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. Ils utilisent également la technique de l'arnaque aux sentiments ou des adresses similaires pour empoisonner votre portefeuille. Ils vous contactent souvent via les réseaux sociaux, par e-mails, par appels téléphoniques non sollicités et par applications de messagerie qui semblent authentiques. Vous risquez alors des pertes financières, le vol d'identité ou la détresse émotionnelle.

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

Restez vigilant face à d'éventuelles fraudes et arnaques 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 qui semble trop belle pour être vraie.

Une offre non sollicitée.

Un rendement rapide et élevé garanti.

Une pression pour agir vite (par exemple, offres à durée limitée qui vous poussent à agir immédiatement).

Une demande de paiement via des méthodes non traçables (par exemple, cryptos, 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 et de *seed phrase* (liste de mots pour accéder et récupérer votre portefeuille crypto).

Plateforme d'échange inconnue.

Un site internet qui a l'air professionnel, mais qui ne contient pas de coordonnées vérifiées, d'informations relatives à l'enregistrement de l'entreprise, d'antécédents ou de présence vérifiable.

URL suspecte ou incorrecte, logo présentant de légères distorsions, ou site internet qui copie l'apparence du site d'une véritable entreprise mais sans détails d'enregistrement vérifiable.

Une pièce jointe suspecte, en particulier un fichier .exe, .scr, .zip ou macro activé Office (.docm, .xlsm).

Les étapes pour vous protéger :

1 Faites une pause et 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'agissez pas ou n'investissez pas et vérifiez soigneusement la source.

2 Vérifiez attentivement la source :

- Vérifiez toujours d'où viennent les messages, les appels, les emails et les liens, même s'ils semblent officiels, provenir d'un ami ou de votre famille, ou même d'une personnalité publique. Rechercher des erreurs d'orthographe, des URL étranges ou des indicateurs de sécurité manquants, par exemple vérifier que le lien du site web inclut un « s » dans « HTTPS » pour s'assurer que le site web est sécurisé, et vérifier toute lettre ajoutée ou manquante dans le nom de l'entreprise.
- N'ouvrez pas de liens à partir de messages non sollicités, n'installez que des applications officielles via des boutiques d'applications de confiance et ne scannez pas de QR codes inconnus.
- Même si une offre semble officielle, vérifiez-la toujours par recoupement avec le site internet de l'entreprise ou assurez-vous que le compte de réseaux sociaux est vérifié (par exemple avec des coches officielles).
- 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 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 de l'ESMA (). Vous pouvez également consulter le site internet de votre autorité financière nationale pour savoir si des alertes ou des listes noires ont été publiées ou la liste I-SCAN de l'OICV (iosco.org/i-scan/).

3 Ne partagez jamais de mots de passe, de clés privées ou de *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 codes de sécurité par e-mail, message ou téléphone.

4 Sécuriser les appareils et les 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 multi-facteurs dans la mesure du possible. Voici quelques conseils sur les mots de passe ici (). Gardez votre protection logicielle et antivirus à jour et activée.

5 Soyez prudent avec 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 groupes de discussion, les forums, les publications sur les réseaux sociaux et les photos peuvent être de précieuses sources de connaissances pour les escrocs. Révéler trop de choses sur vous-même ou sur vos investissements peut faire de vous une cible facile.

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

Arrêtez immédiatement les transactions:

Pour bloquer tout autre virement vers des comptes suspects et éviter des pertes supplémentaires. Arrêtez tout contact avec les escrocs – ignorez leurs appels et leurs emails 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 ; assurez-vous de tous les changer, afin que les fraudeurs ne puissent pas les réutiliser.

Déconnecter et révoquer l'accès:

Révoquez les autorisations suspectes dans votre contrat numérique qui s'exécutent automatiquement sur la blockchain (*smart contract*) pour empêcher les escrocs de dépenser vos jetons sans votre consentement. De nombreux *wallets* et explorateurs de blockchain offrent des outils qui vous permettent de voir quels *smart contracts* ont actuellement accès pour 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 approbations, et
- utiliser le bouton «révoquer» directement depuis la plateforme.

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'inverser la transaction 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 du portefeuille.

Signalez et alertez:

Signalez l'incident à la police ou à votre autorité nationale de surveillance financière (https://www.fsma.be/fr/questions-sur-la-fraude-linvestissement) et informez votre réseau (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 au recouvrement de fonds:

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

Prenez connaissance de l'alerte des autorités européennes de supervision communes pour en savoir plus sur les risques liés aux crypto-actifs «Avertissement Sur Les 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

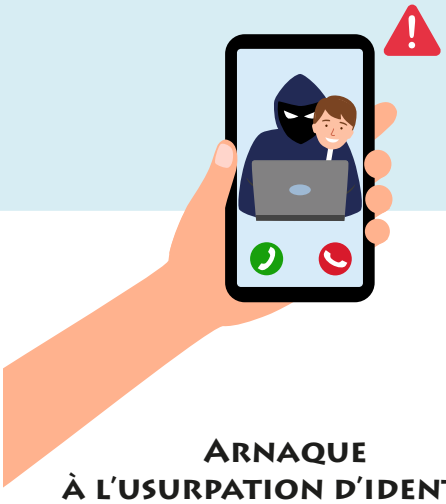
TYPES D'ARNAQUES LIÉES AUX CRYPTO-ACTIFS

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 promet des profits rapides ou des rendements élevés si vous investissez rapidement. On vous encourage à investir un petit montant, puis on vous presse d'investir davantage.

Ce qui pourrait arriver:

Vous découvrez que le jeton 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 une crypto de faible valeur pour en augmenter la valeur (« pump »), puis ont vendu leurs actifs (« dump »), provoquant un krach de la valeur et laissant les investisseurs avec des pertes. 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 une plateforme 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 email d'une personne prétendant être un contact de confiance (par exemple, une plateforme d'échange de crypto, un fournisseur de portefeuille, un support informatique ou même un ami). La personne demande votre *seed phrase* (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 seed phrase, 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 une perte permanente et irréversible de l'accès et de la propriété de vos crypto-actifs. Contrairement aux transactions bancaires, en cas de transferts de crypto-actifs, une fois que vos fonds ont disparu, la récupération est presque impossible.

Phishing

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

Ce qui pourrait arriver:

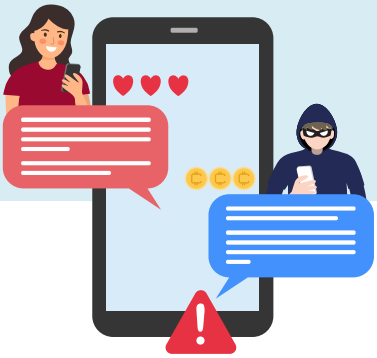
En cliquant sur le lien, en téléchargeant l'application ou en scannant un QR code, vous installez un logiciel malveillant qui permet à l'escroc d'accéder et d'utiliser les informations pour voler vos crypto-actifs ou vos fonds.

Arnaque au cadeau

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

Ce qui pourrait arriver:

Après avoir envoyé vos crypto-actifs, vous ne recevez rien en retour et vous avez perdu 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.



Arnaque aux sentiments

Vous avez été contacté sur les réseaux sociaux, les applications de rencontres ou par téléphone / message par quelqu'un que vous n'avez pas rencontré dans la vie réelle. Cette personne peut s'engager dans des conversations fréquentes, personnelles et romantiques, en construisant la confiance en utilisant de faux profils. Peu à peu, ils orientent la conversation vers des opportunités financières, prétendant d'énormes bénéfices liés à des investissements en crypto-actifs et vous encourageant à investir dans des offres promettant des rendements élevés et de faible risque. Ils vous guident à travers la création d'un compte et le versement d'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 et commettre une usurpation d'identité qui peut avoir des conséquences financières ou juridiques pour vous (par exemple, le fraudeur peut vérifier les portefeuilles volés à votre nom et vous pourriez être tenu responsable des dettes ou des crimes 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 d'investissements en crypto-actifs, souvent soutenus par de faux témoignages et « success » stories. Le projet peut être présenté comme une opportunité de marketing multi-niveaux, où vous gagnez des récompenses non seulement grâce à votre propre investissement, mais aussi en recrutant d'autres personnes. Les premiers investisseurs semblent recevoir des paiements, 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. Au lieu de cela, l'argent provient uniquement de la contribution des nouveaux investisseurs qui est utilisée pour payer les rendements aux organisateurs du projet et aux premiers participants.

Ce qui pourrait arriver:

Une fois que les nouveaux investissements ralentissent, le projet 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 multi -niveaux favorise la propagation rapide de l'arnaque, car les victimes deviennent inconsciemment des promoteurs.

Une adresse ressemblante qui empoisonne 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 celle avec laquelle vous avez déjà interagi. Les escrocs peuvent faire apparaître de fausses adresses de portefeuille dans votre historique de transactions en envoyant une petite quantité de crypto à partir d'une adresse similaire à votre portefeuille. Vous finissez par stocker dans l'activité récente de votre portefeuille ou auto-suggestions la fausse adresse créée par l'escroc. Les escrocs créent délibérément des adresses similaires en changeant seulement quelques caractères, souvent au milieu de l'adresse, pour éviter la détection.

Ce qui pourrait arriver:

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