5 arnaques à éviter absolument

Publié le 02 Jan 2026 par Coinbrief

Dans la crypto, une arnaque réussie se joue rarement sur la technologie seule : elle exploite surtout la précipitation, la confiance et la méconnaissance des signatures et autorisations on-chain. Plusieurs organismes et médias spécialisés alertent régulièrement sur la recrudescence d'escroqueries visant les particuliers, notamment via de faux sites, de faux conseillers et des promesses de gains rapides.

Pourquoi ces arnaques marchent

Les transactions blockchain sont généralement irréversibles, ce qui rend les "erreurs" ou validations sous pression particulièrement coûteuses. Beaucoup d'attaques consistent à vous faire signer quelque chose qui paraît anodin (connexion, approbation, "claim"), mais qui donne en réalité des droits de dépense à un contrat ou à un tiers malveillant.

Les 5 arnaques à éviter absolument

1) Phishing (faux sites / faux supports / liens sponsorisés)
Les escrocs copient l'interface d'un exchange ou d'un wallet (site miroir) et poussent la victime à s'authentifier ou à connecter son portefeuille sur le mauvais domaine. Une fois la confiance installée, ils cherchent à récupérer la seed phrase, des codes 2FA, ou à faire signer une transaction qui vide le portefeuille. Réflexes rapides : taper l'URL manuellement, vérifier le domaine, éviter les liens sponsorisés, et ne jamais communiquer sa seed phrase.

2) Rug pull (projet qui disparaît avec la liquidité)
Le schéma classique : un token est lancé, la hype monte, puis la liquidité est retirée ou le projet est abandonné, rendant la revente impossible ou quasi nulle. Cela touche surtout les micro-cap tokens, memecoins et certains projets DeFi à marketing agressif. Signaux

d'alerte : équipe anonyme + promesses de rendements irréalistes + liquidité non verrouillée + tokenomics opaques.

3) Faux airdrops / giveaways (le "cadeau" qui coûte votre wallet)
Une fausse campagne "claim airdrop" ou "giveaway" vous attire via X/Twitter, Telegram, Discord ou des commentaires sous des posts populaires. Le site vous demande de connecter le wallet puis de signer (ou d'approuver) une opération qui autorise le contrat à transférer vos jetons, ou vous réclame des "frais" pour débloquer le gain. Règle simple : un airdrop légitime ne demande pas de seed phrase et n'exige pas de payer pour "débloquer" une récompense.

4) Fausses applications / fausses extensions de wallet (malware)
Des applications ou extensions se font passer pour des outils connus et servent de cheval de Troie (vol de clés, substitution d'adresse au copier-coller, demandes de signatures piégées). Ces clones circulent via de la pub, du SEO, ou des messages "support" qui vous envoient un faux lien de téléchargement. Mesures efficaces : installer uniquement depuis les sources officielles, vérifier l'éditeur, et éviter d'installer "dans l'urgence" après un message alarmiste.

5) "Pig butchering" (arnaque à la relation + fausse plateforme d'investissement)
L'arnaque démarre souvent par une discussion (réseau social, messagerie, rencontre) puis dérive vers une "opportunité" de trading/DeFi sur une plateforme inconnue mais très convaincante. Les gains affichés sont truqués pour pousser à déposer davantage, puis les retraits sont bloqués avec des prétextes (taxes, vérifications, frais) avant disparition du site ou du "conseiller". Point clé : refuser toute "opportunité" d'investissement proposée en privé et toute plateforme non vérifiable par des sources indépendantes.

Réflexes essentiels (anti-arnaques)

- Ne jamais partager la seed phrase ni valider une demande "support" qui la réclame.
- Lire ce qui est signé : une "approbation" (approve) peut donner un droit de dépense durable.
- Se méfier des promesses de gains garantis et des urgences artificielles ("dernière chance", "compte bloqué").
- Préférer un wallet distinct pour tester la DeFi/airdrops, avec une petite somme, plutôt

que le wallet principal.