Les cryptos et la sécurité.

Nous entrons dans une nouvelles ère, celle de la Blockchain et des cryptomonnaies. Ces technologies, révolutionnaires, se démocratisent de jour en jour et le nombre d'utilisateurs augmente exponentiellement.

Cependant, l'engouement général pour ce qui va bouleverser le monde de la finance et des services, attire aussi arnaques et profiteurs sans scrupules. De par sa nature numérique, la cryptomonnaie facilite et multiplie les mouvements de capitaux, accompagnés de son lot d'opportunistes malhonnêtes, s'engouffrant dans les failles de sécurité laissée ouvertes par certains nouveaux utilisateurs.

Dans cet article, nous allons tenter d'identifier les risques liés à l'utilisation et à l'échange des cryptomonnaies, de l'achat au stockage, en passant par leur transfert et surtout, quelles sont les parades possibles au piratage ou à la perte de ses informations.

1 Une adresse mail sécurisée

Lorsque l'on s'inscrit sur une plateforme d'échange, une étape indispensable est de fournir une adresse mail. Nos boites mails sont souvent vieilles, sur-utilisées et remplies de spam. De plus, des fournisseurs comme Google (Gmail), Yahoo ou Microsoft (Outlook), n'hésitent pas à vendre vos données à des entreprises partenaires. Créer une boite vierge et uniquement dédiée au monde de la crypto, est donc vivement recommandé. Cela évitera de continuer à fournir des informations précieuses dans une boite vérolée, une manne providentielle qui pourrait servir les intérêts de hackers. Heureusement, il existe des entreprises de messagerie conscientes, sécurisées et anonymes, permettant le chiffrement de vos informations (Protonmail, Tutanota pour citer les principales).

2 Les plateformes d'échange

Le choix de la plateforme d'échange est aussi un paramètre à ne pas négliger quand on commence dans les cryptos. Il est fortement recommandé de choisir parmi les plateformes qui ont pignon sur rue, en

se référant aux sites de classement (Coin Market Cap pour ne citer que lui). En effet, certaines pourraient vous hameçonner avec des offres attractives et des frais de transaction bas, souvent au dépend de la sécurité et du sérieux de l'entreprise. On pourra prendre l'exemple de Idax, dont les patrons ont fui avec les capitaux ou Pancake Swap, qui a connu récemment une faille de sécurité. Pour cela il est recommandé aux nouveaux investisseurs comme aux plus chevronnés, de ne pas laisser ses cryptos dormir sur les plateformes d' échange. Ce qui nous amène à notre troisième chapitre : conserver ses fonds en sécurité.

3 Les portefeuilles cryptos (wallet)

- les wallets dématerialisées (software) :

Il existe une solution et simple souvent gratuite pour sécuriser ses cryptomonnaies. Des logiciels en ligne permettant de conserver ses capitaux en sécurité, les wallet. Celles-ci utilisent des identifiants de connexion complexes, rendant très difficile le piratage, grâce à des suites de 24 ou 12 mots (phrase mnémonique) et des clés privées uniques de 64 caractères. Couplée à un identifiant et un mot de passe, cette solution est indispensable pour éviter quelques déconvenues. Mew, Metamask, Trustwallet ou Whetio wallet en sont quelques exemples. Leur plus grand défaut est qu'elles sont en ligne, donc exposées.

- les wallets physiques (hardware) :

Pour pallier au risque d'exposer ses cryptos en ligne, il existe une solution parfaite : les hardware wallets.
Elles se présentent souvent sous la forme d'une clé usb et offrent les mêmes options de sécurité que leur consœurs numériques. Elles permettent de plus, de conserver ses fonds sur un support qui n'est connecté que lorsque que vous la branchez à votre ordinateur et vous devrez taper un code PIN directement sur la clé pour l'activer. Ledger ou Trezor sont de bons exemples dans ce domaine. Leur plus grand défaut est celui d'être physiques, donc susceptibles d'être détériorées ou perdues.

4 Des sites internet sûrs pour éviter le phishing (hameçonnage)

Une méthode souvent employée et parfois négligée par les utilisateurs de cryptos et d'internet en général, est le phishing. Certains hackers créent des copies presque parfaites de sites internet existants, afin de tout simplement récupérer vos identifiants de connexion, numéros de carte bleue etc… (on peut trouver par exemple de nombreux sites imitant MEW). Afin d'éviter au maximum de tomber dans ce traquenard, il faut être vigilant et vérifier le nom du domaine, qui doit être conforme et identique à l'original. Ne suivez pas aveuglément des liens dans les forums ou dans vos boites mails, utilisez des liens sûrs. Le choix d'un navigateur est aussi important, certains vous avertiront sur le taux de confiance du site sur lequel vous surfez et empêchent certains sites de collecter vos informations et données grâce aux cookies, comme Brave ou Opera.
Ces navigateurs permettent aussi de se connecter via un VPN, logiciel, souvent payant, qui va créer un tunnel sécurisé entre vous et internet (NordNet, Cyberghost …).

5 Conserver ses identifiants en sécurité

Comme nous avons pu le voir plus haut, les méthodes de sécurisations sont nombreuses. Il faut donc les conserver à l'abri des regards indiscrets ainsi que de l'oubli. Il est fortement conseillé de garder ces informations de connexion sur différents supports :

- **Le bloc-note :** Aussi simple que cela puisse paraitre, noter ses identifiants sur un support papier est une solution qui vous permettra de ne pas oublier ou perdre vos infos de connexion dans un ordinateur ou autre support numérique, qui aurait eu la mauvaise idée d'arrêter de fonctionner sans prévenir. Et le papier est hors ligne !

- **Les supports numériques :** On peut aussi conserver ses mots de passe, mnémoniques et autres identifiants dans une clé usb, un disque dur ou simplement en photo, tant que ces derniers sont utilisés au minimum en ligne.

Conclusion

Comme nous avons pu le voir, hackers et arnaqueurs ne manquent

pas de ressources pour dévaliser vos capitaux. Ils profitent de l'engouement et de la méconnaissance du grand public pour les cryptomonnaies. Cependant, il existe de nombreuses parades pour contrer ces attaques, de la plus simple, à la plus technologique.
Bien qu'en essayant, on ne peut pas fournir une liste exhaustive des risques et parades, tellement la technologie des Blockchains évolue rapidement. Mais avec ces informations, vous avez déjà de quoi parer à la plupart d'entre eux.

Bon trade à vous, allez en sécurité !

Le Mehd.