l'historique de votre portefeuille. Cette adresse ressemble à l'une de celles avec laquelle vous aviez déjà interagi. Les escrocs peuvent piéger votre historique de transactions avec de fausses adresses de portefeuille en vous envoyant une petite quantité de crypto-actifs depuis une adresse semblable à une adresse figurant dans votre historique. Les escrocs créent délibérément ces adresses similaires en changeant seulement quelques caractères, souvent au milieu de l'adresse, pour mieux masquer la supercherie. Vous finissez par sélectionner dans l'activité récente de votre portefeuille ou par l'auto-complétion la fausse adresse créée par l'escroc au lieu de celle que vous vouliez utiliser.

***Ce qui pourrait arriver :***

*Lorsque vous transmettez des crypto-actifs en copiant la mauvaise adresse à partir de l'historique de votre portefeuille, vous les envoyez sans le savoir vers le portefeuille de l'escroc. Étant donné que les transactions en crypto-actifs sont en général irréversibles, vos actifs sont, dans la plupart des cas, perdus définitivement. Cette arnaque repose sur l'illusion visuelle et l'inattention de l'utilisateur, en exploitant l'habitude de copier et coller des adresses de portefeuille sans vérification minutieuse de ces adresses.*