Guide des bonnes pratiques de confidentialité et de sécurité en informatique

LARGO CATALÃO

Table des matières

Introduction

Ce manuel a pour objectif de sensibiliser le lecteur à la cybersécurité et lui fournir l'ensemble des outils nécessaires. Il n'a en aucun cas vocation à imposer les pratiques présentées dans ce guide mais à conseiller les utilisateurs novices. Il est nécessaire que chacun se face sa propre idée et ses propres critiques concernant chacune des solutions présentées. Certains aspects de ce document peuvent être perçus comme radicaux ou extrêmes mais ils sont basés sur des faits démontrés par des organismes ou entités compétentes et reconnues.

Toutes les informations et données présentées dans ce document sont basées sur des connaissances personnelles ou tirées de ressources disponibles en fin de document dans la partie Bibliographie. Je vous laisse également quelques liens intéressant dans la partie Annexe.

Si vous observez des erreurs dans le document ou des informations pertinentes à ajouter vous pouvez me contacter par mail à largo.9fh0k@simplelogin.fr.

Vous pouvez retrouver la dernière version de ce document à l'adresse suivante : https://largo.web-edu.fr

1. Anonymat et confidentialité

Les notions d'anonymat et de confidentialité sont des notions que beaucoup de gens confondent.

1.1. Anonymat

L'anonymat consiste à être anonyme, c'est-à-dire de ne pas pouvoir identifier une personne.

NB : le mode navigation privé dans un navigateur ne vous rend pas anonyme, son seul atout est de ne pas stocker l'historique des recherches et supprime l'ensemble des cookies à sa sortie. Cependant, il est tout de même possible de consulter l'historique de la navigation privé via la commande ipconfig/displaydns, et le supprimer via la commande ipconfig/flushdns dans l'invite de commande Windows.

1.2. Confidentialité

La confidentialité est le fait de ne pas divulguer ses informations personnelles. Cela englobe toute donnée permettant l'identification d'un individu.

« Cela permet notamment d'éviter une possible usurpation d'identité. »

Cependant, certaines entreprises souhaitent garder les données de leurs utilisateurs et vont ainsi anonymiser les données comme le prévoit le RGPD[1] (en Europe). Leurs noms, prénoms, dates de naissance, adresse postale, IP et e-mail sont retirés de la fiche clients. Ainsi, les entreprises peuvent par la suite vendre et acheter ces bases de données. Dans les faits, cet anonymat n'est pas garanti malgré les mesures prises, il a été démontré dans une étude[2] qu'en recroisant 15 bases de données différentes, on obtenait le profil des personnes concernées dans près de 99,98 % des cas.

Lorsqu'on navigue sur internet, nous nous rendons sur des sites ou allons sur les réseaux sociaux. Sans le savoir nous donnons quotidiennement un grand nombre d'informations sur nous telle que notre localisation. D'après une étude de l'Irish Council for Civil Liberties datant de mai 2022, nous donnons involontairement 376 fois par jour une information à une entreprise : des informations personnelles sur nous, soit 1 fois toutes les 15s sur une journée de 24h.

Je mets également à disposition en fin de document des liens vers la CNIL française pour se renseigner sur vos droits concernant vos données personnelles.

---

1 Le Règlement Général sur la Protection des Données est entré en application le 25 mai 2018.
Il harmonise les règles et les pratiques européennes, applicables en matière de protection des données à caractère personnel. Il concerne les entités publiques ou privées, établies dans l'UE ou touchant des personnes dans l'UE. Lesntreprises de toutes tailles, administrations et collectivités qui traitent des données à caractère personnel sont concernées.

2 Étude réalisée par des chercheurs de l'Université catholique de Louvain et l'Imperial College de Londres https://www.nature.com/articles/s41467-019-10933-3

2. Naviguer sur Internet

Lorsqu'on est petit et que l'on commence à utiliser internet on nous dit souvent qu'internet est dangereux, qu'il faut faire attention, qu'il ne faut pas cliquer sur n'importe quoi. Pourtant, plus on grandit et que l'on est habitué à utiliser nos ordinateurs, et aller sur internet, moins on fait attention. Il suffit parfois d'un clic sur un lien figurant sur un mail qui semblerait être de la part d'un organisme officiel et vous voilà victime d'une cyber attaque. Vous pouvez vous en rendre compte et avoir votre PC qui ralenti ou qui « plante » mais cela peut être bien plus discret avec un virus qui reste sur votre PC sans que vous le sachiez mais qui récolte tout ce que vous tapez sur votre clavier.

L'empreinte numérique d'une personne est composée de centaines d'éléments tels que la taille de son écran, le modèle de machine utilisé, le système d'exploitation, quels sites visite-t-il régulièrement, quels réseaux sociaux utilise-t-il, etc.

2.1. Les cookies et traqueurs tiers

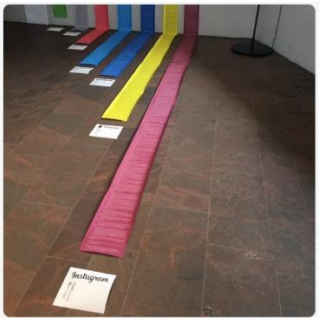
Lorsque nous naviguons au quotidien sur Internet, nous laissons derrière nous nos habitudes d'utilisations, les sites que l'on visite, le nom de notre banque, le fait qu'on cherche une voiture, que l'on va partir en vacances, etc. Ces informations sont transmises aux sites que l'on consulte par des traqueurs (trackers) ou encore lorsqu'on accepte la politique de confidentialité du site en question. En acceptant, nous autorisons le site à collecter toutes les sortes de données nous concernant et à déposer des cookies permettant ainsi de nous retrouver lorsque nous consultons un autre site. Ce qui forme ce qu'on appelle l'empreinte numérique.

Source : citroen.fr

C'est pourquoi, grâce au RGPD les sites qui récoltent et revendent des informations sur leurs internautes sont tenus d'avoir leur consentement et nous sommes libres de refuser ou d'accepter la récolte de nos données (partiellement ou totalement). Cependant, tous les cookies ne sont pas néfastes, certains servent au bon visionnage de la page Web ou d'autre à l'enregistrement de vos informations de connexions afin que vous n'ayez pas à vous reconnecter constamment.

2.2. Conditions Générales d'Utilisation

Alors que seulement 7% des Français affirment lire les CGU, Dima Yarovinsky un étudiant en design a décidé d'imprimer en format A4 les CGU des sites les plus connu (de gauche à droite), Whatsapp, Google, Tinder, Twitter, Facebook, Snapchat et Instagram :



De son coté, une juriste Britannique, Jenny Afia a publié en 2017 une vulgarisation des CGU du réseaux social américain Instagram (traduites par Bisness Insider) :

1. Tu as le droit de te sentir en sécurité quand tu utilises Instagram.

2. Officiellement, tu es propriétaire des photos et vidéos que tu postes, mais nous avons le droit de les utiliser, et de laisser d'autres personnes les utiliser, partout dans le monde. Les gens nous paient pour les utiliser, et nous ne te paierons pas.

3. Tu es responsable de tout ce que tu fais sur Instagram et de tout ce que tu postes.

4. On considère que ce tu postes t'appartient, et ce que tu postes ne doit pas enfreindre la loi. Si c'est le cas, tu auras une amende, et tu devras payer cette amende.

5. Même si tu es responsable des informations que tu mets sur Instagram, nous pouvons les garder, les utiliser et les partager avec des entreprises connectées à Instagram. Cela inclut ton nom, ton adresse mail, ton école, où tu vis, tes photos, ton numéro de téléphone, tes "likes" et "dislikes", où tu vas, où tes amis vont, combien de fois tu utilises Instagram dans la journée, ta date d'anniversaire, à qui tu parles ainsi que tes messages privés.

6. Nous ne sommes pas responsables de ce que font les autres entreprises avec tes informations. Nous ne vendrons ou ne louerons pas tes infos personnelles à d'autres entreprises sans ta permission.

7. Quand tu supprimes ton compte, nous gardons ces informations personnelles sur toi, tes photos, aussi longtemps que raisonnable dans un but financier. Tu peux en savoir plus sur notre politique de vie privée.

8. Instagram n'est pas non plus responsable de :
Les liens sur Instagram d'autres entreprises ou les personnes qu'on ne contrôle pas, même si c'est nous qui t'envoyons ces liens.
Ce qu'il peut se passer si tu connectes ton compte Instagram à une autre appli ou un site. Par exemple, si tu partages une photo et que l'autre application prend tes informations personnelles.
Le coût de la 3G quand tu utilises Instagram.
Si tes photos sont perdues ou volées sur Instagram.

9. Même si Instagram n'est pas responsable de ce qu'il t'arrive quand tu utilises l'appli, nous avons beaucoup de pouvoirs :
On peut t'envoyer des pubs ciblées en fonction de tes intérêts, que l'on surveille. Tu ne peux pas nous empêcher de le faire, et ce ne sera pas toujours précisé dans la pub.
Nous pouvons modifier ou supprimer ton Instagram, ou t'empêcher d'accéder à l'appli, quand on veut, sans que tu sois prévenu. On peut aussi supprimer certains de tes posts sans te dire pourquoi. Si nous le faisons, nous ne te devrons pas d'argent, et tu n'auras pas le droit de te plaindre.
On peut t'obliger à abandonner ton nom d'utilisateur, pour n'importe quelle raison.

Nous pouvons – mais ne sommes pas obligés – supprimer ou modifier des contenus d'utilisateurs qui enfreignent les règles. Nous ne sommes pas responsables si quelqu'un les enfreint, mais si tu le fais, tu es responsable.

11. Même si tes données ne t'appartiennent pas, les nôtres nous appartiennent. Tu ne peux pas copier-coller les logos d'Instagram ou les autres contenus qu'on crée, ni les modifier, ni les supprimer.

12. Tu peux supprimer ton compte en remplissant ce formulaire. Si tu le fais, tes photos disparaîtront de ton profil mais si quelqu'un d'autre les a partagées, elles apparaîtront encore peut-être sur Instagram.

13. Nous pouvons modifier ces règles quand on veut en postant une mise à jour sur Instagram, que tu l'aies remarqué ou non.

A la lecture de ces règles, cela fait froid dans le dos et dites-vous que vous avez surement accepté ces règles sans même savoir de quoi il s'agissait. Il est important de sensibiliser les enfants dès leur premier contact à internet aux risques qu'ils encourent et comment s'en prémunir. Il est important de noté que près de 76 % des 12-17 ans utilisent les réseaux sociaux.

2.3. Navigateur et moteur de recherche

Afin de limiter au maximum la collecte de nos données, nous pouvons utiliser des navigateurs et moteurs de recherche plus respectueux de la vie privée.

Sur ordinateur :

- Mozilla Firefox (recommandé)
- Brave (basé sur Chrome)
- Tor Browser (Pages lentes à charger du fait de son fonctionnement)

Couplé d'un moteur de recherche

- DuckDuckGo (recommandé)
- StartPage (made in Europe)
- Qwant (made in France)

Il est recommandé de mettre des extensions (addons) sur son navigateur afin de préserver sa confidentialité. En effet, lorsqu'on réalise une recherche via Duck, la recherche est réalisée dans le respect de notre vie privée, mais dès lors que l'on clique sur un site nous ne sommes plus protégés, ainsi, voici une liste non-exhaustive d'extensions (Je conseille d'en mettre plusieurs, leurs effets sont cumulatifs.) :

- uBlock Origin (bloque les traqueurs de site web / RECOMMANDER)
- DuckDuckGo Privacy Essentials (bloque les traqueurs de site web)
- Malwarebytes Browser Guard (bloque les traqueurs de site web + rôle d'un antivirus)
- Facebook Container (bloque les boutons Facebook)

Sur téléphone :

- DuckDuckGo
- Qwant
- Mozilla Firefox + DuckDuckGo/Qwant

Certains moteurs de recherche tels que DuckDuckGo ou Qwant existent en navigateur. On peut également choisir Mozilla Firefox, couplé du moteur de recherche DuckDuckGo et permettre la synchronisation des pages Web entre son ordinateur et son téléphone. DuckDuckGo propose également en version bêta un anti-traqueur d'application. Lorsqu'on réalise une recherche sur le net, Duck est en mesure de bloquer les traqueurs, alors

que lorsqu'il s'agit d'application telle que Amazon, celles-ci envoient directement les informations à son serveur. Mais avec la nouvelle fonctionnalité de DuckDuckGo App Tracking Protection, Duck créé un proxy au sein de votre smartphone, contraignant l'ensemble des applications à faire transiter leurs données par celui-ci. Ainsi, un minimum de données statistiques ou commerciales sont envoyées par les applications. A noter qu'une récente polémique touche le navigateur à la suite d'un contrat passé avec Microsoft, cependant, cela n'affecterait que le blocage des traqueurs Microsoft et non la confidentialité des recherches.

En cas de doute concernant un bouton lien, passez votre souris au-dessus (sans cliquer) et le lien s'affichera en bas à gauche de votre navigateur ou de votre boite mail. Sur smartphone un appuie long sur celui-ci permet de visualiser le lien et de le copier ou de l'ouvrir.

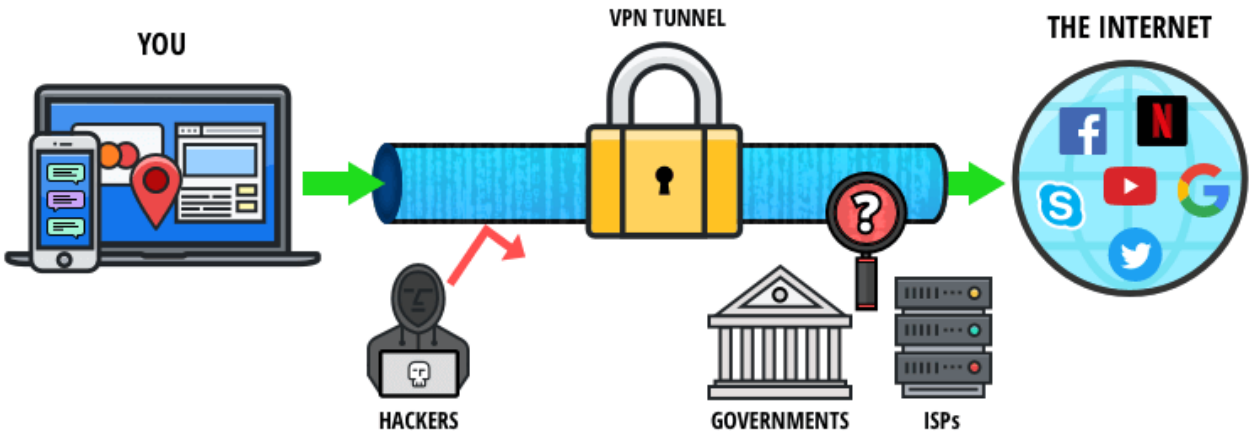
Afin de vous rendre compte à quel point une page web peut détecter et collecter ce que vous faites, je vous recommande de vous rendre sur le site : https://clickclickclick.click/

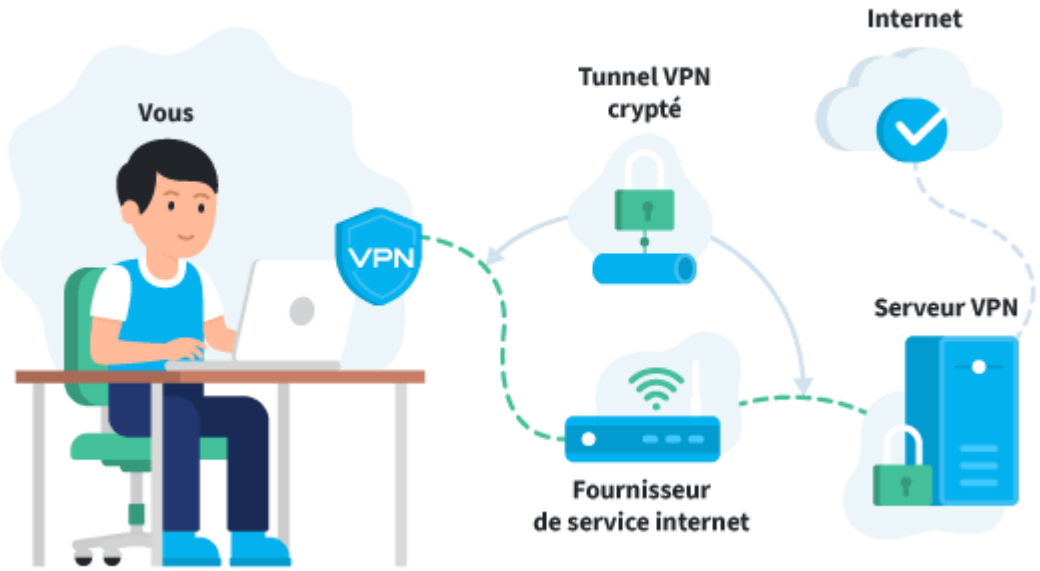
Quel que soit le navigateur que vous utilisez, il est important de vérifier les paramètres de celui-ci, voici une liste non exhaustive de points que vous devriez vérifier :

- Effacer l'historique de navigation ou de téléchargement régulièrement
- Refuser la géolocalisation par défaut
- Supprimer les cookies à la sortie du navigateur
- Effacer les données de saisie automatique
- Effacer les mots de passe enregistrés
- Demander à ne pas être pisté par les sites web
- Interdire le téléchargement automatique et demander une confirmation à chaque fois
- Installer des outils de protection de la confidentialité (extensions)

2.4. Qu'en est-il des VPN ?

Nombreux sont ceux qui ont souscrit à un VPN (Virtual Private Network = Réseau Virtuel Privé) afin de sécuriser leur connexion sur internet et de masquer leur adresse IP. Avant de mettre en avant ou critiquer cette technologie, revenons-en au fonctionnement même de ce qu'est un VPN.





Lorsque l'on navigue sur internet, nous sollicitons notre fournisseur internet afin d'accéder au site que nous souhaitons consulter. Alors que lorsqu'on utilise un VPN, celui-ci va chiffrer votre connexion et réaliser la recherche à notre place, ainsi le site que vous consultez connaîtra l'adresse IP du server VPN mais pas le vôtre. La majorité des utilisateurs de VPN en ont un dans le seul but de pouvoir accéder à du contenu en streaming disponible uniquement dans un pays étranger ou encore payer un jeu en ligne 10X moins chère en se localisant dans un autre pays où le coût de la vie est moindre. D'autres personnes les utilisent afin de contourner la censure du pays dans lequel ils résident et avoir une plus grande liberté sur internet, comme tout simplement pouvoir visionner le dessin animé Winnie l'ourson en Chine (article de L'Express).

Initialement, les VPN étaient dédiés au monde professionnel et avaient pour seul objectif de permettre aux salariés d'une entreprise de se connecter de manière sécurisée à leurs serveurs internes lors de leurs déplacements. Depuis quelques années nous sommes envahis par des publicités en tout genre vantant les mérites des VPN et affirmant que nous avons tous besoins d'en avoir un sinon notre vie privé en serait impactée. Les plus présents sur le marché tels que NordVPN, Surfshark ou encore ExpressVPN (scandale ExpressVPN / en anglais) pour ne citer qu'eux, sont relayés sur les réseaux, sur Youtube et dans des blogs à coup de : « Top 10 des meilleurs VPN en XXXX ». Mais dans les faits, si l'on regarde d'un peu plus près : Souscrire à ce service c'est accepter que l'ensemble de vos données internet transitent par un serveur unique détenu par une entreprise pouvant être contrainte par les gouvernements (Cloud Act par LesEchos) de fournir les informations vous concernant. Malgré leurs promesses de ne pas conserver votre IP, vous n'avez aucun moyen de vérifier cela. De plus, s'il est gratuit c'est accepter d'être vous-même le produit et ainsi de fournir une quantité d'information personnelles leurs permettant de les vendre et de rentabiliser votre utilisation à leur service. De plus, le chiffrement militaire dont se targue ces services pour chiffrer votre connexion n'est autre que le chiffrement http**s**.

Je vous laisse visionner la courte vidéo (10 min) réalisée par Micode et qui explique très bien l'utilité d'un VPN.

Si malgré cela, vous souhaitez tout de même souscrire à un VPN, je vous conseille d'en prendre un respectueux de la vie privée et se trouvant en Europe :

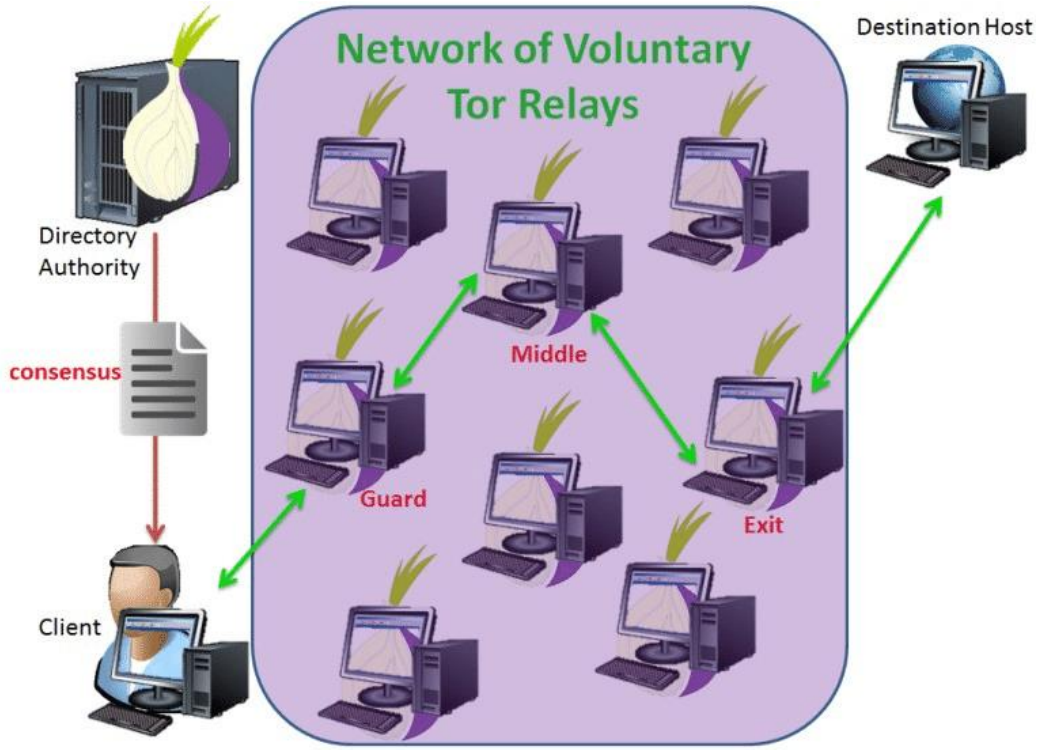
- ProtonVPN (sous la juridiction suisse / juridiction qui garantit l'anonymisation des connexions VPN et interdit la levé de cette protection quelle que soit la demande / ne fait pas partie des quatorze yeux)
- CyberGhost (Européen)

Pas en Europe mais recommandé dans cet article par DuckDuckGo (article relatant les points importants à vérifier avant d'utiliser un VPN) :

- TorGuard (rien à voir avec le réseau Tor)

Si vous avez besoin d'une anonymisation maximale de votre trafic internet, la meilleur solution est surement TorBrowser. Il réalise la même chose qu'un VPN (hormis qu'il soit plus lent) mais va augmenter la sécurité en masquant l'IP du client en passant par plusieurs serveurs.

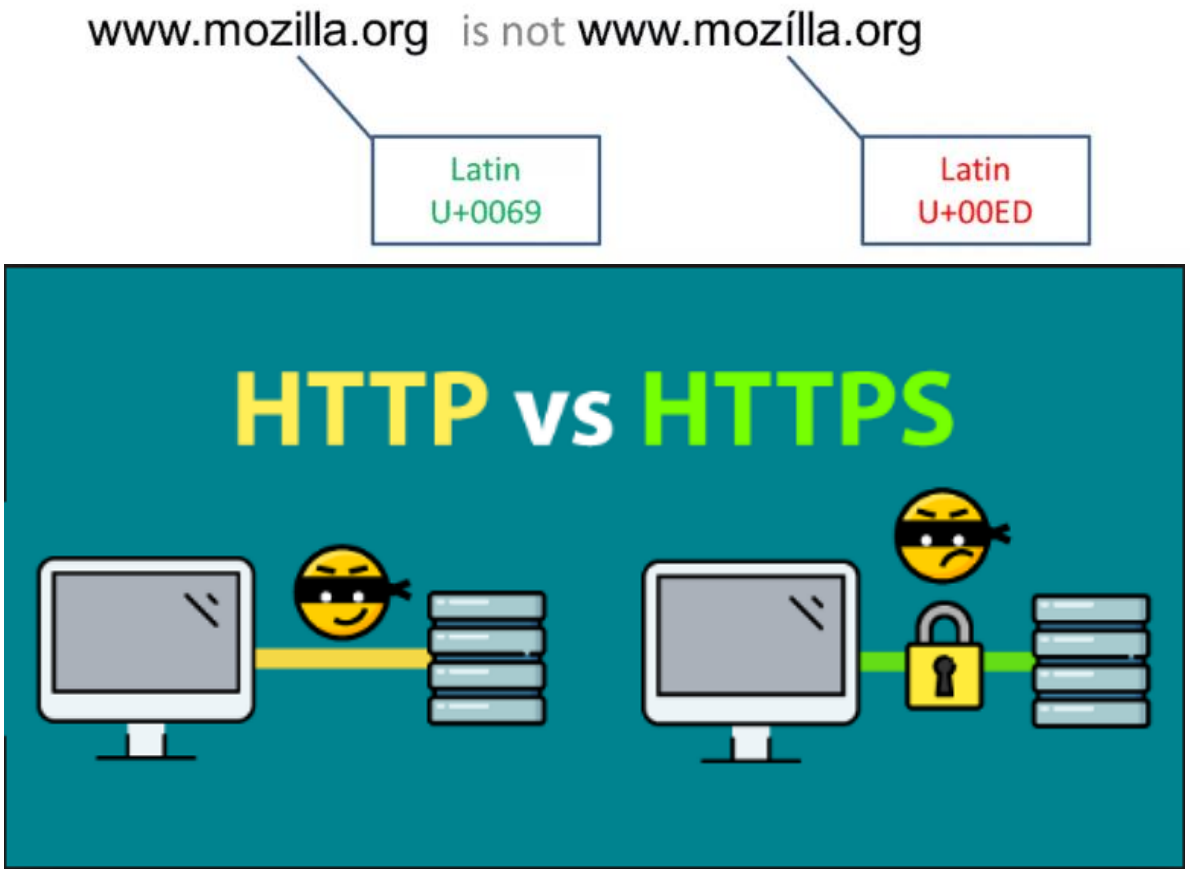
Comparateur VPN VS Tor	VPN	TOR
Vitesse		
Compatibilité avec tous les appareils		
Partage de fichier en P2P		
Anonymité maximale		
Protège toutes les connexions		
Prix		
Facilité à configurer		
Accès à un SAV		



2.5. Ingénierie sociale

Malgré tous les différents systèmes mis en place et quelle que soit la solidité de votre mot de passe ou la mise en place de la double authentification, les hackers parviennent encore à passer outre. C'est pourquoi il est nécessaire de faire attention à 3 points.

1. Les courriels que l'on reçoit sur notre boîte de réception sont peut-être des tentatives de phishings, il faut donc s'assurer que l'expéditeur est fiable (au caractère près).
2. L'adresse url d'un site web peut nous mettre en danger, il faut donc vérifier l'exactitude de celle-ci, ainsi que s'assurer que nous sommes bien en HTTP**S** :



Source : www.datarain.com

3. Ne jamais divulguer son mot de passe : les administrateurs ou sites auxquels on se connecte n'ont pas besoin de notre mot de passe pour « vérifier notre identité », faire des « contrôles » ou toute autre demande, ils possèdent leurs propres accès administrateurs ne nécessitant pas de vous solliciter.

3. Niveau de sécurité

Lorsqu'on se connecte sur une plateforme, un site ou une application, nous utilisons généralement le même couple : identifiant/mot de passe. Malheureusement, ils ne sont pas toujours suffisants et il est nécessaire d'ajouter une authentification à double étape (2FA/2 Factory Authentication). Parmi les différents moyens qui existent, nous avons (du moins fiable au plus fiable) l'authentification :

- par SMS, par notification depuis une application reconnu,
- par OTP (One Time Password),
- par une carte à puce ou encore par clé « physique ».

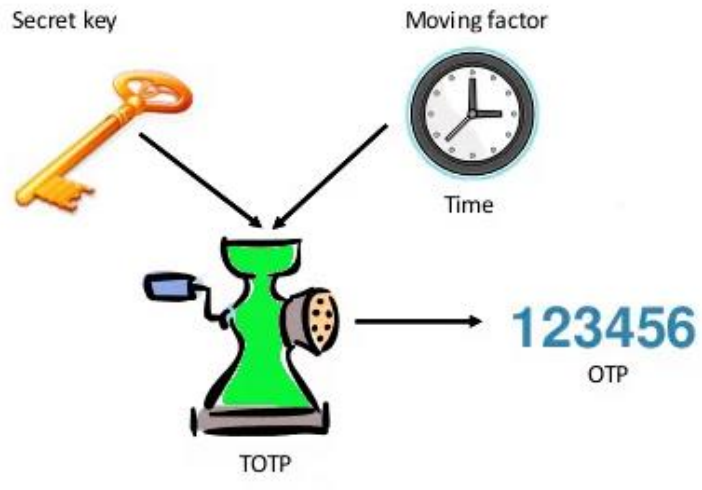
Source : www.expert-com.com

Ces moyens permettent de confirmer votre identité par un code aléatoire généralement composé de 6 chiffres.

En fonction de la méthode de double authentification, il est plus ou moins fastidieux de s'authentifier. Les méthodes lourdes et agaçantes n'incitent pas à sécuriser ses comptes, car se connecter à un compte devient fastidieux. Mais l'authentification par SMS est la plus régulièrement contournée par les hackers. C'est pourquoi, je vous conseille deux méthodes de double authentification : par TOTP ou par clé physique.

3.1. TOTP – Time-based One Time Password

Le TOTP-2FA est basé sur la génération d'un code à 6 chiffres. On l'obtient par la combinaison d'un facteur temps et d'une clé secrète.

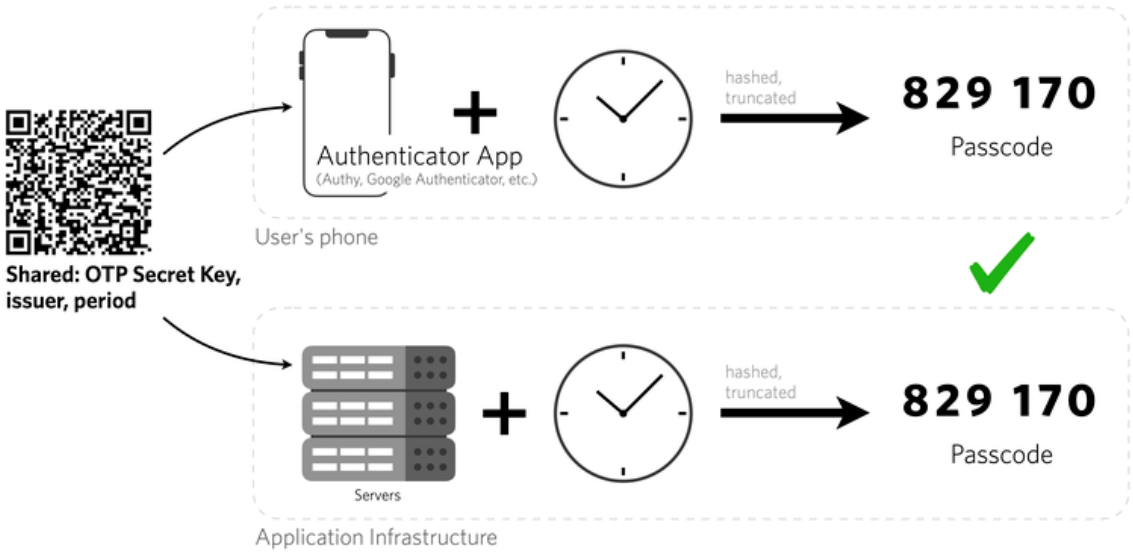


Source : www.protectimus.com

Il existe différentes applications sur le marché permettant de sauvegarder ces TOTP :

- Google authentificateur (la plus connu / clé sauvegardée sur l'appareil / sans paramétrage compliqué)
- DUO
- Bitwarden (Avec l'offre payante)
- Yubikey (Nécessite l'achat d'une Yubikey de chez Yubico)

Lorsqu'on rentre ce code lors de la connexion, celui-ci est comparé au code que le serveur à générer.



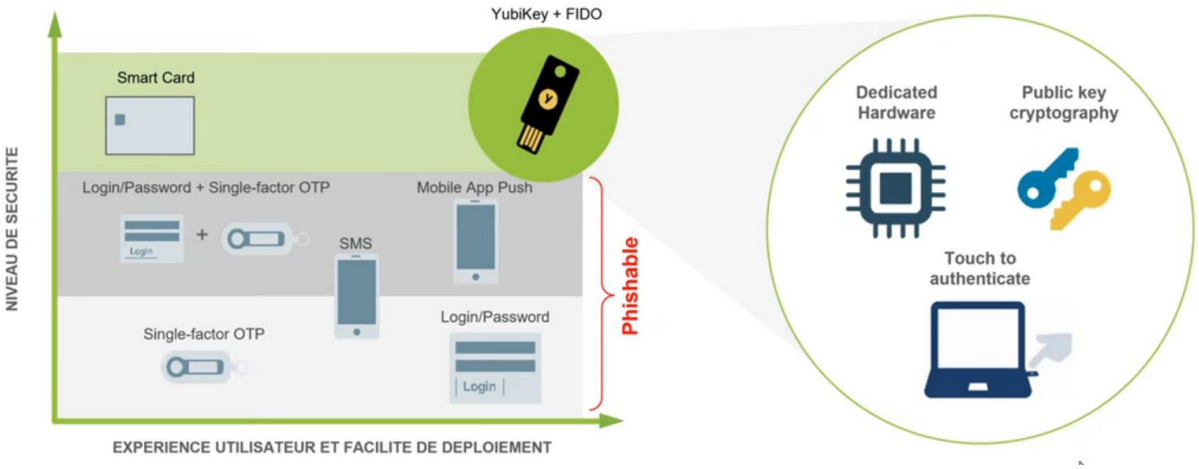
Source : www.twilio.com

3.2. Clé physique

Les clés physiques restent le moyen de double authentification les plus rapide et les plus sûrs. En effet, composé d'un jeton, elles assurent que la personne souhaitant se connecter possède la clé physique et que la TOTP n'a pas été piraté (Hack de Google Authentification). Ces clés sont résistantes pour la plupart à la poussière, à l'eau, à la casse ainsi qu'aux tentatives de piratage.

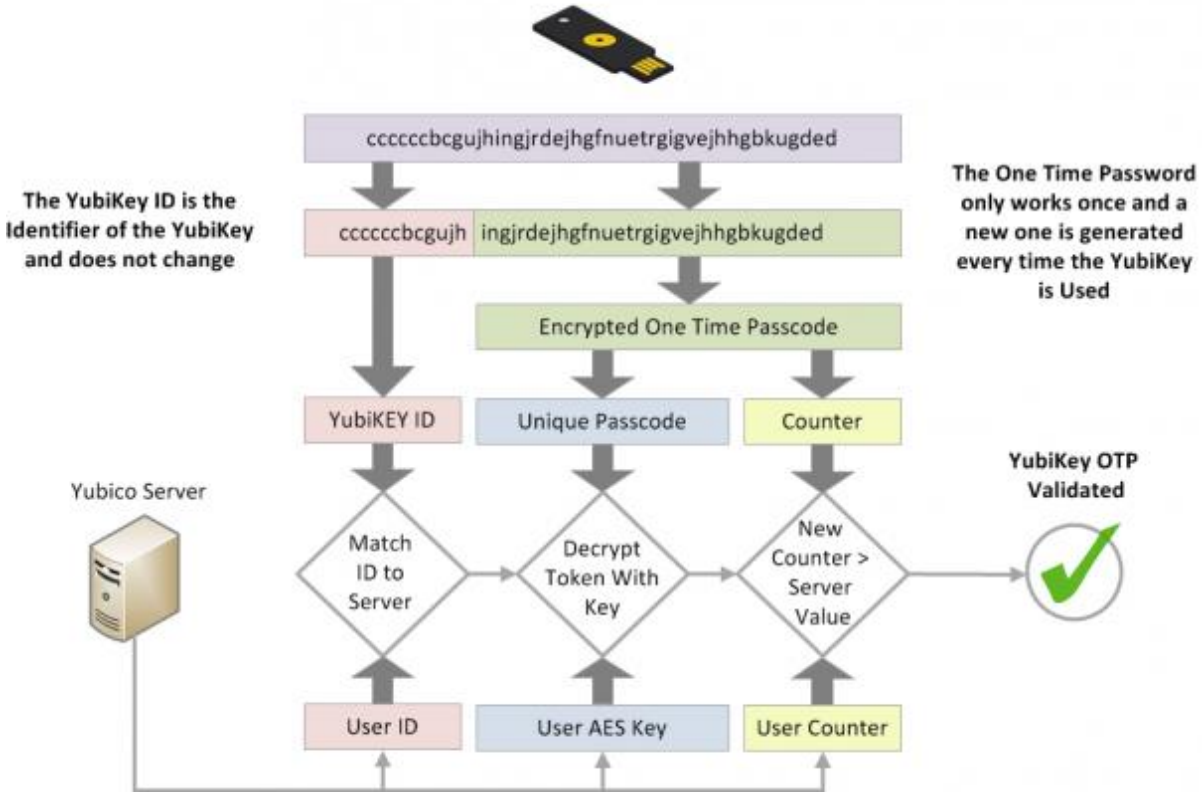
Voici une liste des clés physiques reconnues :

- Yubikey (marque historique avec une expérience dans le domaine inégalée, offre un large panel de clés en fonction de son utilisation et propose un quiz pour la choisir la plus adaptée à vos besoins)
- Google Titan (a subi des failles critiques après sa sortie en 2020)
- Kensington VeryMark (utilisation limitée et basée sur un petit lecteur d'empreinte digitale donc plus facilement contournable)



Source : www.yubico.com

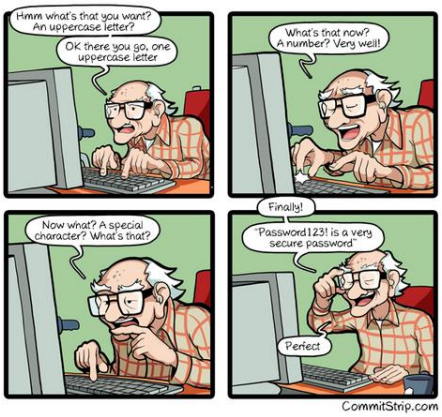
Fonctionnement d'une Yubikey :



Source : www.yubico.com

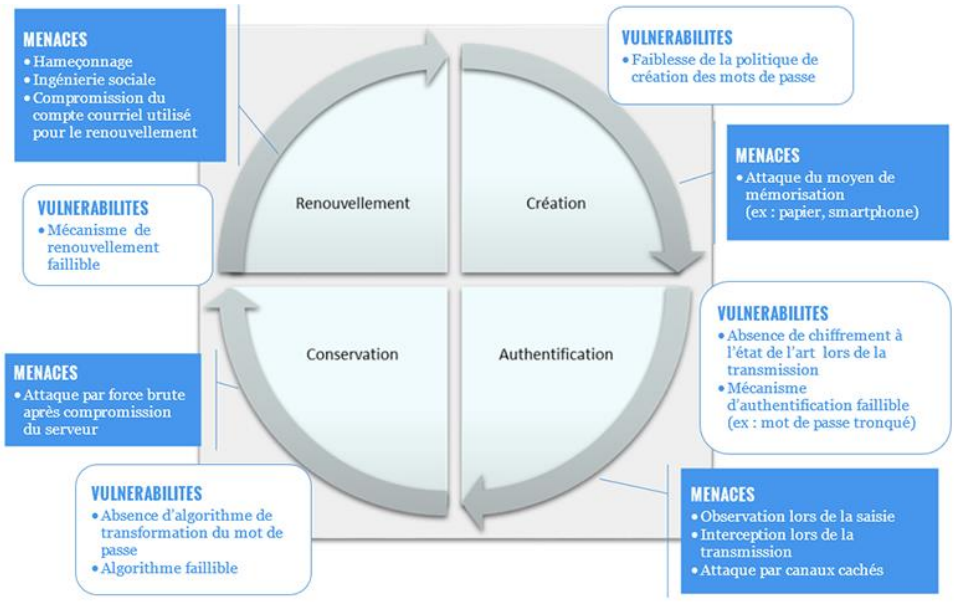
4. Gestionnaires de mot de passe

La plupart des gens utilisent un seul mot de passe pour tous leurs comptes avec une variante pour chaque site



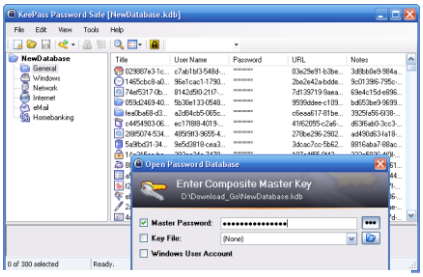
en se disant que c'est suffisamment sécurisé comme ça. Malheureusement, la réalité est toute autre, la règle n°1 est de ne jamais utiliser le même mot de passe pour plusieurs comptes ou ayant un lien avec nous. La seconde est de créer un mot de passe fort, soit d'une longueur de 18 caractères (J'applique personnellement une taille minimale de 25 caractères.) ou plus, mais comprenant des MAJUSCULES, des minuscules, des n0m8re5 et des c@ractè®es spé©iau⊗. Il ne faut pas oublier que si un hacker accède à un de vos comptes, il peut accéder à vos données personnelles, telles que votre adresse postale, e-mail (l'identifiant du site peut ne pas être votre adresse électronique, mais un pseudo), votre date de naissance, votre IP, votre numéro de téléphone, vos préférences (site de rencontre), etc. De nombreux sites proposent de vérifier localement (donc rien n'est transmis à leurs serveurs) la solidité d'un mot de passe (site gouvernemental français ou Kaspersky).

Je vous invite à consulter cette page de la CNIL (*Commission Nationale de l'Informatique et des Libertés*) dédiée au mot de passe ou celui-ci (toujours de la CNIL) pour créer un mot de passe.



Source : www.ssi.gouv.fr

Afin de sauvegarder ses mots de passe tous différents et in-mémorisable, voici une liste non-exhaustive de gestionnaires de mot de passe reconnus :

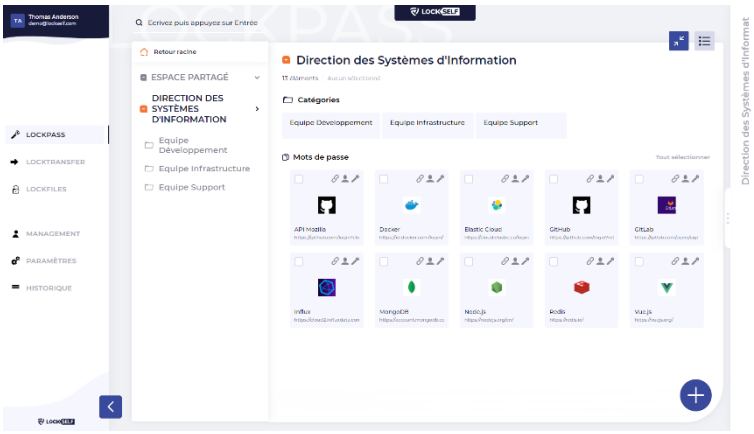


Source : www.blogdumoderateur.com

KeePass, le gestionnaire de mot de passe le plus reconnu, Open Source, mis à jour régulièrement, gratuit et validé par l'ANSSI (agence nationale de la sécurité des systèmes d'information) il vous permet de stocker vos mots de passe en toute sécurité sur votre ordinateur dans un fichier chiffré.

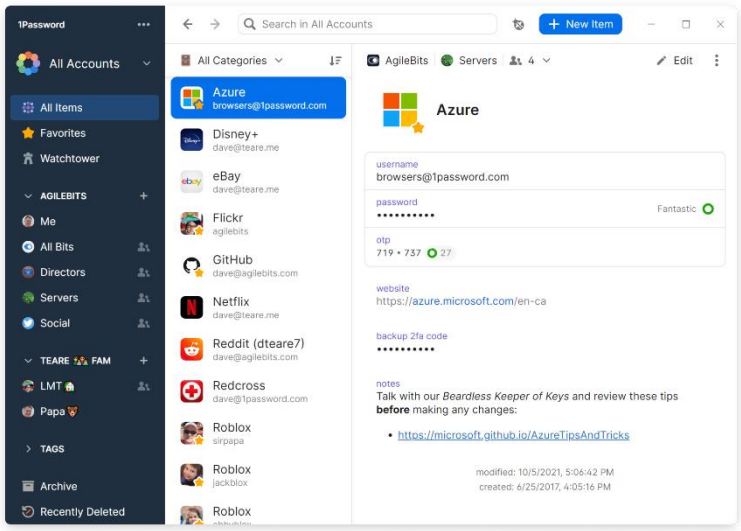
ATTENTION : le site officiel est https://keepass.info et non ~~keepass.fr~~

LockSafe, un gestionnaire de mot made in France, validé par l'ANSSI, mais payant et davantage destiné aux entreprises.



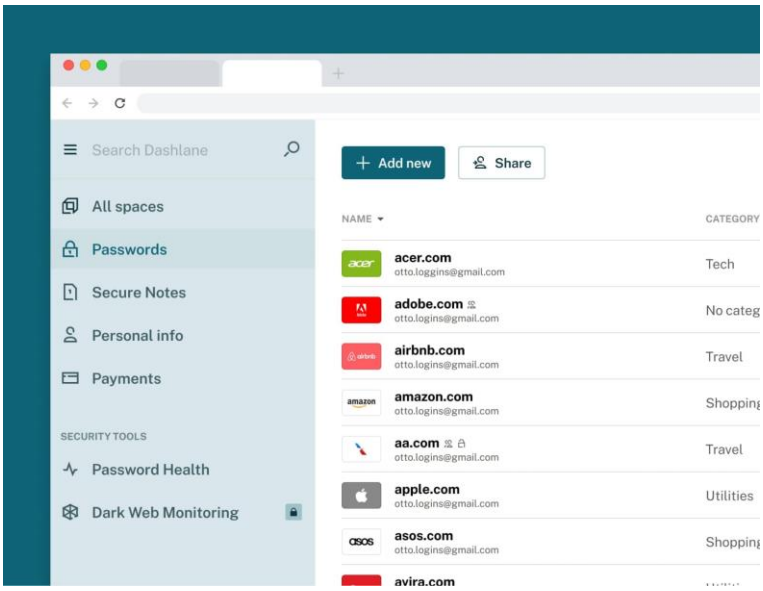
Source : catalogue.numerique.gouv.fr

OnePassword, ce gestionnaire de mot de passe payant offre une large gamme d'option.



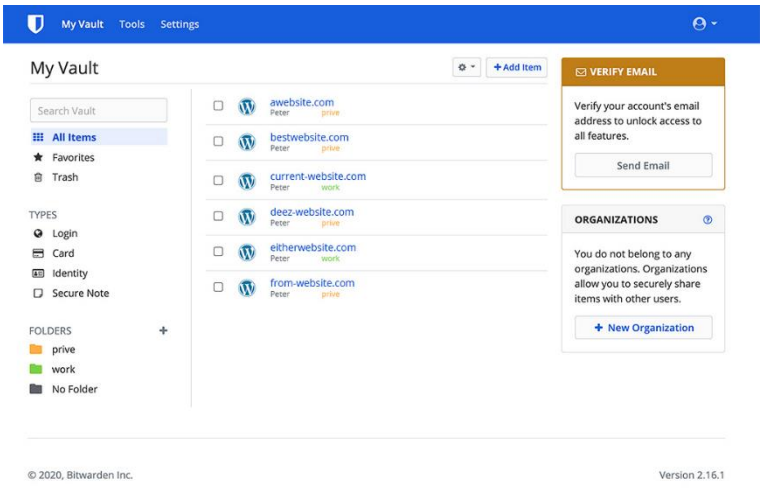
Source : 1password.com

Dashlane, ce gestionnaire de mot de passe possède une offre gratuite mais limitée à 50 mots de passe et sur 1 appareil.



Source : www.dashlane.com

Bitwarden est Open Source et offre quant à lui la possibilité de stocker ses mots de passe, notes et informations personnelles sur un cloud crypté sur le principe du cryptage zéro accès (vous seul détenez le mot de passe de votre coffre). Ce qui vous permet d'accéder à votre coffre où que vous soyez. Son offre gratuite pour particulier vous permet d'avoir le strict minimum attendu sans le moindre coût avec la possibilité d'utiliser l'application sur iOS/Android, l'extension sur navigateur (Chrome/Mozilla Firefox/Brave/Opéra, etc.), l'application bureau sur votre OS préféré (MacOs, Windows, Linux) ou sur le web. Vous pouvez également partager vos mots de passe avec un autre membre de votre famille gratuitement en créant une organisation. Malheureusement, la fonction TOTP n'est pas disponible sur la version gratuite… Il sera donc nécessaire d'utiliser une autre application (voir précédente partie), vous pouvez tout de même y stocker les clés de vos TOTP dans l'espace dédié en cas de perte de vos TOTP sur l'autre application. (pour plus d'information et un article du cnet-tech). Outre le générateur de mot de passe intégré à Bitwarden, le service offre aussi la possibilité de générer un identifiant via votre compte SimpleLogin (voir plus loin dans le Guide)



Source : www.bitwarden.com

N'oubliez pas de configurer la **double authentification** pour votre gestionnaire de mot de passe et de mettre un **mot de passe fort** car c'est tout de même celui qui protégera tous vos mots de passe. Je conseille d'utiliser comme mot de passe maître **une grande phrase sans lien avec vous** ainsi, vous la retiendrez plus facilement. Également, puisque vous devrez constamment utiliser votre gestionnaire de mot de passe pour vous connecter à un site, enregistrez pour chacun des mots de passe forts (30 à 50 caractères), comme vous ne les mémorisez pas cela ne changera rien pour vous hormis **garantir la sécurité de vos comptes**.

Comparons-les (uniquement les offres Grand publique) :

OUI NON SANS DONNÉ	KeePass	OnePassword	Dashlane	Bitwarden
Offre gratuite*				
Offre payante				
Open Source				
Plus de 1 appareil			P	
Mac				
iPhone	N			
PC				
Android	N			
Linux				
Chrome OS				
Synchronisation entre les appareils				
2FA	E			P
Mot de passe illimité			P	
Extension sur navigateur				
Stockage de documents			P	P
Partage de document			P	
Partage de mot de passe				
Chiffrement 0 accè**				
Accè d'urgence***				P
FAQ				
SAV				

*les essai ne sont pas considérés comme des offres gratuites

**L'organisme ne peut pas avoir accès à votre coffre-fort

***Permet à une personne de confiance d'avoir accès au coffre-fort en cas de problème

N : Non officiel

E : Via l'ajout d'une extension (pas forcément officiel)

P : Uniquement offre payante

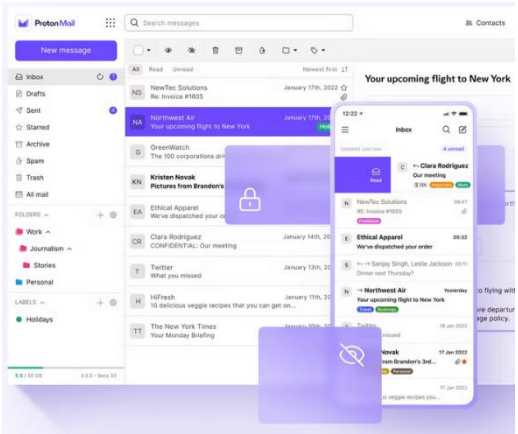
5. Boîte mail sécurisée

A présent, parlons de boîtes mail. Il existe différents services de messagerie plus ou moins connus et plus ou moins respectueux de la vie privée, tel que Gmail, Yahoo, Outlook et bien d'autres. Notre boîte mail renferme des informations des plus privées telles que nos résultats d'analyses médicales, nos rendez-vous médicaux, nos vacances organisées, etc. Il est donc primordial d'utiliser un service de messagerie qui ne lise pas, n'analyse pas ou ne collecte pas des données sur ce que l'on reçoit ou fait. Étant également le moyen de réinitialiser nos mots de passe sur les sites web ou applications que l'on utilise, la sécurité et la protection de celle-ci ne doit pas être oublié. Vous pouvez vérifier si votre mail n'a pas fuité suite à une cyber attaque via l'annexe à la fin du guide. Nous allons donc voir quels sont les services de messageries fiables.

Protonmail, leader dans les boîtes de réception sécurisées offre un cryptage de bout-en-bout à ses utilisateurs et un stockage de vos mails sur leurs serveurs avec une politique zéro accès. Open source, elle propose un écosystème comparable à Google. Son offre gratuite comprenant une messagerie, un agenda sécurisé, un VPN et un service Cloud vous permet de quitter Google pour un service plus respectueux de votre vie privé. De plus, Proton à mis en place une fonctionnalité sur sa version Web (pas encore dispo sur mobile) permettant de bloquer les traqueurs contenues dans les mails. En effet, selon une étude mené en 2017 (vulgarisation de l'étude) par Steven ENGLEHARDT, Jeffrey HAN, ET Arvind NARAYANA, près de 70% des e-mails reçu comportent un ou plusieurs traqueurs. Ces « mouchards » transmis dans les mails sous forme d'images ou images transparentes, permettent aux entreprises de collecter des données sur vous, telles que : votre IP, est-ce que vous avez ouvert le mail, l'heure à laquelle vous avez ouvert le mail, la machine utilisée (ordinateur, smartphone), votre système d'exploitation, la version de votre navigateur ou de votre application, etc.

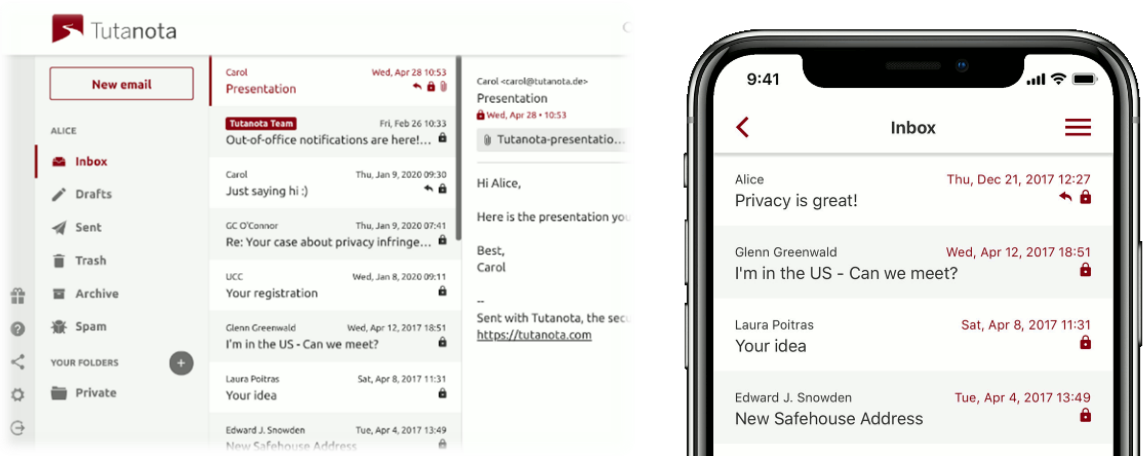
Cette start-up, suisse créée par des ingénieurs du CERN, répond aux normes de sécurité et de confidentialité européenne. Elle ne collecte aucune donnée, pas même votre IP (par défaut, mais elle peut être contrainte par les autorités suisses d'activer cette fonctionnalité d'enregistrement d'IP). Mais alors comment fait-elle pour financer tout cela ? Par des donations privées et par ses offres payantes pour les entreprises ou les particuliers. Engagée pour la protection de la vie privé pour tous, Proton défend devant les tribunaux suisses ses utilisateurs.

> *« Toutes les données utilisateurs sont protégées par la loi fédérale suisse sur la protection des données (LPD) et l'ordonnance relative à la loi fédérale suisse sur la protection des données (OLPD) qui offrent aux individus et aux sociétés l'une des plus fortes protections de la vie privée au monde. Comme ProtonMail est en dehors des juridictions des USA et de l'UE, seule une décision judiciaire du tribunal cantonal de Genève ou du tribunal fédéral suisse peut nous contraindre à divulguer les informations extrêmement limitées dont nous disposons sur les utilisateurs. 50 millions de personnes dans le monde ont souscrit à Proton pour sécuriser leurs informations » - Proton Technologie AG*



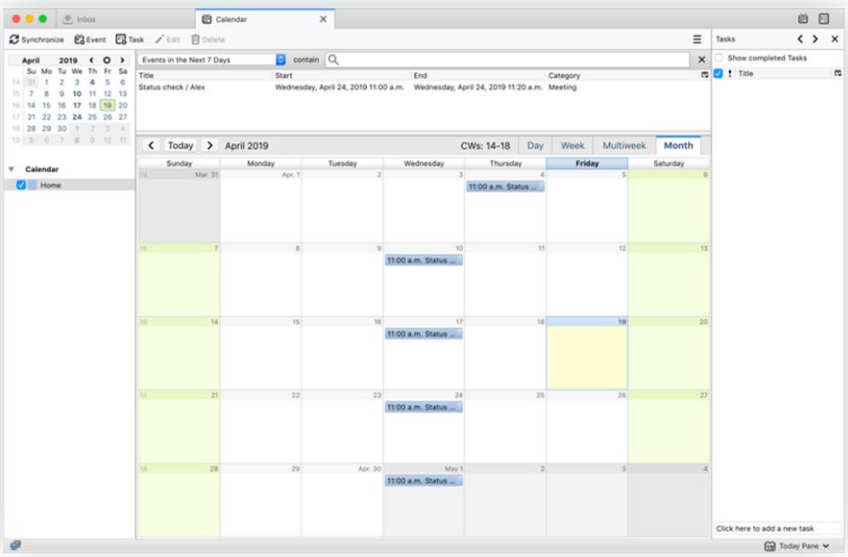
Source : www.protonmail.com

Tutanota est similaire à la précédente messagerie, celle-ci est basée en Allemagne et offre également un compte gratuit permettant d'avoir un calendrier et un boite mail sécurisé.



Source : tutanota.com

Thunderbird est une filiale de la Fondation Mozilla qui milite également pour la vie privée sur Internet. Malheureusement, il n'existe pas d'application mobile (en cours de développement) et ses fonctionnalités sont plus limitées.



Source : www.thunderbird.net

Lorsque vous vous rendez sur certains sites et qu'ils proposent de vous inscrire à leur news letters, DuckDuckGo Email Protection est surement la meilleure solution. Duck offre la possibilité à ses utilisateurs de se créer une adresse email @duck.com et renseigner une adresse mail de réception que vous utilisé. Une fois la création de l'adresse mail duck réalisé, vous pouvez à présent renseigner votre adresse mail duck sur les sites que vous fréquentez. Lorsque vous souhaité ajouté votre adresse duck à un site, s'il s'agît par exemple de s'abonner à une liste de mail vous pouvez générer une adresse duck aléatoire grâce à l'extension (addons ou extensions) sur votre navigateur mais tout de même recevoir les mails purgé de leurs traqueurs sur votre adresse de destination.

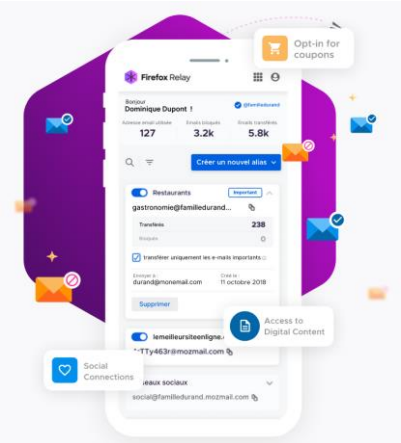
NB : Cette fonctionnalité est actuellement en version bêta est n'est disponible que sur liste d'attente en se rendant sur l'application mobile DuckDuckGo > Paramètre > Confidentialité > Protection des e-mails.

Source : DuckDuckGo

Mare de recevoir des spams sur votre boite mail ? Une start-up française du nom de SimpleLogin propose un service d'alias comme DuckDuckGo mais sans la suppression des traqueurs. Vous allez me dire mais quel est son avantage ? L'avantage de cette solution est qu'elle vous permet de générer 10 alias (offre gratuite). Je l'utilise personnellement lors de la création d'un compte sur un site web. Avec son extension de navigateur disponible sur Mozilla et Chrome, SimpleLogin permet de générer automatiquement d'un simple clic une adresse mail associée au site en question. Ainsi votre véritable adresse mail reste préservée des spams. Rien de mieux qu'une petite vidéo pour expliquer tout ça : lien vers la vidéo (en anglais mais sous-titrage disponible et tout est montré en image). N'oubliez pas qu'à la suite d'une fuite de données votre adresse mail peut se retrouver sur le darknet, en ayant des alias vous vous prémunissez de cela et pouvez en changer si besoin. Racheté en avril 2022 par Proton, SimpleLogin devrait potentiellement être intégré dans l'écosystème Proton afin d'envoyer plus facilement un mail avec un alias SimpleLogin. Il est déjà possible de se connecter à SimpleLogin via ses identifiant Proton. A noter que ce rachat ne limite pas SimpleLogin, il lui fournit du budget supplémentaire et reste indépendant, vous pouvez encore le combiner avec un autre service de messagerie que ProtonMail.

Source : SimpleLogin

D'autres alternatives existent telles que Firefox Relay qui offre quant à lui 5 alias gratuit et bloque les traqueurs contenue dans les mails. Il est important de noter qu'ils utilisent Amazon SES.



Source : Firefox Relay

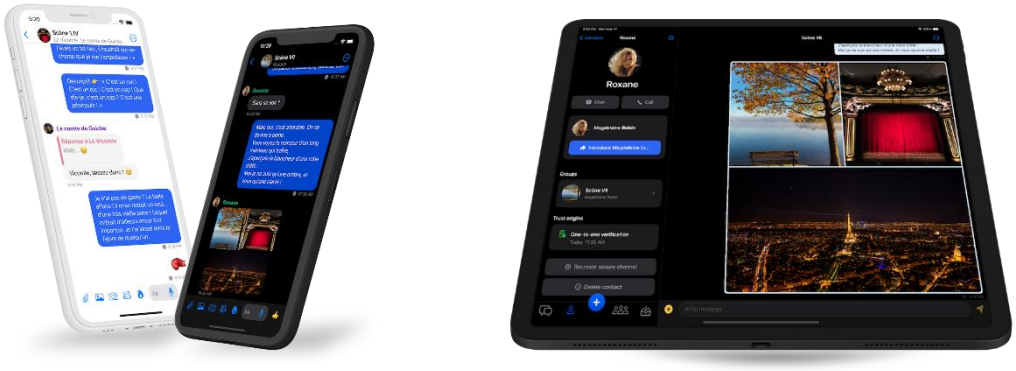
Ou encore Anonaddy qui offre une infinité d'alias mais malheureusement sans possibilité de répondre au mail avec la version gratuite.

6. Messagerie instantané et sécurisée

Au quotidien, nous n'utilisons pas notre boîte mail pour parler avec nos proches. Les sms ne sont pas sécurisés et pourtant, nous échangeons des données a priori anodines, mais pouvant être utilisées contre nous comme nos horaires de retour à la maison, nos rendez-vous médicaux, etc... C'est pourquoi, il est bien d'utiliser un service de messagerie qui crypte de bout en bout nos messages sans les analyser. Voici une liste de messageries sécurisées :

Olvid : français, validé par l'ANSSI (fonctionnalité d'appel uniquement sur version payante) et open source (certaines fonctionnalitées sont payantes mais les messages sont et resterons gratuits).

Olvid ne fonctionne pas comme Signal et WhatsApp avec un serveur centrale qui va agir comme tiers de confiance. Olvid est une messagerie à taille humaine ne nécessitant aucune validation par un tiers de confiance (serveur centrale) pour créer une discussion entre deux personnes. Le problème majeur du serveur centrale est qu'il va avoir comme rôle d'associer à votre numéro de téléphone votre clé publique de chiffrement pour que les personnes puissent interagir avec vous. Si ce serveur est corrompu, hack et qu'il vous fournit un « «coffre-fort » pour votre message qui possède une porte dérobé (back door) vous n'en saurez rien et votre conversation sera exposé. Olvid a réalisé une prouesse technique en supprimant ce serveur de confiance et en ne demandant aucun numéro de téléphone. Ainsi pour initier une discussion avec une personne vous aurez juste à scanner son QRCode d'application et vous échanger le codes qui s'affichent sur vos écrans (le tiers de confiance c'est vous et le coffre sécurisé pour envoyer un message à quelqu'un est sûre), cette procédure peut être réalisé en physique ou à l'aide d'un simple appel téléphonique.



Olvid est la première messagerie instantanée certifiée CSPN par l'ANSSI

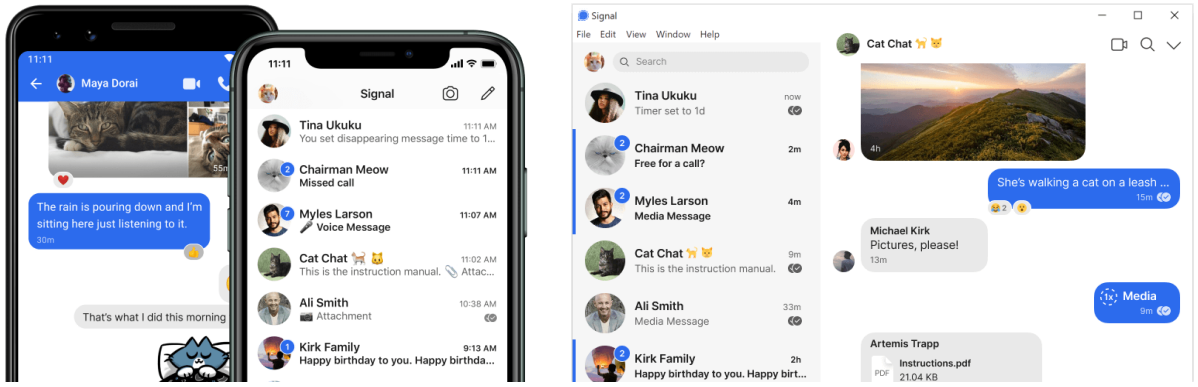
VISA DE SÉCURITÉ — AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION — ANSSI

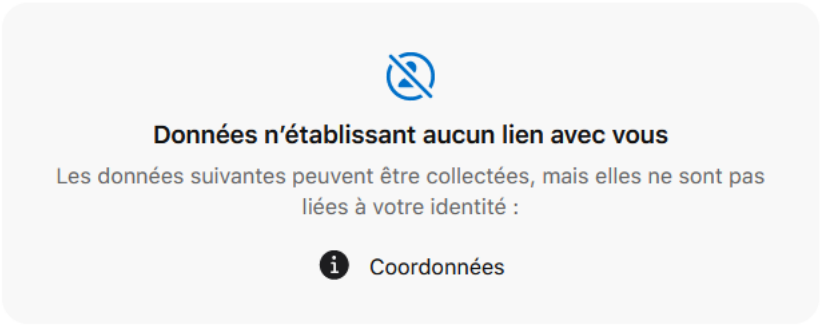
Données non collectées

Le développeur ne collecte aucune donnée avec cette app.

Source : Apple (informations saisie par le développeur de l'application)

Signal : gratuit et Open Source. Similaire à WhatsApp mais récupère moins d'information personnel.

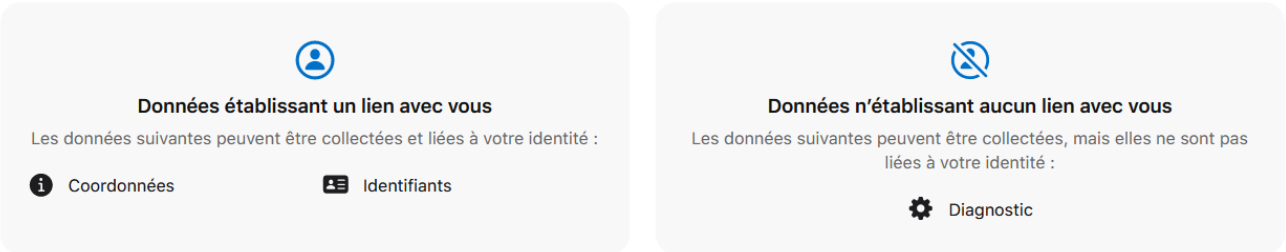




Source : Apple (informations saisie par le développeur de l'application)

Coordonnées : Numéro de téléphone

Threema : ne nécessite aucun contact pour s'inscrire, pas même un mail, un numéro de téléphone ou un compte rattaché. Achat unique de 3,99 € sur le store.



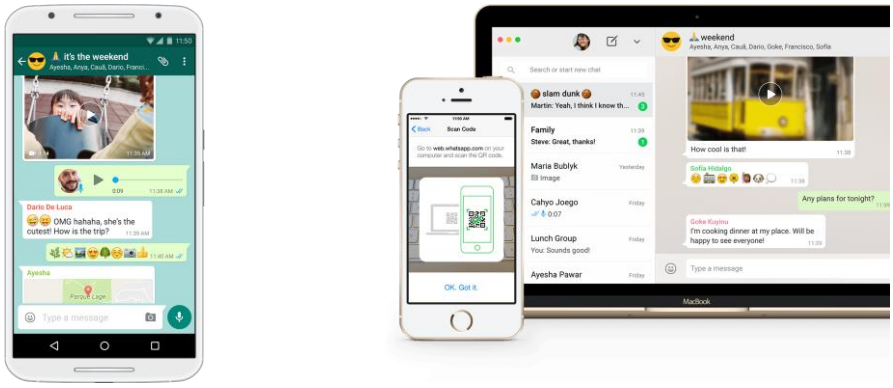
Source : Apple (informations saisie par le développeur de l'application)

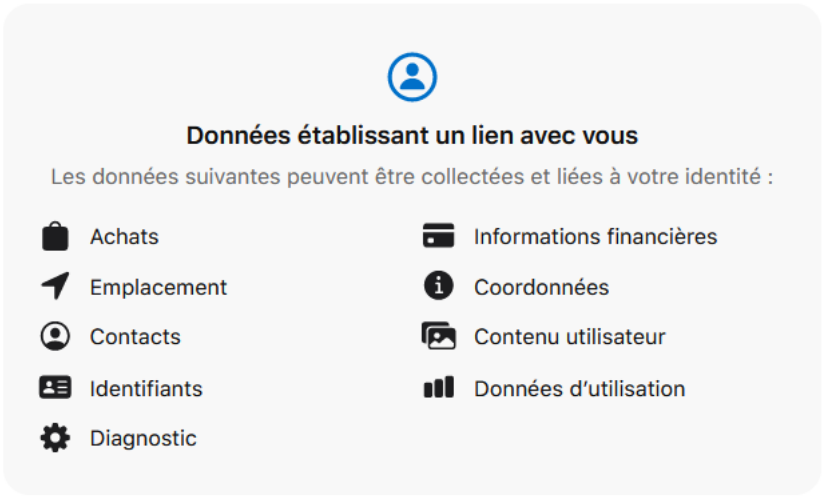
Coordonnées : Adresse e-mail et numéro de téléphone

Identifiants : Identifiant de l'utilisateur

Diagnostic : Données sur les pannes

Whatsapp : modèle commerciale intrusif et by META !s





Source : Apple (informations saisies par le développeur de l'application)

Identifiants : Identifiant de l'appareil et Identifiant de l'utilisateur

Données d'utilisation : Données publicitaires et Interaction avec le produit

Achats : Historique d'achats

Emplacement : Emplacement approximatif

Coordonnées : Numéro de téléphone et Adresse e-mail

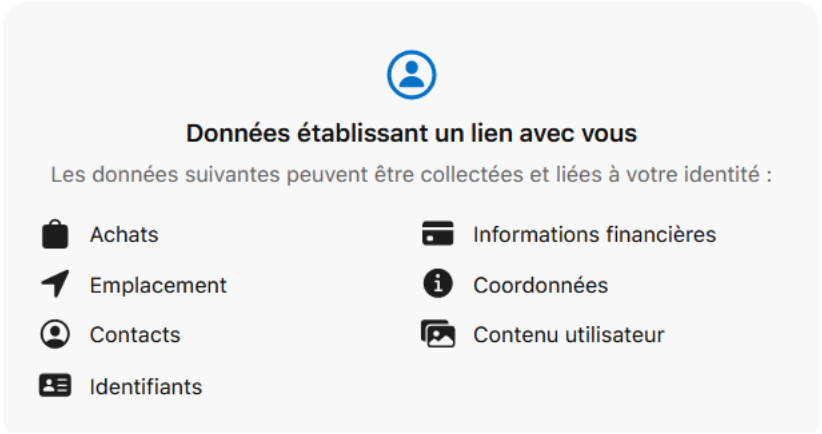
Contenu utilisateur : Assistance client et Autre contenu utilisateur

Diagnostic : Données sur les pannes, Données de performance et Autres données de diagnostic

Informations financières : Informations de paiement

Contacts : Contacts

Telegram : stocke par défaut de manière permanente les messages sur son serveur, ces messages peuvent être lus par le fournisseur de service et le chiffrement des conversations n'est pas activé par défaut (indisponible pour les groupes de conversations)



Source : Apple (informations saisies par le développeur de l'application)

Achats : Historique d'achats

Informations financières : Informations de paiement

Emplacement : Emplacement précis

Coordonnées : Nom et Numéro de téléphone

Contacts : Contacts

Contenu utilisateur : E-mails ou SMS, Photos ou vidéos, Données audio et Contenu des expériences de jeu

Identifiants : Identifiant de l'utilisateur

Comparons-les services de messagerie instantanées que nous venons de voir :

	Signal	Olvid	Whatsapp	Threema	Telegram
Offre gratuite	OUI	OUI	OUI	NON	OUI
Offre payante	NON	OUI	NON	OUI	OUI
Anonyme	NON	OUI	NON	OUI	NON
Cryptage de bout en bout	OUI	OUI	OUI	OUI	NON
Chiffrement incontournable	OUI	OUI	NON	OUI	NON
Server appartenant à l'organisme	NON	NON (la sécurité ne réside pas sur les serveur, tout sur pace sur les devices)	NON	OUI	NON
Non stockage des message sur les servers	OUI	OUI	NON	OUI	NON
Non utilisation des données des utilisateurs à des fins marketing	OUI	OUI	NON	OUI	OUI
Carnet d'adresse non nécessaire	OUI	OUI	OUI	OUI	NON
Conformité RGPD	NON	OUI	NON	OUI	NON
Vérification des contacts	OUI	OUI	OUI	OUI	NON
Open Source	OUI	OUI	NON	OUI	OUI
Juridiction	États-Unis	France	États-Unis	Suisse	
Message	OUI	OUI	OUI	OUI	OUI
Appel audio	OUI	P	OUI	OUI	OUI
Visio	OUI	P	OUI	OUI	OUI
iOS	OUI	OUI	OUI	OUI	OUI
Android	OUI	OUI	OUI	OUI	OUI
Web	OUI	Android uniquement / B iOS	OUI	OUI	OUI

SANS DONNÉE

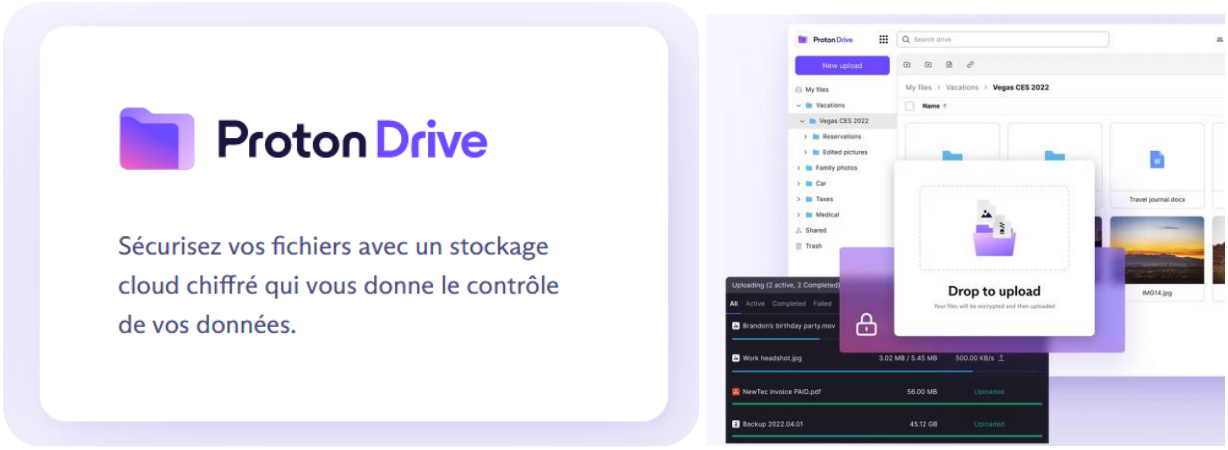
P : Uniquement via l'offre payante

B : Bientôt disponible

7. Cloud et stockage

Alors que les clés USB sont de moins en moins utilisées, nous nous tournons de plus en plus vers d'autres solutions sur lesquelles stocker nos photos de familles telle que, Google Drive. Il est en effet bien pratique de pouvoir accéder à tous ses documents sur tous ses appareils grâce à une simple connexion internet. Mais avez-vous réfléchis à qui pourrait avoir accès à votre « Drive » ? Êtes-vous réellement les seules à pouvoir y avoir accès en toute confidentialité ? Lorsque ce sont des photos d'anniversaire ou des travaux déjà rendu pour le travail cela vous importe peu qu'une autre personne puisse y avoir accès. Mais il est intéressant de pouvoir stocker numériquement nos papiers d'identité, les factures, les papiers de la banque ou encore ses ordonnances dans le cas où on ne sait jamais il y aurait une catastrophe naturelle ou un feu chez vous. La question de quel stockage utiliser devient tout de suite bien plus pertinente car personne ne voudrait voir sa CNI fuiter à droite ou à gauche sur internet. Ainsi, je vous propose dans cette section différentes solutions pour répondre à cette contrainte. Cependant, pour les fadas des clés USB je vous détaillerai comment sécuriser les données qu'elles contiennent.

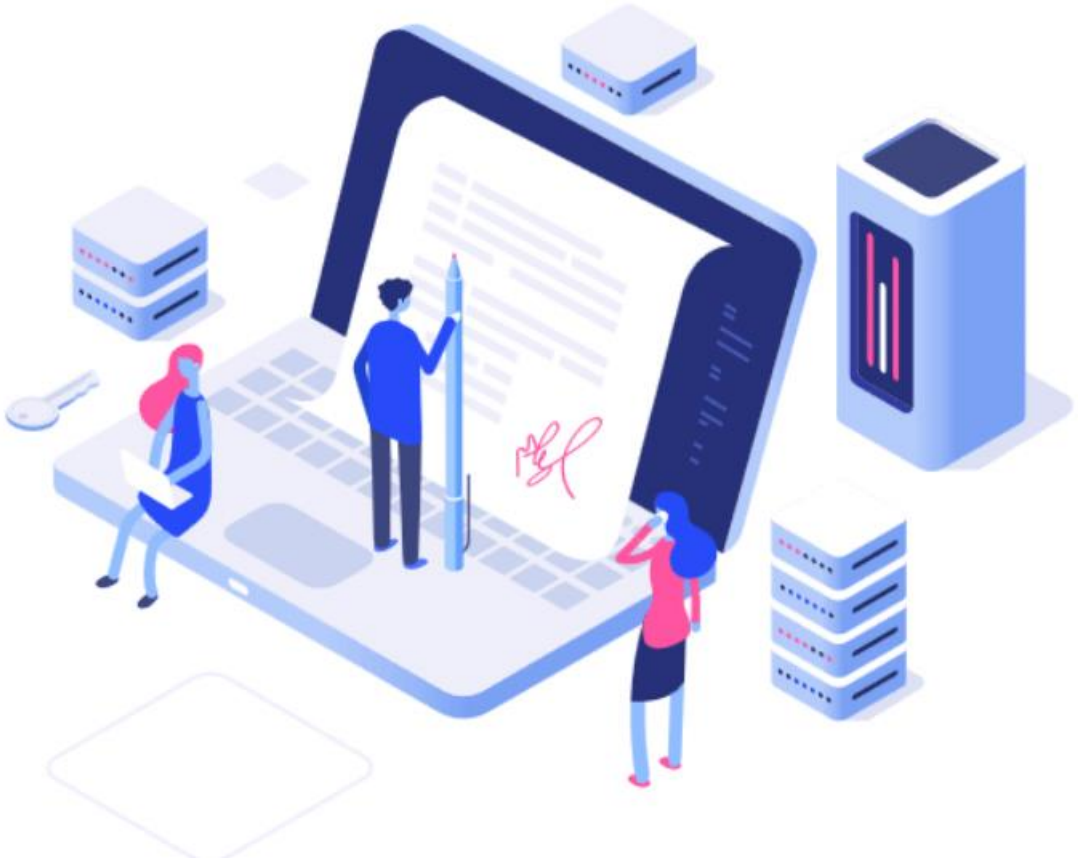
Proton Drive est une des solutions de l'entreprise Proton AG qui propose dans l'offre gratuite 1Gb de stockage pour le compte. Proton reste dans la même lancée avec son offre drive que pour ses autres services en offrant un service zéro accès et chiffré. Certes le stockage est très petit mais comme début si vous ne voulez stocker que le stricte minimum et que vous avez ou souhaitez avoir un compte Proton c'est intéressant.



Source : Proton AG

Offre Proton		
Free	1GB	0€
Mail Plus	15GB	4,99€/mois - 3,99€/mois pour 1an - 4,49€/mois pour 2ans
Proton Unlimited	500GB	11,99€/mois - 9,99€/mois pour an - 7,99€/mois pour 2ans

Vous pouvez également être un simple utilisateur gratuit de Proton et désireux d'avoir un stockage plus important pour votre Drive et basé au seins de l'UE (Allemagne), Filen peut être votre solution. Avec son stockage zéro accès et des offres à vie avantageuses il se démarque des autres.



Source : Filen

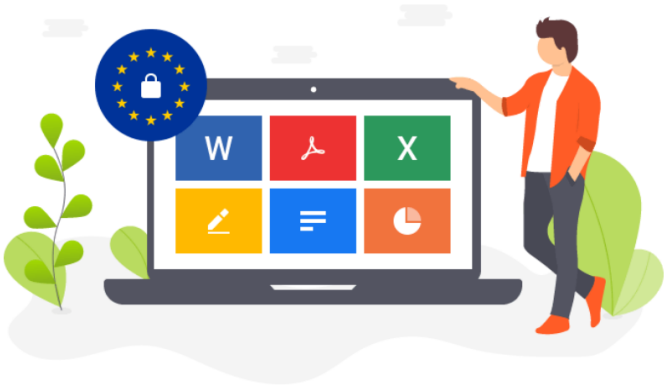
Offre Filen		
Free	10GB	0€
Starter	100GB	0,92€/mois – 29,99€€/LifeTime (voir offre du moment pour LifeTime et cumulable)
Pro I	500Go	3,99€/mois – 39,99€/an
Pro II	2To	8,99/mois – 89,99€/an
Pro III	5To	17,99€/mois – 179,99€/an

Si vous souhaitez plus de stockage gratuitement Méga inclut dans son offre gratuite 20GB de stockage chiffré (← vidéo explicative) et zéro accès.

Source : MEGA

Offre MEGA		
Free	20GB	0€
Pro Lite	400GB	4,99€/mois – 49,99€/an
Pro I	2To	9,99€/mois – 99,99€/an
Pro II	8To	19,99/mois – 199,99€/an
Pro III	16To	29,99€/mois – 299,99€/an

pCloud est un autre service hébergé en suisse et qui propose des stockages à vie non chiffré et la possibilité avec une option à vie ou mensuel de chiffrer les documents sensible.

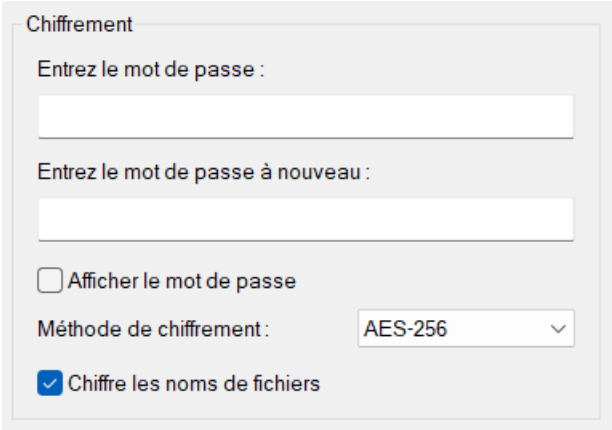


Source : pCloud

Offre pCloud		
Gratuit	10GB	0€
Premium	500GB	Offre mensuel et à vie disponible (prix varie en fonction des promotions)
Premium Plus	2To	
Forfait personnalisé	10To	
Option Chiffrement	✔	

Maintenant que nous avons vu un peu plus en détails les différents cloud qui existent parlons des clés USB. Lorsque l'on souhaite conserver des documents très importants sur une clé USB on peut se tourner vers des clés USB vendues par des grands noms de la tech et qui garantissent le plus haut niveau de sécurité et comme quoi elles seraient inviolables. En réalité ce n'est pas aussi simple et une étude récente a démontré qu'il était possible (pour un geek) de contourner toutes les sécurités qu'elles intègrent pour une majorité d'entre elles (malheureusement je ne retrouve plus l'étude qui appuie les propos que j'avance et je vous prie de bien vouloir me croire pour cette fois ci). Mais alors comment sécuriser ses documents ?

Avec une simple clé USB et le logiciel 7-Zip, ce logiciel sert initialement à compresser des fichiers mais il embarque également la possibilité de les ZIPer en les chiffrant avec un mot de passe :



Seule la méthode AES-256 est disponible mais ce chiffrement est considéré comme le plus haut standard de chiffrement symétrique qui existe actuellement. Pensez à mettre un mot de passe fort (Rappel : 20char min, lettres minuscules, lettres Majuscules, chiffres et charactères spéciaux ; le « ! » est le plus utilisé donc je vous conseille d'en mettre d'autres).

Attention :

- Une clé USB a une durée de vie inférieur à 10 ans.
- Pensez à faire de multiples sauvegardes (mais évitez de stocker vos 3 clés USB à votre domicile car vous risquez de tout perdre en cas de vol ou d'incendie…)
- Certaines clés USB sur le marché sont bidouillées et affichent par exemple 64Go de stockage mais en réalité elles ne supportent que 5Go et suppriment vos fichiers présents si vous ajoutez plus de 5Go. Je conseille donc de les acheter chez des marques connues tel que Kensington, SanDisk, Samsung…
- Utilisez Clé USB neuve de préférence

Je ne suis pas sans vous rappeler qu'il est très peu recommandé de brancher sa clé USB sur l'ordinateur de quelqu'un et inversement une clé USB qui ne vous appartient pas sur votre PC. Il est toujours préférable lors d'un échange de document de se l'envoyer par mail ou via un lien drive ou par un lien de partage de ficher (je recommande SwissTransfert à d'autres services moins rigoureux sur la vie privé). Je recommande également l'installation de Panda USB Vaccine qui est un logiciel limitant les attaques par clé USB. Mais surtout pensez à faire un petit ⊞ + L ou ctrl+⌘+Q avant de quitter votre PC pour verrouiller votre écran.

8. Modèle de menace

Un modèle de menace permet de se prémunir et adopter un comportement adapté à la situation. En fonction de si vous êtes un individu lambda, un journaliste, une personnalité politique ou encore un lanceur d'alerte, votre modèle de menace sera différent.

Voici trois points à regarder :

1. Identifier ce que l'on veut protéger
2. Identifier les risques qui pèsent sur nous
3. Identifier les mesures pour s'en prémunir

Je vous propose de regarder la conférence Souriez, vous êtes en sécurité : comprendre les modèles de menaces (50 min) publié par Capitole du Libre. Elle explique les questions qu'il faut se poser ainsi que comment s'en prémunir. Je ne suis pas complétement d'accord avec elle sur certains point (notamment le fait d'utiliser un mot de passe fort pour tous ses sites peux être judicieux) mais dans le fond l'introspection et les exemples qui sont citées sont pertinents.

9. Quelques chiffres

Types de données exposées lors des failles de sécurité :

Personnelle	30%
Paiement	23%
Médicale	21%
Bancaire	9%
Interne	6%
Secrets	6%
Autre	5%

Où retrouve-t-on le plus de malware :

Phishing / Ingénierie sociale	43%
Site non sécurisé	30%
Avertissement frauduleux	15%
Réseau social	8%
Autre	4%

Nombre de mails frauduleux reçus par les entreprises par an :

Taille de l'entreprises par employé	Mail frauduleux
1 – 250	1 à 323
251 – 500	1 à 356
501 – 1000	1 à 391
1001 – 1500	1 à 823
1501 – 2500	1 à 440
2501 +	1 à 556

Sources : ProtonMail – www.protonmailcom

Conclusion

Ne soyez pas ou ne devenez pas paranoïaque, intégrez les notions au fur et à mesure. Vous verrez que cela deviendra un réflexe comme de fermer la porte de chez vous en partant. Il est tout de même nécessaire de se faire sa propre idée sur chaque point abordé dans ce guide. De plus, dans la majorité des cas lorsqu'un service est gratuit, c'est que vous êtes le produit (excepté pour les services open source). Posez-vous donc la question : est-ce que je préfère payer pour un service respectueux de ma vie privé ou est-ce que je préfère utiliser un service sans me soucier de ma vie privée et des potentielles impacts que cela engendrera ? (La réponse à cette question est personnelle et à chacun de se faire sa propre idée sur le sujet.)

Vous pouvez retrouver la dernière version de ce document à l'adresse suivante : https://largo.web-edu.fr

Annexe

Est-ce que mes données ont fuité ou mon adresse mail est-elle corrompue ou piratée ?

- https://haveibeenpwned.com/
- https://www.dehashed.com/
- https://monitor.firefox.com/

Bibliographie

1 - Anonymat et confidentialité

Etude relative au croisement de base de données et la non-efficacité de l'anonymisation des données :
https://www.blogdumoderateur.com/donnees-anonymisees-identifier-personnes/

Etude de l'Irish Council for Civil Liberties (CNIL Irlandaise) sur la divulgation de manière inconsciente de donnée personnel à des entreprises :
https://www.iccl.ie/digital-data/iccl-report-on-the-scale-of-real-time-bidding-data-broadcasts-in-the-u-s-and-europe/

Les droits pour maîtriser vos données personnelles :
https://www.cnil.fr/fr/les-droits-pour-maitriser-vos-donnees-personnelles

Les courriers pour agir :
https://www.cnil.fr/fr/modeles/courrier

2 - Naviguer sur Internet

Les CGU de Whatsapp, Google, Tinder, Twitter, Facebook, Snapchat et Instagram en image :
https://twitter.com/hailmika/status/992391607302451200?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E992391607302451200%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.bfmtv.com%2Ftech%2Fvie-numerique%2Fseuls-7-des-internautes-francais-lisent-attentivement-les-conditions-d-utilisation_AN-201806040050.html

Vulgarisation des CGU d'Instagram
https://linc.cnil.fr/fr/une-juriste-traduit-les-cgu-dinstagram-pour-les-enfants-et-les-adultes

76% des 12-17 sont sur les réseaux sociaux :
https://www.familywebcare.com/nos-enfants-sont-ils-accrocs-au-smartphone-et-reseaux-sociaux-statistiques-dangers-comment-les-proteger/

Tester ce qu'un site peut faire :
https://clickclickclick.click/

Winnie l'ourson censuré en Chine :
https://www.lexpress.fr/actualite/monde/asie/winnie-l-ourson-censure-en-chine-parce-qu-il-ressemble-au-president-xi-jinping_1928038.html

Scandale ExpressVPN :
https://www.hackread.com/edward-snowden-stop-using-expressvpn/

Qu'est-ce qu'un VPN par le vidéaste Micode :
https://www.youtube.com/watch?v=ckZGQ5cLIfs

Principe de fonctionnement du réseau TOR :
https://itigic.com/fr/how-tor-routing-works-to-protect-privacy/

3 - Niveau de sécurité

Google authentification hack par des pirates :
https://www.zdnet.com/article/android-malware-can-steal-google-authenticator-2fa-codes/

Quel Yubikey est la mieux adapté à vos besoins ? :
https://www.yubico.com/comparez-les-produits/?lang=fr

4 - Gestionnaire de mot de passe :

Vérifier la solidité de vos mots de passe (ATTENTION NE METTAIS JAMAIS VOS VRAIS MOTS DE PASSES, remplacez certains, caractères cela vous donneras une idée de leur résistance):
https://ssi.economie.gouv.fr/motdepasse
https://password.kaspersky.com/fr/

Définir un bon mot de passe :
https://www.cnil.fr/fr/les-conseils-de-la-cnil-pour-un-bon-mot-de-passe
https://www.cnil.fr/fr/generer-un-mot-de-passe-solide

Article sur les gestionnaires de mots de passe :
https://www.cnet.com/tech/services-and-software/bitwarden-review-the-best-free-password-manager-for-2021/

FAQ Bitwarden :
https://bitwarden.com/help/

5 - Boîte mail sécurisé :

Politique zéro accès de ProtonMail :
https://proton.me/fr/mail/security

Bloqueur de traqueur ProtonMail :
https://proton.me/support/email-tracker-protection

Etude sur la quantité de traqueur dans les mails :
https://senglehardt.com/papers/pets18_email_tracking.pdf
Et sa vulgarisation :
https://freedom-to-tinker.com/2017/09/28/i-never-signed-up-for-this-privacy-implications-of-email-tracking/

DuckDuckGo Email protection :
https://spreadprivacy.com/introducing-email-protection-beta/

Qu'est-ce que SimpleLogin ? (en anglais) :
https://youtu.be/KxK5Mq8LfAg

6 - Messagerie instantané et sécurisé :

Tout est déjà dans le chapitre en question ;)

7 - Modèle de menace :

Conférence : Souriez, vous êtes en sécurité : comprendre les modèles de menaces (50 min) publié par Capitole du Libre :
https://www.youtube.com/watch?v=mnO4GBCNOe8

A l'air du numérique nos objets connectés font désormais partie de nos vies, aussi bien pour le travail que pour le perso. Constamment sur nos smartphone, tablette ou ordinateur nous naviguons à un âge de plus en plus jeune sur la vague d'internet. Mais cela n'est pas sans risque et exposons nos données personnelles sur la toile en toute inconscience.
Vous trouverez dans ce guide les outils pour vous prémunir des menaces les plus courantes.