



**L'Hérôïne Monero dit :
Fais pas le con**

Maitrisez la Sécurité de Votre Bourse d'Échange

Les bourses d'échange peuvent être une manière pratique d'acheter et de vendre plus de Monero, mais toutes les bourses ne naissent pas égales.

Voici quelques éléments à garder en tête lorsque vous souhaitez conserver vos Monero en sécurité si vous utilisez des bourses.

1. Faites vos propres recherches avant d'utiliser une quelconque bourse. Essayez d'obtenir les réponses à ces questions :

- Y a-t'il des critiques positives disponibles sur des sources tierces ? Sont-elles fiables ?
- A-t-elle déjà été attaquée ? La réponse à l'attaque était-elle appropriée ?
- Depuis combien de temps la bourse est en fonctionnement ?
- Les créateurs / gestionnaires sont-ils des individus ou entités connus ou réputés ?
- Pouvez-vous maintenir votre confidentialité en ne partageant aucune information personnelle ?
- Le site web utilise-t'il des précautions de sécurité comme des captcha ou une authentification à deux facteurs (2FA) ? A-t'il un certificat de sécurité légitime et commence-t'il avec <https://> ?
- Si vous avez prévu de déclarer des impôts, la bourse permet-elle de télécharger des rapports pour faciliter les preuves d'ordre d'achat et de vente ?

2. Les bourses créent leurs propres portefeuilles pour vous. Vous n'aurez certainement pas accès à la phrase mnémorique du portefeuille de la bourse. Si la bourse est attaquée ou s'avère être une arnaque, vous pourriez perdre la quantité de XMR disponible sur votre portefeuille. Une bonne règle de base est de ne garder des XMR sur une bourse que si vous prévoyez de les utiliser rapidement. Sinon, déplacez-les sur un portefeuille que vous contrôlez.

3. Si vous voulez échanger des montants important sur une bourse, envisagez de tester la transaction en échangeant d'abord un montant plus faible. Ce montant de test ne devrait pas être plus élevé que ce que vous accepteriez de perdre.

4. Pour chaque transaction XMR, vérifiez toujours deux fois les adresses de dépôts et d'envoi du portefeuille pour vous assurer qu'elles sont correctes. Même si vous copiez/collez l'adresse, vérifiez qu'elle a été collée correctement, car il y a des attaques connues qui change une adresse de cryptomonnaie lorsqu'elle est copiée / collée. Si votre équipement a été d'une quelconque façon infecté par un logiciel malveillant, une simple double vérification pour confirmer qu'elle a été collée correctement est tout ce dont vous aurez besoin pour protéger vos XMR.

5. À l'avenir, les bourses décentralisées deviendront plus fréquentes. Monero étant une cryptomonnaie décentralisée, ces bourses sont en phase avec la philosophie de Monero. Envisagez de les utiliser, mais faites toujours vos propres recherches d'abord.