Hors-série n°3

L'hygiène numérique & les cryptomonnaies

L'hygiène informatique… vaste sujet ! J'en ai fait en partie mon métier et un constat est clair :
Dans 99% des cas, le problème est entre la chaise et clavier !

De façon générale mais plus encore lorsque l'on manipule des crypto monnaies, il est important de ne pas faire n'importe quoi avec son ordinateur / smartphone. Il n'existe pas de système sûr à 100%. C'est une chimère après laquelle on peut courir toute une vie. Cependant, à défaut d'atteindre ces 100%, il existe des méthodes pour s'en approcher. Voici donc quelques exemples, méthodes, réflexes, réflexions autour de la sécurité que je vous invite à suivre. Je commencerai par ceux qui ne coûtent rien, ou pas grand-chose. Puis, suivant votre capital et la valeur de vos cryptomonnaies, vous exposerai des méthodes pour aller plus loin. La maître mot à mon sens est « diversification ».

Niveau 1 - Tout est gratuit ! Et important.

Admettons que vous disposez d'un faible capital en cryptomonnaies, et que vous souhaitez simplement savoir ce que vous pourriez faire pour limiter les risques sans avoir à dépenser plus d'argent. Ces conseils sont aussi valables pour la vie de tous les jours ; Vous utilisez votre PC pour accéder à votre banque, au site des impôts, votre boîte mail, vos photos/vidéos privées etc. alors apprenez les bons réflexes 😊

1. Gardez vos appareils numériques à jour. Windows, Android, iOS, tous ces systèmes proposent des mises à jour de sécurité régulières. Ne pas les faire c'est vous exposer encore d'avantage à ce que vos appareils soient compromis, et quelqu'un puisse en prendre le contrôle à distance ou enregistrer toutes vos frappes au clavier.

2. Utilisez sur votre PC un compte qui ne soit pas « administrateur » de la machine. De cette façon si vous cliquez sur un mauvais lien qui essaie d'installer quelque chose à votre insu, on vous demandera un mot passe. Vous pourrez alors vous dire que ce n'est pas normal, cliquer sur « Annuler » et vous dire « Ouf, je l'ai échappé belle ».

3. N'installez un logiciel que depuis les sites de son éditeur ! N'allez pas les prendre sur Clubic, Softsonic ou je ne sais quoi. Pour télécharger greenshot par exemple, un logiciel de prises d'écran, c'est greenshot.org par 01net. Qu'ont à gagner ceux qui proposent les logiciels des autres ? Attirer du monde ? En tout cas ils n'ont pas le même souci de proposer les sources saines des logiciels que les éditeurs eux-mêmes.

4. Faîtes une analyse régulière de votre PC à l'aide de votre antivirus et d'un anti-malware. Windows intègre un antivirus gratuit. Il est léger mais a le mérite d'exister. Pour les malwares j'utilise MalwareBytes, il y en a d'autres (DYOR 😉). Là encore à télécharger sur le site de l'éditeur, évidemment ! https://fr.malwarebytes.com/

5. Utilisez un serveur DNS fiable. Un DNS converti google.fr en adresse IP pour que votre PC s'y connecte. Que se passe-t-il si le DNS renvoie l'IP d'un site contrefait ? Vous y accèderez et n'en saurez rien. Vous saisirez vos mots de passe etc. qui seront alors enregistrés par le site, donc le ou les pirates.

6. Ayez des appareils aussi propres que possible. Pas de sites/applications bizarres ou douteux, de pornographie ou de smartphone rooté avec des applications téléchargées autre part que le store officiel. Evitez les jeux vidéo, limitez l'accès de vos enfants au PC qui vous sert aux tâches administratives. On les aime, ce n'est pas la question, mais l'erreur est humaine. « Mais maman, ils disaient que c'était gratuit pourtant ! ». L'idéal étant d'avoir un équipement dédié ou presque aux cryptomonnaies. Le strict minimum, nécessaire et suffisant.

7. Créez des comptes sur plusieurs échanges et répartissez vos cryptomonnaies de façon équitable. Cela limitera vos pertes si un échange venait à ne plus être disponible. (Piratage, attaque DDOS, poursuites judiciaires etc)

8. Ayez une vraie gestion de vos mots de passe. Rien de pire qu'avoir le même mot de passe partout avec le nom de votre chien ou la date de naissance de vos enfants. Il est primordial d'avoir un mot de passe différent pour chaque échange/application, qui soit généré de façon aléatoire, 16 caractères, avec symboles.

   « Aaahh impossible à retenir ! ». J'utilise LastPass pour cela, un mot de passe très complexe principal à retenir + connexion à Last Pass avec une double authentification. Je ne connais aucun de mes mots de passe, je n'en ai pas besoin.

   D'autre part un code PIN « 0000 » c'est NUL ! Qu'on soit clair. Une personne prend votre portable, sort carte SIM, la met dans un autre portable et peut recevoir tous vos SMS. Changez le 😉

9. Activez la double authentification (2FA, 2 factors authentication) sur TOUS vos comptes. Le principe est soit, en plus de votre mot de passe, de recevoir un code par SMS quand vous vous connectez, soit d'utiliser une application de type Google authenticator qui vous génère un code de confirmation qui change toutes les 30 secondes.

10. Formez-vous, par exemple à l'aide des MOOC de l'ANSSI afin d'apprendre à identifier des mails douteux et à ne pas cliquer sur n'importe quoi. https://secnumacademie.gouv.fr/

11. Ne communiquez pas sur les réseaux sociaux concernant vos crypto monnaies. Vous en avez, super, mais évitez de devenir une cible. Une personne pourrait voir votre post où mettez que « ça y est j'ai dépassé les 10000 euros » et faire du « social engineering » sur vous. Chercher tous vos comptes sur Twitter/Instagram/Facebook etc. pour identifier le nom de votre chien, vos passions, le ou les échanges sur lesquels vous êtes, trouver peut-être votre adresse électronique et chercher vos mots de passe ou vous envoyer un magnifique mail contrefait en se faisant passer pour votre échange avec plein de détails sur votre vie privée. Le parfait guet-à-pents. Archivez vos anciens posts qui n'ont plus aucune utilité. Fermez votre compte Facebook et supprimez l'application de votre Smartphone. Cette application est le plus gros cheval de Troie de l'histoire et tout le monde s'en fou, c'est formidable 🤣 « Ben oui mais c'est pratique ! Alors bon… ». -> Utilisez Signal.

Si déjà vous cochez toutes ces cases, **bravo !** Vous êtes vraiment sur la bonne voie et plus soucieux de votre comportement en ligne que 95% des utilisateurs.

Niveau 2 : budget < 150€

Admettons que vous ayez aujourd'hui une somme plus importante en crypto monnaies, disons 2000€ pour donner un exemple, que vous respectiez déjà tous les points du niveau 1 (impressionnant !) mais que vous aimeriez aller plus loin. On ne sait jamais, votre PC pourrait se retrouver compris, une clé USB d'un copain, un site de streaming, un logiciel téléchargé sur Softsonic ou que sais-je… Pour le principe, dîtes-vous que votre appareil est compromis et demandez-vous ce que quelqu'un qui y a accès pourrait faire de vos données et de vos accès. Oui, c'est inquiétant !

Utilisez alors un « cold wallet » pour la majorité de vos crypto monnaies (>80%). J'utilise entre autres deux Ledger Nano, il y en a d'autres comme Ellipal, comparez et choisissez le vôtre.

Un cold wallet s'achète sur le site du fabriquant, pas sur Amazon. « Ah ben oui mais c'est moins cher ! ». On s'en fiche ! Vous n'avez aucune garantie que le portefeuille que vous achetez sur Amazon provienne bien du fabriquant. On fait quoi si le revendeur a changé le logiciel interne au Wallet pour récupérer toutes vos cryptos ? 😅 Ces portefeuille hors ligne ont le gros avantage d'être hors ligne justement. Aucune action ne peut être faîte alors sur vos crypto monnaies sans une action physique de votre part, brancher le wallet, et taper un code PIN dessus.

Une Ledger Nano S peut stocker 4 cryptomonnaies différentes en raison de la taille de sa mémoire. Environ 60€. https://shop.ledger.com/products/ledger-nano-s

Un Ledger Nano X peut en stocker BEAUCOUP plus. https://shop.ledger.com/products/ledger-nano-x

Il n'est pas question de quantité de cryptomonnaies mais bien de cryptomonnaies différentes. Exemple BTC, ETH, XRP XLM. Vous pouvez en avoir autant de chaque que vous voulez mais pas une cinquième.

Là encore, si votre budget le permet, je vous invite à en avoir au moins 2, de marques différentes. Pourquoi ? On ne sait jamais. Imaginez que le logiciel interne de Ledger ait un souci lors d'une mise à jour, faisant tomber en panne tous les Ledgers dans le monde en même temps. Pour restaurer votre portefeuille, il vous en faudra un autre. Mais tous les clients vont en vouloir un autre donc tout le monde va en commander en même temps. Vous croyez vraiment faire partie des chanceux de l'avoir sous 4 jours ?

Ce qu'il faut retenir c'est que la meilleure protection reste la diversification. La majorité hors ligne, sur deux cold wallets si possible, en avoir un étant déjà un très bon début, et le reste réparti sur plusieurs échanges, ou wallets de type Metamask etc.

Niveau 3 : budget illimité

Vous avez déjà tout fait sur les niveaux 1 et 2 mais ça ne vous suffit pas ? Vous êtes paranoïaques ? Vous avez 30 000 000 de dollars en cryptos ? Les institutions complotent pour faire exploser une EMP près de chez vous ? Un satellite vous observe par la fenêtre de votre chambre quand vous tapez au clavier ? Votre fournisseur d'accès sait tout de votre vie numérique et un de leur salarié essaie de vous pirater ? Si on devient extrémiste de la sécurité, jusqu'où pouvons-nous aller ?

Aucun jugement là-dedans, je suis moi-même très à cheval sur la sécurité et le respect de ma vie privée et de mes données personnelles, je ne vous jetterai pas la pierre. Alors voici quelques idées pour aller plus loin.

1. Remplacez le routeur de votre opérateur. Ben oui, pourquoi utiliser la box de free ou d'Orange ? Vous avez la possibilité d'en installer un autre. J'utilise personnellement celui-là, pour sa simplicité mais aussi pour la solution de contrôle parental qu'il propose. Synology en propose un sympa. De 200 à 1500€.
2. Achetez d'autres cold wallets, la diversification est une excellente protection.
3. Utilisez un VPN pour tout. Lorsque vous postez un message sur les réseaux sociaux, votre adresse IP est enregistrée par le serveur. Un petit malin pourrait donc récupérer votre adresse IP personnelle et tenter d'accéder aux données de celui qui « vient enfin d'arriver à 10000€ ! ». Vous pouvez configurer un VPN directement sur certains routeurs de sorte que votre adresse IP n'est jamais révélée
   lée, par aucun de vos équipements.
4. N'utilisez pas les clouds publics. Achetez un NAS, DYOR, j'aime bien Synology, mettez-le chez vous, branché sur un onduleur, et ne stockez RIEN chez Google, Apple et consort, que ce soit vos photos comme vos contacts etc. Désactivez la localisation et la synchronisation sur leurs plateformes.
5. Ayez votre propre serveur de messagerie et votre propre domaine. Il est de notoriété publique de Google scanne les e-mails de ses clients, officiellement pour proposer de la publicité ciblée. Ben voyons !
6. Ne partagez RIEN sur les réseaux sociaux. Fermez votre compte Facebook, s'il vous plaît. Dans une formation sur la cyber sécurité donné dans une école reconnue, le premier cours consiste à expliquer aux étudiants pourquoi et comment le faire. Pourquoi à votre avis ?
7. Ayez au moins DEUX équipements dédiés aux cryptomonnaies, les deux à jour, avec votre solution de double authentification type Google Authenticator sur les deux, le second devant rester éteint 99% du temps, à n'utiliser que pour installer les mises à jour lors d'une défaillance du premier.
8. Stockez votre second PC ainsi que vos cold wallets dans une cage de Faraday pour les protéger des ondes électromagnétiques. Il existe plein de tutoriaux pour réaliser la vôtre sur Internet.
9. Effectuez des sauvegardes régulières de votre PC à l'aide d'outils comme Veeam. **Attention, sauvegarder, c'est dupliquer**. Donc faîtes une sauvegarde sur un disque dur ou un NAS par exemple, puis dupliquez la sauvegarde sur un autre support.

Vous l'aurez compris, la sécurité ce n'est pas juste un bon antivirus. C'est un ensemble de mesures, d'habitudes, de comportement à avoir ou à éviter et qui vont, mis bout à bout, non pas sécuriser à 100% mais limiter les risques au maximum.

D'autres idées / exemples vont certainement me venir à l'esprit dans le temps, je mettrai donc le document à jour régulièrement.

Soyez prudents ! 😉