

Comment ne pas perdre vos cryptos

Une liste de contrôle : ce qu'il ne faut jamais faire, comment vous protéger et que faire si c'est déjà arrivé.

À ne jamais faire

- 1 **Ne donnez jamais à personne votre phrase de récupération (12-24 mots) ni votre clé privée.** Aucune plateforme d'échange, aucun support, aucun policier ne la demandera. Qui vous la demande veut vous voler.
- 2 **N'investissez jamais via quelqu'un rencontré en ligne :** sur une appli de rencontre, Telegram, WhatsApp ou Facebook. C'est ainsi que commencent la plupart des arnaques, même après des mois d'échanges.
- 3 **Ne croyez jamais aux gains garantis.** « 2 % par jour », « sans risque », « aujourd'hui seulement » signifient toujours une arnaque.
- 4 **Ne payez jamais pour retirer votre propre argent.** Si des « frais », une « taxe » ou une « assurance » sont exigés avant un versement, l'argent est déjà perdu.
- 5 **N'installez jamais d'application d'accès à distance** (AnyDesk, TeamViewer, etc.) parce qu'on vous le demande.
- 6 **Ne répondez jamais à un « support » qui vous a écrit en premier.** Les vrais administrateurs et employés de plateformes n'écrivent pas en premier.
- 7 **Un appel de votre « banque », de votre « plateforme » ou de « la police » ?** Raccrochez et appelez vous-même le numéro officiel.
- 8 **N'approuvez jamais dans votre portefeuille ce que vous ne comprenez pas.** Un seul « Approuver » (Approve) ou « Signer » (Sign) sur un faux site peut vider tout le portefeuille.
- 9 **Vérifiez l'adresse du destinataire en entier, pas seulement le début et la fin.** Ne copiez pas d'adresses depuis l'historique des transactions : les escrocs y glissent des adresses presque identiques.
- 10 **Ne faites jamais confiance aux services de « récupération »** qui garantissent de récupérer votre argent ou veulent des cryptos d'avance. C'est la deuxième arnaque après la première.

Comment vous protéger

- Tapez vous-même l'adresse de la plateforme d'échange ou ouvrez-la depuis un favori. De faux sites apparaissent dans les résultats Google et les annonces.
- Utilisez une plateforme d'échange agréée dans votre pays ou votre région. Activez la validation en deux étapes avec une application d'authentification, pas par SMS.
- Activez sur votre plateforme la liste blanche d'adresses de retrait : l'argent ne pourra partir que vers des adresses que vous avez approuvées.
- Gardez les montants importants sur un portefeuille matériel acheté uniquement auprès du fabricant.
- De temps en temps, vérifiez à quels sites votre portefeuille a donné des autorisations et révoquez celles qui ne servent plus (par exemple avec revoke.cash).

Si c'est déjà arrivé

- 1 **Ne payez plus rien** et cessez tout contact avec les escrocs.
- 2 **Conservez les preuves :** identifiants de transaction (TxID), adresses, montants, heures, et captures d'écran des conversations et du site.
- 3 **Signalez-le immédiatement** à votre plateforme d'échange et à la police. Les premières heures comptent le plus : tant que l'argent est encore sur une plateforme d'échange, il peut être gelé.
- 4 **S'il faut retracer où est passé l'argent** et préparer des preuves pour la police et la plateforme d'échange : trailforensics.com.