Experts Crypto

Bulletin d'information septembre 2023

INTRODUCTION

Le mois de septembre est la période de reprise pour la majorité d'entre nous. Nous espérons que cet été a pu être agréable pour tous.

Dans la newsletter de ce mois, nous souhaitions vous proposer un panorama des bonnes pratiques de la sécurité informatique.

Nous avons la chance de travailler avec des individus formés et compétents dans ce domaine, il nous parait judicieux de vous communiquer certaines informations utiles.

Si à la lecture de ce document vous sentez le besoin d'aller plus loin, vous pouvez nous adresser vos demandes spécifiques à : contact@uap.company

ANALYSE TECHNIQUE

Bitcoin en hebdomadaire
Le mois de septembre a été relativement plat. Le prix s'est déplacé entre 27500 et 24900 $ pour une volatilité sur le mois de 9%.

Le prix est revenu au niveau des 27 200 $ en fin de mois, après avoir maintenu le niveau du précèdent point bas de juin un peu en dessous des 25 000 $.

Octobre est un mois favorable à la hausse comme peux le montrer l'historique des performances du Bitcoin. Le 4ème trimestre de l'année a régulièrement été une période favorable surtout les années ou la performance n'a pas été exagérée durant l'année.

BTC | Daily returns(%) | Weekly returns(%) | Monthly returns(%) | Quarterly returns(%)

Time	January	February	March	April	May	June	July	August	September	October	November	December
2023	39.63%	0.03%	22.96%	2.81%	-6.98%	11.98%	-4.02%	-11.29%	4.04%			
2022	-16.68%	12.21%	5.39%	-17.3%	-15.6%	-37.28%	16.8%	-13.88%	-3.12%	5.56%	-16.23%	-3.59%
2021	14.51%	36.78%	29.84%	-1.98%	-35.31%	-5.95%	18.19%	13.8%	-7.03%	39.93%	-7.11%	-18.9%
2020	29.95%	-8.6%	-24.92%	34.26%	9.51%	-3.18%	24.03%	2.83%	-7.51%	27.7%	42.95%	46.92%
2019	-8.58%	11.14%	7.05%	34.36%	52.38%	26.67%	-6.59%	-4.6%	-13.38%	10.17%	-17.27%	-5.15%
2018	-25.41%	0.47%	-32.85%	33.43%	-18.99%	-14.62%	20.96%	-9.27%	-5.58%	-3.83%	-36.57%	-5.15%
2017	-0.04%	23.07%	-9.05%	32.71%	52.71%	10.45%	17.92%	65.32%	-7.44%	47.81%	53.48%	38.89%
2016	-14.83%	20.08%	-5.35%	7.27%	18.78%	27.14%	-7.67%	-7.49%	6.04%	14.71%	5.42%	30.8%
2015	-33.05%	18.43%	-4.38%	-3.46%	-3.17%	15.19%	8.2%	-18.67%	2.35%	33.49%	19.27%	13.83%
2014	10.03%	-31.03%	-17.25%	-1.6%	39.46%	2.2%	-9.69%	-17.55%	-19.01%	-12.95%	12.82%	-15.11%
2013	44.05%	61.77%	172.76%	50.01%	-8.56%	-29.89%	9.6%	30.42%	-1.76%	60.79%	449.35%	-34.81%

Le marché reste en attente de l'approbation des ETFs qui permettront de rouvrir une dynamique d'investissement. La SEC (Security Exchange Commission) continue de repousser les demandes des institutions dont les dates finales d'approbation sont communiquées pour mars 2024.

S&P 500 en hebdomadaire

Pour les activités boursières traditionnelles, nous pouvons observer une volatilité baissière plus conséquente sur le S&P500 (indice US). L'intérêt pour les investisseurs a bien été présent en 2023 sur les actions. En effet, les bénéfices des entreprises en 2022 ont été conséquents, donnant lieu à des dividendes importantes.

Les entreprises ont réussi à augmenter leurs tarifs proportionnellement à l'augmentation des prix de l'Energie ce qui se traduit par une inflation généralisée. Les investisseurs en 2023 ont gardé confiance dans les entreprises à pouvoir continuer de dégager des marges ; ce qui a poussé le prix des actions à la hausse sur le premier semestre de l'année.

Une correction d'encore 5 à 10% sur l'indice S&P 500 semble probable.

ANALYSE FONDAMENTALE

Dans ce chapitre nous souhaitons vous partager nos connaissances et pratiques relatives à une activité digitale saine. Internet offre des possibilités quasi infinies à ses utilisateurs laissant place à la créativité des moins bien intentionnés.

Les hackers connaissent le fonctionnement des applications informatiques, des protocoles réseaux et des principes de sécurisation des informations qui transitent. Le piratage est une pratique fastidieuse qui dans certains des cas, peut être très rémunérateur.

Un hacker ou pirate informatique reste un homme derrière une machine. Ce dernier agit de manière rationnelle, à savoir mener une action profitable. C'est pourquoi ils visent en majorité des profils qui sont sensibles ou juteux. Que son objectif soit financier, politique ou à des fins de nuisance, il déploiera des moyens proportionnés au résultat attendu. Ces actions vont toujours nécessiter des ressources, elles peuvent être : du temps investi dans l'action, l'achat d'informations, des ressources informatiques conséquentes, …

En somme, en piratage, on attaque que si le jeu en vaut la chandelle. Le pirate identifie le point de vulnérabilité le plus facilement exploitable pour un enjeu (financier ou nuisance) qui dépassera l'investissement engagé. Dit plus clairement, s'il n'y a rien à voler, aucun pirate ne va s'y intéresser et si le système est sécurisé, il cherchera la porte la plus faible du système.

En sécurité informatique, il est primordial de mener les actions de sécurité sur les maillons les plus faibles.

La sécurité informatique vise à combler les failles naturellement présentes dans les applications et protocoles. L'état actuel de l'informatique est le résultat de modifications et apports de sécurité à la suite de failles et piratages subits ces 30 dernières années.

1. Votre poste informatique et/est mobile

La première fois que j'ai vu l'informatique chez moi, j'avais 11 ans, ça ressemblait physiquement à cela. Lorsque je revois cette photo, je prends conscience que les systèmes informatiques et les réseaux ont suivi une évolution exponentielle au cours des dernières décennies.

Le développement de l'informatique au sens large a permis de faciliter les échanges d'informations générant des gains de productivité considérables qui ont transformé le monde économique.
Les progrès matériels et réseaux ont amenés à la création de nombreux appareils, connectés à internet, pour lesquels nous comprenons de moins en moins le fonctionnement.

Il est donc important de considérer l'informatique comme un ensemble d'éléments : matériels, réseaux, applications, protocoles, systèmes qui communiquent entre eux.

Parmi ces éléments, vous êtes physiquement en interface avec **un ordinateur** (fixe ou portable) et **un smart mobile**. Ces derniers sont connectés au réseau internet et les communications sont quasi permanentes avec ce dernier.

a. Protegez vos appareils mobiles

Les téléphones mobiles intelligents (smartphones) et tablettes informatiques sont devenus des instruments pratiques du quotidien, tant pour un usage personnel que professionnel.

Ces terminaux disposent de nombreuses fonctionnalités :

- Capteurs divers (GPS, altimètre, gyromètre, accéléromètre, microphone, caméra, etc.)
- Communication par liaison sans-fil
- Grande capacité de stockage
- Performances permettant l'usage d'applications sophistiquées.

Ces terminaux permettent par exemple, en plus d'être joignable, de consulter ses courriels et de naviguer sur internet à la recherche de tout type d'information. Plus encore, ils rendent possible la connexion à un réseau d'entreprise pour travailler sur des applications métier ou accéder à des documents comme tout un chacun le ferait depuis son poste de travail professionnel. En parallèle, de nombreux usages personnels, souvent ludiques, de ces appareils sont entrés dans les mœurs.
Ils contiennent tout autant et plus d'informations personnelles ou sensibles que votre ordinateur. Ils sont aussi plus faciles à perdre ou à se faire voler. Ces appareils mobiles sont, malgré tout, généralement bien moins sécurisés que les ordinateurs par leurs propriétaires.

b. Mettez en place un code d'accès

Qu'il s'agisse du code de déverrouillage ou du code PIN de votre téléphone ou votre ordinateur, ces protections complémentaires empêcheront une personne malintentionnée de pouvoir se servir facilement de votre appareil si vous en perdez le contrôle (perte, vol, abandon) et donc d'accéder à vos informations.

Bien entendu, vos codes d'accès doivent être suffisamment difficiles à deviner (évitez 0000 ou 1234, votre date de naissance). Activez également le verrouillage automatique de votre appareil afin que le code d'accès soit demandé au bout de quelques minutes si vous laissez votre appareil sans surveillance.

c. Faites des sauvegardes

Votre appareil mobile contient généralement des informations que vous n'avez nulle part ailleurs, comme votre répertoire de contacts, vos messages, vos photos… Pensez à le sauvegarder régulièrement car vous pourriez tout perdre en cas de casse, de perte ou de vol.

d. Contrôler les autorisations de vos applications

Vérifiez également les autorisations que vous donnez à vos applications lors de leur première installation, mais aussi après leurs mises à jour car leurs autorisations peuvent évoluer.
Certaines applications demandent parfois des droits très importants sur vos informations et qui peuvent être « surprenants ». Par exemple, un simple jeu de cartes « gratuit » qui vous demanderait l'autorisation d'accéder à votre répertoire, vos messages, votre position GPS ou encore votre appareil photo est évidemment suspect. Au moindre doute, n'installez pas l'application et choisissez en une autre.

Pour supprimer une application qui se lance au démarrage sur votre ordinateur (Windows), vous pouvez y accéder par le "Gestionnaire des taches"

- Ctrl+Alt+Suppr -> gestionnaire de taches -> applications de démarrage

Sur votre téléphone mobile (Android ou iPhone) ouvrez l'application des "Paramètres" puis consultez les autorisations données à vos applications.

e. Ne stockez pas d'informations confidentielles sans protection

Ne notez jamais d'informations secrètes comme vos mots de passe, informations personnelles ou vos codes bancaires dans votre messagerie ou un fichier non chiffré sur votre appareil mobile.

Un cybercriminel qui aurait pris le contrôle de votre appareil pourrait facilement les récupérer. En outre, certaines applications que vous avez installées peuvent aussi accéder et récupérer ces informations dont vous perdriez alors le contrôle. Pour protéger vos informations secrètes, utilisez une solution de chiffrement avec un mot de passe solide.

2. Des mots de passe robustes

L'informatique nous amène à utiliser un ou plusieurs mots de passe pour sécuriser l'accès à nos appareils et applications du quotidien.
Banque, e-commerce, messagerie électronique, documents, administration : de nombreuses démarches de notre vie quotidienne passent désormais par Internet et par la création de comptes sur les différents sites. Nombre de ces espaces privatifs contiennent des informations confidentielles qui ne doivent pas être rendues disponibles à des personnes non habilitées.

a. Générer un mot de passe fort

Un bon mot de passe peut contenir, par exemple, au moins 12 caractères et 4 types différents : des minuscules, des majuscules, des chiffres et des caractères spéciaux.

Un mot de passe ne doit rien dire sur vous :
Personne ne doit deviner votre mot de passe à partir du nom de votre chien ou de votre film préféré. Encore trop de personnes génère des mots de passe avec le nom de leur conjoint et la date de naissance de leur premier enfant.
On retrouvera des mots de passe de type : Corine1903$ ou Paul2712*

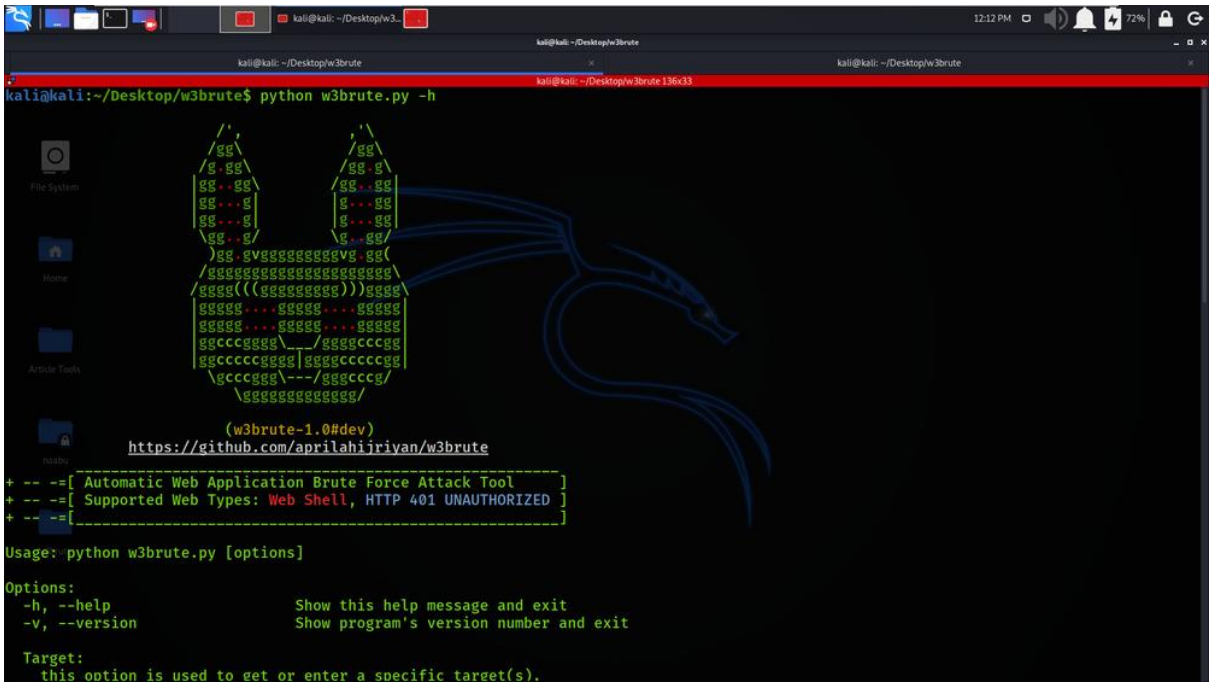
https://generateurdemotdepasse.fr/
Ce site permet de générer des mots de passe difficilement attaquable.
En voici quelques exemples :
Zc<%.r8A6W8q
]3Ri}9<NRyi3
7tT39gK<c@)F

b. Cracker un mot de passe

L'**attaque par force brute** est une méthode utilisée pour trouver un mot de passe ou une clé. Il s'agit de tester, une à une, toutes les combinaisons possibles.

Cette méthode est en général considérée comme la plus simple parmi les techniques car nécessitant le moins de connaissance. Elle permet de casser tout type de mot de passe en un temps fini indépendamment de la protection utilisée, mais le temps augmente avec la longueur du mot de passe. En théorie, la complexité d'une attaque par force brute est une fonction exponentielle de la longueur du mot de passe, la rendant en principe impossible pour des mots de passe de longueur moyenne. En pratique, des optimisations peuvent donner des résultats dans des délais beaucoup plus courts.

Cette méthode est souvent combinée avec l'attaque par dictionnaire et par table arc-en-ciel pour trouver le secret plus rapidement. Elle peut être combinée avec de l'ingénierie sociale qui consiste à récupérer des informations d'un individu et de les inclure dans des listes.

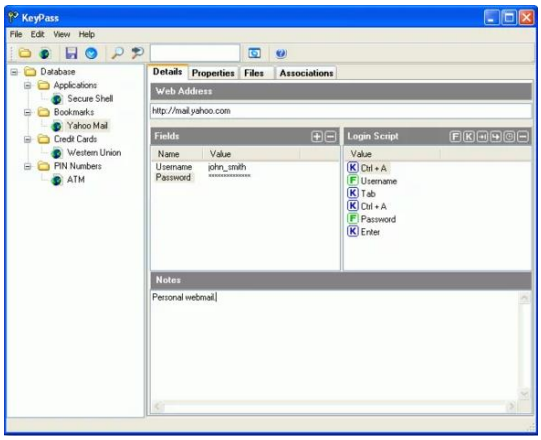


c. Sécuriser ses mots de passe

Depuis plusieurs années, la multiplication des applications et services digitaux nous amènent à la création de nouveaux mots de passe régulièrement.

Le comportement humain et le manque d'outils nous amène à créer de nouveaux mots de passe qui peuvent se ressembler, avec des caractères dont on se souvient facilement. Toutefois nous savons que pour des enjeux de simplicité, nous augmentons les chances d'attaques avec cette pratique.

Pour bien faire, nous vous conseillons d'utiliser un logiciel de gestion de mot de passe, qui servira de « coffre à clés » numérique. Il permet de stocker vos mots de passe de manière chiffrée l'ensemble de vos mots de passe et il est accessible via un seul mot de passe.



Ici le lien pour télécharger l'application :

https://keepassxc.org/

3. Piratage de la boite mail

La boite mail pour les pirates est considérée comme un vecteur d'attaque de masse. Il permet de réaliser des opérations de piratage sur une grande quantité de cibles en investissant peu de moyens. Mais les opérations de hacking peuvent, tout autant, cibler un individu unique.

Le piratage de boîte mail est une prise de contrôle par un autre individu, ayant des fins malveillantes. Il est possible d'être victime de piratage de nombreuses manières : un mot de passe facile à deviner, être la cible d'une campagne de phishing ou encore d'un virus, entre autres.
Chacune de ces situations peut mettre en évidence une usurpation d'identité. Dans ce cas, l'accès à d'autres services risque également d'être compromis.

a. Comment savoir si votre boîte mail a été piratée ?

Il existe un moyen très simple et efficace de vérifier si votre adresse (et mot de passe) de boîte mail a été piratée : le site Web "have i been pwned?" .

Voici comment en quelques étapes :

- Allez sur le site https://haveibeenpwned.com/.
- Entrez l'adresse email ou le numéro de téléphone que vous souhaitez vérifier à l'endroit indiqué.
- Cliquez sur la droite sur pwned ?
- Découvrez le résultat : en vert, vous avez de la chance, cet identifiant ne figure pas dans les listes du site. En rouge, attention, votre adresse ou numéro de téléphone figure dans une fuite de données.

Pour exemple : l'adresse mail que j'utilise depuis plus de 15 ans a été piratée dans 6 brèches de sécurité et est maintenant disponible dans des bases de données sur le DarkWeb que des hackers achètent pour mener leurs attaques.
Ceci ne m'empêche pas de l'utiliser mais je reçois régulièrement des mails frauduleux ce qui m'oblige à une attention particulière.

b. Quelques bonnes pratiques avec la boite mail

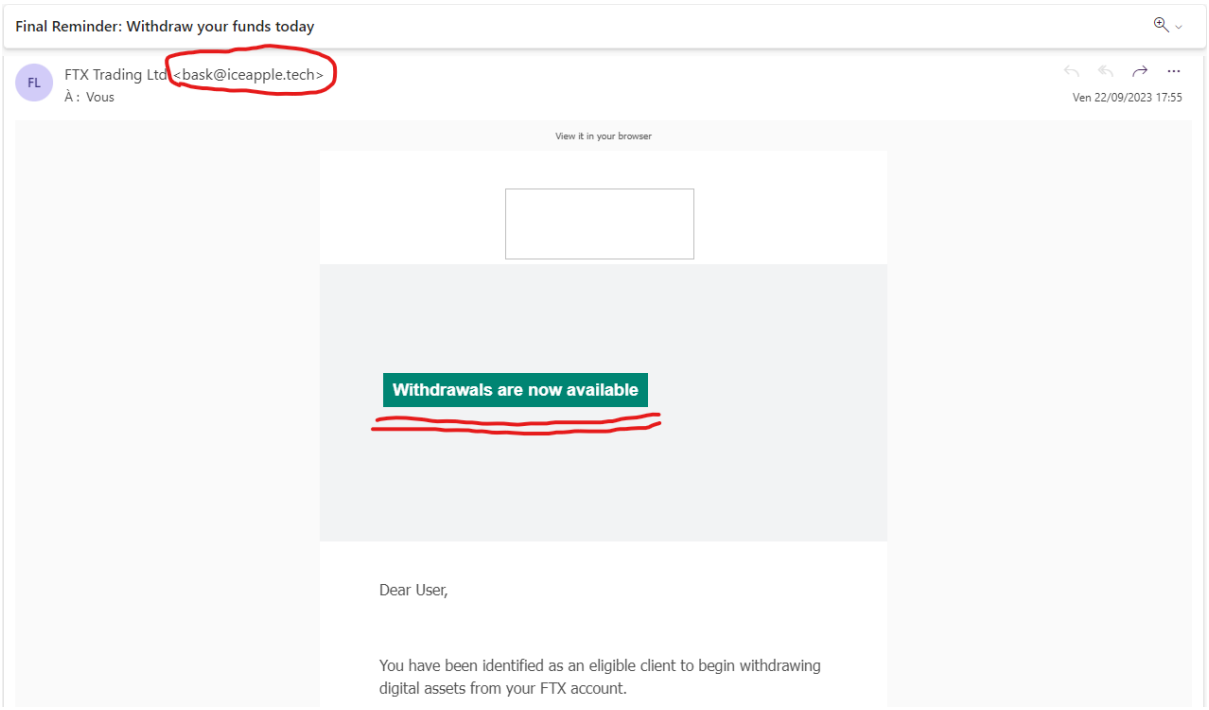
La boite mail est régulièrement l'objet d'attaque de type hameçonnage (phishing en anglais) qui est une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe…) et/ou bancaires en se faisant passer pour un tiers de confiance.

Vous devez, comme moi, recevoir des mails de publicité, des mails avec des pièces jointes de type photo ou document PDF. Ces campagnes sont de plus en plus sophistiquées et souvent en phase avec l'actualité.

Pour exemple, j'étais en possession d'un compte FTX pour les cryptoactifs. Depuis 2022, l'entreprise est sous le contrôle de la juridiction américaine en attente du procès. Il y a quelques semaines j'ai rempli un document via le site en ligne du liquidateur pour m'identifier en tant qu'ancien client et tenter de récupérer mes avoirs.

Depuis cet enregistrement auprès du liquidateur, je reçois des mails suspects reprenant le même format et m'invitant à communiquer des informations supplémentaires.

Soyez vigilants sur les informations que vous communiquez et a qui vous les envoyez !



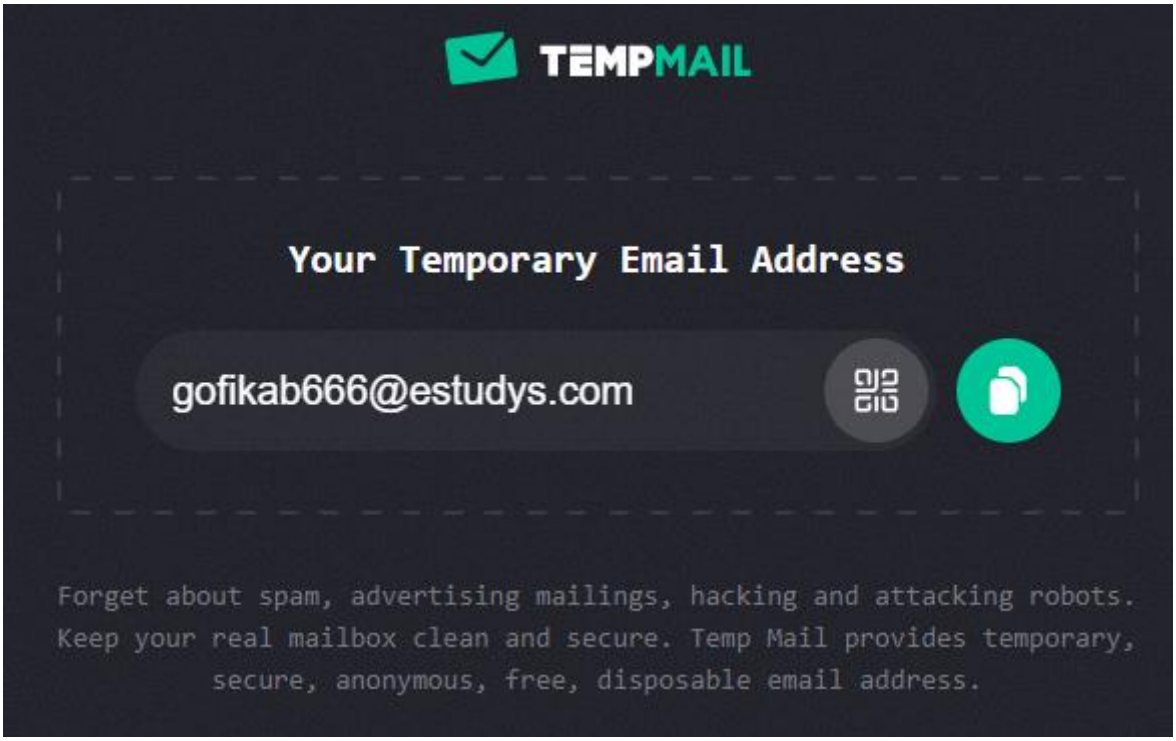
Les bonnes pratiques :

- Vérifier toujours l'expéditeur (pas le nom mais l'adresse mail)
- Soyez attentif au niveau de langage du courriel
- Soyez attentif au format du mail, les hackers reproduisent des mails légitimes mais laissent parfois des signes de modifications
- Vérifiez les liens dans le courriel (passez votre souris sur le lien, puis en bas à gauche ou à droite de votre écran vous verrez l'adresse URL du lien)
- Interrogez-vous sur la légitimité des demandes qui vous sont faites
- L'adresse de messagerie source n'est pas un critère fiable car les hackers sophistiqués pourraient simuler des adresses mail légitimes.

Adoptez une attitude sceptique lorsque vous utilisez votre boite mail. Partez du principe que les informations qui arrivent dans votre boites mail ont été envoyées par un pirate, ce dernier va vous inciter à cliquer sur des éléments du mail qui vous semblent parfaitement légitime et habituel.

Enfin dans certains cas de navigation, il vous est demandé de fournir une adresse mail pour recevoir une documentation ou bien vous souhaitez télécharger une version démo d'un logiciel ou tout autre cas.
Votre mail communiqué, ne vous sera demandé qu'une fois généralement puis en validant avoir reçu le mail, vous aurez accès au service. Dans ce type de cas, vous pouvez utiliser **une adresse mail éphémère**.

Voici un petit outil simple pour réduire votre surface d'attaque : https://temp-mail.org/en/



4. Navigation sur internet

Internet repose sur des protocoles de communication, sur lesquels de nombreuses entreprises ont créé leurs services digitaux par le biais de site web ou d'applications. Ces applications nécessitent souvent de créer votre espace personnel sur leurs plateformes.

Ainsi vous communiquez dans la majorité des cas :

- Votre adresse mail
- Votre adresse postale
- Date de naissance
- Numéro de téléphone
- Numéros de carte bancaire

Les entreprises du numérique conservent vos informations sur leurs serveurs et sont responsables de la sécurisation des données de leurs clients.
De plus, toute votre activité sur internet est tracée, récoltée par le biais des métadonnées ou des cookies qui donnent des informations sur votre personne ou sur votre comportement.

Une attitude simple à adopter lorsque vous naviguez est de tenter de laisser le moins de traces, mais ce n'est pas évident.

a. Reduire votre empreinte numérique

Utiliser un VPN, Virtual Private Network ou réseau virtuel privé.

Ce type de logiciel vous permet d'empêcher un tiers de faire le lien entre votre adresse IP et votre activité sur internet. Un VPN va agir comme une passerelle vers Internet, camouflant l'adresse IP de l'utilisateur.

Même dans le confort de vos quatre murs, l'utilisation d'un VPN pour votre activité Internet habituelle n'est pas une mauvaise idée. En général, cela vous empêchera de laisser des traces sur Internet qui pourraient être espionnées par votre fournisseur d'accès internet (FAI) ou par les entreprises pour cibler vos préférences et revendre vos informations personnelles. Bien que vous n'ayez certainement rien à vous reprocher, c'est juste une solution pour gérer au mieux votre vie privée.

Ici, vous pourrez aller plus loin sur le sujet : https://www.journaldugeek.com/vpn/

Limiter la quantité de logiciels installés sur vos appareils.

La plupart des logiciels communiquent par les ports réseaux (canaux qui se multiplient et augmentent la surface d'attaque possible). De plus certains logiciels peuvent être installés lors de l'installation d'autres logiciels. Pensez à nettoyer votre ordinateur ou téléphone de temps à autres.

Sur Windows : paramètres -> applications -> désinstaller les applications inutiles
Sur téléphone : paramètres -> applications -> désinstaller les applications inutiles

Limiter les services des navigateurs internet

Les navigateurs Internet ont bien évolué ces dernières années pour vous permettre une navigation toujours plus fluide. Pour ce faire, ils enregistrent vos informations des sites tiers pour que vous puissiez automatiser la réouverture de votre compte lors d'une nouvelle session.

Chrome, Brave, Firefox, Edge sont les principaux. Soyez vigilent, ils vous proposent d'enregistrer les identifiants et mots de passe des applications web, vos informations bancaires.

Bien que ces services rendent la navigation bien plus agréable, les bonnes pratiques vous recommanderons de renoncer à la facilité et de désactiver ou décliner à chaque proposition d'enregistrement.

Sur Navigateur Chrome :
Paramètres -> confidentialité et sécurité -> effacer les données de navigation
Paramètres -> saisie des mots de passe -> gestionnaire de mot de passe

b. Les réseaux wifi privés

Votre box internet permet de vous connecter à internet en filaire ou par le biais du réseau wifi.
Les fournisseur classique (Orange, Bouygues, SFR, …) proposent des mécanismes de sécurité par défaut qui sont aux normes, pas d'inquiétudes fortes de ce côté. Toutefois, il faut veiller à vérifier :

- Utiliser WPA ou WPA2 et éviter WEP ou sans chiffrement (sans mot de passe)
- Modifier le mot de passe par défaut de votre réseau wifi car ces informations sont connues des pirates
- Désactiver le WPS (option qui permet de se connecter au wifi en cliquant sur le bouton de la box)

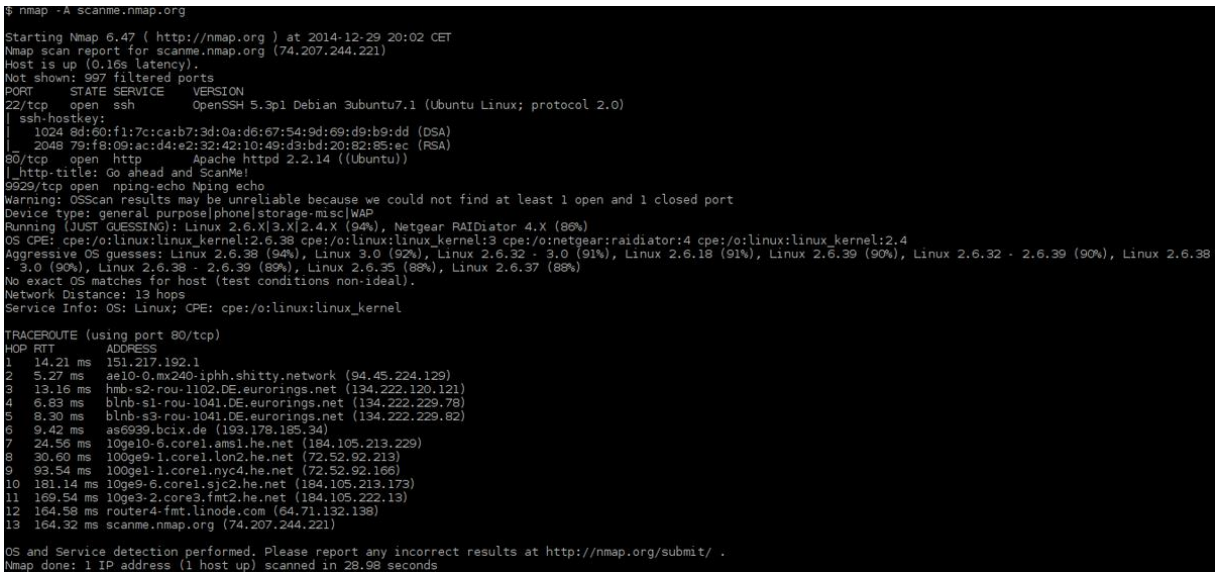
c. Les réseaux wifi nomades

Les wifi Nomade ou réseau publiques sont ceux auxquels vous pouvez vous connecter lors de vos déplacements : avion, train, café, bibliothèque, hôtel, aéroport, séminaires.

Peu de personnes le font mais l'idéal est d'utiliser un VPN, car sur un réseau publique, toutes les connexions et les échanges d'informations sont visibles (sauf les connexions chiffrées de type HTTPS).

Si vous êtes dans un séminaire dont le thème est la finance, un hacker sera intéressé à pirater vos informations en vue de vous voler.

Un logiciel comme https://nmap.org/ permet de scanner les activités d'un réseau.



d. Les logiciels espions

Les Spyware sont des petits programmes qui peuvent être installés sur votre poste lorsque vous cliquer sur un document d'un mail frauduleux. Une fois infecté, l'attaquant peut récupérer certaines informations on fonction des capacités du logiciel.

Pour exemple :
Lorsque vous vous connectez à votre service bancaire en ligne, il vous demande de cliquer à la souris sur un clavier numérique et vous ne pouvez pas taper au clavier par exemple,
C'est un mécanisme de sécurité qui vise à se prémunir des Keylogger (type de spyware) qui permet d'enregistrer les frappes au clavier. Ainsi l'attaquant aurait la possibilité de lier votre code (tapé au clavier) à votre activité en cours, navigation sur le site de la banque Société Général.

Le hacker peut ainsi :
Identifier les frappes du clavier : Roger.durand5@gmail.com ….. Theresse2909$
Et lier au site web actuellement visité : https://particuliers.sg.fr/

CONCLUSION

Le proverbe dit : « Mieux vaut prévenir que guérir. » Nous pouvons dire que dans le domaine informatique, prévenir est impératif, parce que guérir est impossible et de toute façon ne sert à rien.

Lorsqu'un accident ou un pirate a volé ou détruit les données il n'y a pas ou peu de recours tout simplement.

La sécurité ne doit pas être perçue comme une contrainte car elle donne de la cohérence à la gestion et permet d'adopter vis-à-vis des risques et menaces une attitude préventive et proactive, et pas seulement réactive.

Une attitude simple à adopter : moins vous êtes visible sur internet moins vous vous exposez aux attaques.

C'est comme dans la vie, n'attirez pas les envieux avec votre image numérique.
Les hackers vont rechercher les proies faciles, il ne faut pas faire partie de ceux qui laisse leur porte ouverte.