COURS 3 : Sécurité crypto : protège ton argent comme un pro

Module 3.1 — Les erreurs qui peuvent te ruiner (et comment les éviter)

Dans la crypto, **les gains peuvent être rapides**, mais **les pertes aussi**… et souvent, elles viennent de **mauvaises habitudes** ou d'un **excès de confiance**.

Voici les **erreurs les plus dangereuses** que tu dois connaître **avant même** d'acheter ta première cryptomonnaie.

❌ Erreur n°1 — Laisser ses cryptos sur une plateforme sans contrôle

Beaucoup de débutants laissent leurs fonds sur un exchange (Binance, KuCoin, etc.). Le problème : si la plateforme ferme, se fait hacker, ou bloque ton compte, **tes cryptos sont perdues**.

Solution :

- Utilise un wallet personnel (Metamask, Trust Wallet, Ledger…).
- **Règle d'or** : *"Not your keys, not your coins"* (si tu n'as pas les clés privées, tu n'es pas propriétaire).

❌ Erreur n°2 — Partager sa phrase de récupération ou ses clés privées

Ta **phrase de récupération (seed phrase)**, c'est **le double des clés de ta maison**.
Si quelqu'un l'a, il peut vider ton portefeuille, même si tu as un mot de passe.

Solution :

- Ne jamais la stocker en ligne (Google Drive, email, WhatsApp…).
- Écris-la sur papier, garde-la dans un endroit sûr et **hors ligne**.
- Ne la communique **à personne**, même à un "support technique".

❌ Erreur n°3 — Croire aux promesses de gains garantis

Si quelqu'un te promet **"X2 garanti"**, c'est un mensonge.
Dans la crypto, il n'existe **aucun investissement sans risque**.

Solution :

- Fuis les projets qui promettent des rendements fixes irréalistes.
- Apprends à analyser un projet avant d'investir (on verra ça plus tard dans la formation).

❌ Erreur n°4 — Se précipiter par FOMO

La **FOMO (Fear Of Missing Out)** pousse à acheter n'importe quoi "avant que ça monte".
Résultat : tu achètes au plus haut… et tu vends paniqué quand ça chute.

Solution :

- Fixe tes règles d'achat à l'avance.
- Ne mets jamais tout ton capital sur un seul coup.

❌ Erreur n°5 — Ne pas activer la sécurité 2FA

Un mot de passe seul ne suffit pas : un pirate peut le voler.
Sans 2FA (authentification à deux facteurs), ton compte est vulnérable.

Solution :

- Active toujours le 2FA avec **Google Authenticator** ou **Authy**.
- Évite le SMS, plus facile à pirater.

Ce qu'il faut retenir

- La sécurité **n'est pas un détail**, c'est la base.
- 80 % des pertes en crypto viennent **d'erreurs humaines évitables**.
- Si tu appliques ces règles dès aujourd'hui, tu es déjà **plus protégé que la majorité des débutants**.

Dans le prochain module, tu vas découvrir **les clés privées et phrases de récupération** : pourquoi elles sont ton véritable trésor et comment les protéger à vie.

Module 3.2 — Clés privées et phrases secrètes : la clé de ton royaume crypto

En crypto, il y a **une vérité absolue** :

Si tu contrôles tes clés, tu contrôles ton argent.
Si tu ne les contrôles pas, quelqu'un d'autre peut le faire à ta place.

C'est ici que les notions de **clé privée** et **phrase de récupération** entrent en jeu.

1. La clé privée : ta signature numérique

- C'est **un code unique** qui te permet d'accéder à tes cryptos et de signer des transactions.
- Si quelqu'un l'obtient, il peut envoyer **tout ton argent** où il veut.
- C'est l'équivalent **numérique** de la clé d'un coffre-fort.

Important :

- Tu ne "vois" pas directement ta clé privée si tu utilises un wallet classique, mais elle existe en arrière-plan.
- Les plateformes centralisées (Binance, etc.) **gardent la clé pour toi** → ce qui veut dire que tu dépends de leur sécurité.

2. La phrase de récupération (seed phrase)

- C'est **une suite de 12 à 24 mots** qui permet de recréer ton portefeuille **n'importe où**.
- Elle contient en réalité **toutes tes clés privées**.
- Si tu la perds, tu perds l'accès à tes cryptos.
- Si quelqu'un l'a, **il a accès à tout**.

Astuce : pense à cette phrase comme **la "clé maîtresse"** qui ouvre toutes les portes de ton royaume crypto.

3. Ce qu'il ne faut JAMAIS faire

- ❌ Ne jamais la prendre en photo.
- ❌ Ne jamais la sauvegarder sur Google Drive, Dropbox, WhatsApp, email…
- ❌ Ne jamais la donner, même à quelqu'un qui prétend être du support technique.
- ❌ Ne jamais la saisir sur un site dont tu n'es pas sûr à 100 %.

4. Comment bien les protéger

- Écris ta phrase de récupération **à la main** sur papier.
- Stocke-la dans un endroit sûr (coffre, tiroir sécurisé…).
- Fais 2 copies, au cas où une est détruite (incendie, inondation…).
- Pour plus de sécurité, utilise une **plaque en métal** résistante au feu et à l'eau.
- Ne l'entre jamais sur un ordinateur ou un téléphone qui pourrait être piraté.

5. Bonus : la méthode "hors ligne" (cold storage)

- Un **cold wallet** (comme un Ledger ou Trezor) garde tes clés **hors ligne**.
- Même si ton ordinateur est infecté, tes clés restent **en sécurité**.
- C'est la solution **la plus sûre** pour les gros montants.

Ce qu'il faut retenir

- **Clé privée = ta signature**
- **Phrase de récupération = ton passeport maître**
- Si tu les perds ou les partages, c'est comme **laisser ton coffre-fort ouvert**.

Dans le prochain module, tu vas découvrir **les différents types de portefeuilles** (hot wallet, cold wallet…) et apprendre **quand utiliser lequel** pour protéger au mieux tes fonds.

Module 3.3 — Hot wallet ou cold wallet : quel coffre-fort te convient le mieux ?

Tu sais maintenant que **tes clés privées** et **ta phrase de récupération** sont la base de ta sécurité crypto.
Mais **où** et **comment** les garder en sécurité ?
C'est là que les notions de **hot wallet** et **cold wallet** entrent en jeu.

1. Le hot wallet : rapide mais connecté

- **Définition :** un portefeuille **connecté à Internet** en permanence.
- **Exemples :** Metamask, Trust Wallet, Phantom, portefeuilles intégrés aux exchanges (Binance, KuCoin…).
- **Avantages :**
    - Accès facile et rapide à tes fonds.
    - Idéal pour les transactions fréquentes.
    - Gratuit ou peu coûteux.
- **Inconvénients :**
    - Plus exposé aux piratages (phishing, malwares).
    - Si ton appareil est compromis, tes fonds sont en danger.

Conseil :
Utilise un hot wallet pour de **petites sommes**, comme ton porte-monnaie de tous les jours.

2. Le cold wallet : la forteresse hors ligne

- **Définition :** un portefeuille **non connecté à Internet**.
- **Exemples :** Ledger Nano, Trezor, portefeuilles papier, plaques de sauvegarde en métal.
- **Avantages :**
    - Sécurité maximale contre les hackers.
    - Tes clés privées restent hors ligne.
    - Idéal pour les économies à long terme.
- **Inconvénients :**
    - Moins pratique pour des transactions fréquentes.
    - Coût d'achat (environ 70 à 150 € pour un hardware wallet).

Conseil :
Utilise un cold wallet pour **stocker de grosses sommes ou ton épargne long terme**.

3. Trouver ton équilibre : la stratégie “2 poches”

Comme dans la vie réelle :

- **Poche 1 :** Hot wallet = transactions quotidiennes, petits montants.
- **Poche 2 :** Cold wallet = stockage sécurisé, long terme.

Exemple :

- 5 à 10 % de tes cryptos → hot wallet.
- 90 à 95 % de tes cryptos → cold wallet.

4. Pièges à éviter

- Acheter un cold wallet **seulement sur le site officiel** (pas sur Amazon ou d’occasion).
- Toujours **initialiser le wallet toi-même**.
- Ne jamais connecter un cold wallet à un appareil suspect.

Ce qu’il faut retenir

- **Hot wallet = pratique** mais plus exposé.
- **Cold wallet = ultra-sécurisé** mais moins pratique.
- L’idéal est d’utiliser **les deux**, selon la valeur et l’usage de tes cryptos.

Dans le prochain module, tu vas apprendre à **détecter et éviter les arnaques** les plus fréquentes dans le monde de la crypto, pour ne pas perdre ton argent à cause de pièges bien ficelés.

Module 3.4 — Arnaques et phishing : comment ne jamais tomber dans le piège

En crypto, les hackers ne viennent pas toujours casser des systèmes complexes…
Souvent, ils **t'arnaquent en te poussant à leur donner toi-même tes accès**.
C'est ce qu'on appelle **l'ingénierie sociale** : manipuler l'humain plutôt que la machine.

Le but de ce module :

- **Repérer les arnaques** avant qu'elles ne t'atteignent.
- **Réagir correctement** si tu es ciblé.

1. Les arnaques les plus courantes

a) Phishing par email ou site cloné

- Un email qui ressemble à celui de Binance, Metamask, etc.
- Un lien qui t'amène sur un faux site identique au vrai.
- Objectif : te faire entrer ta **phrase de récupération** ou tes identifiants.

Réflexe :

- Ne clique jamais sur un lien reçu par email.
- Tape toujours l'adresse manuellement ou utilise un favori enregistré.
- Vérifie que l'URL commence bien par **https://** et correspond exactement au site officiel.

b) Faux support technique

- Un faux agent te contacte sur Telegram, WhatsApp ou Discord.
- Il prétend t'aider à "récupérer" tes fonds ou "résoudre un problème".
- Il te demande ta seed phrase ou t'envoie un fichier malveillant.

Réflexe :

- Aucune plateforme légitime ne te demandera ta phrase de récupération.
- Bloque et signale immédiatement.

c) Airdrops et cadeaux "trop beaux pour être vrais"

- Un message : "Vous avez gagné 1 000 USDT, cliquez ici pour réclamer !"
- En réalité : un lien qui vide ton wallet ou t'oblige à signer une transaction piégée.

Réflexe :

- Si c’est gratuit et incroyable… c’est probablement une arnaque.
- Ne connecte jamais ton wallet à un site inconnu.

d) Pump & dump / faux investissements

- Une personne te promet un rendement énorme et rapide.
- Envoie-toi un lien pour “investir” → tu perds tout.
- Souvent accompagné de screenshots truqués.

Réflexe :

- Fuis tout projet qui promet des gains garantis.
- Ne mets jamais d’argent que tu ne peux pas perdre.

2. Plan de défense anti-arnaque

1. **Doute toujours** des messages non sollicités.
2. **Ne communique jamais** ta phrase de récupération.
3. **Vérifie l’URL** avant toute connexion à un site.
4. **Utilise un wallet séparé** pour tester les nouvelles plateformes.
5. **Active les notifications** sur tes wallets et exchanges.

3. Que faire si tu es piégé ?

- **Si tu as cliqué sur un lien mais pas donné tes infos :**
  - Change tes mots de passe immédiatement.
  - Analyse ton appareil avec un antivirus.
- **Si tu as donné ta seed phrase :**
  - Transfère immédiatement tes fonds vers un nouveau wallet sécurisé.
  - Considère l’ancien comme perdu.

Ce qu’il faut retenir

- Les hackers attaquent **ton attention et ta confiance**, pas seulement ton ordinateur.
- Ton **cerveau** est ton meilleur antivirus.
- Un bon réflexe peut te sauver **des milliers d’euros**.

Dans le prochain module, on mettra tout ça en pratique avec **un plan de sécurité crypto en 5 étapes**, simple à suivre pour dormir tranquille.

Module 3.5 — Sécuriser tes cryptos en 5 étapes simples

Protéger tes cryptos n'est pas réservé aux experts en cybersécurité.
Avec quelques **bons réflexes**, tu peux déjà être **beaucoup plus protégé que 90 % des débutants**.

Voici **un plan de sécurité en 5 étapes simples** que tu peux mettre en place dès maintenant.

1. Choisis le bon wallet et sépare tes usages

- Utilise **un hot wallet** (Metamask, Trust Wallet…) pour tes transactions quotidiennes.
- Utilise **un cold wallet** (Ledger, Trezor) pour ton épargne long terme.
- Ne garde sur un exchange que le strict nécessaire.

Astuce : applique la **règle des deux poches** :

- Poche 1 (hot) = argent de tous les jours.
- Poche 2 (cold) = ton coffre-fort.

2. Protège ta phrase de récupération et tes clés privées

- Écris ta seed phrase sur papier (ou gravée sur métal).
- Garde-la dans un lieu sûr, **hors ligne**.
- Ne la partage **jamais** avec qui que ce soit.
- Fais une ou deux copies dans des endroits séparés.

Règle d'or : *Si quelqu'un a ta phrase, il a ton argent.*

3. Active les sécurités supplémentaires

- Active le **2FA (Google Authenticator)** sur tous tes comptes crypto.
- Utilise des mots de passe **longs et uniques** pour chaque plateforme.
- Change régulièrement tes mots de passe.
- Sur ton téléphone et PC : verrouillage par code + empreinte digitale.

Astuce : un gestionnaire de mots de passe fiable peut t'aider à tout retenir.

4. Reste vigilant contre les arnaques

- Ne clique pas sur les liens envoyés par email ou message.

- Vérifie toujours l'URL des sites.
- Méfie-toi des "opportunités" trop belles pour être vraies.
- Ne communique jamais ta seed phrase, même à un "support technique".

Rappel : ton cerveau est ton meilleur antivirus.

5. Fais un contrôle régulier de ta sécurité

- Vérifie tes wallets et comptes au moins **une fois par mois**.
- Mets à jour tes applications et ton firmware de cold wallet.
- Supprime les apps ou extensions que tu n'utilises plus.
- Passe en revue où et comment tes clés/phrases sont stockées.

Astuce : mets un rappel mensuel dans ton agenda.

Conclusion

La sécurité crypto n'est pas un événement unique, c'est **une habitude**.
Si tu appliques ces 5 étapes, tu réduis **énormément** les risques de perdre tes fonds.

Bravo, tu viens de terminer le **Bloc 3** 🎉
Tu as maintenant les bases pour **protéger ton argent comme un pro**.

Prochaine étape : **Bloc 4 — Acheter et vendre des cryptos sans te tromper**.
Tu vas apprendre à passer à l'action **en toute sécurité et au meilleur prix**.