

# Guide des bases de la protection de la vie privée

par Silent Guard

Bonjour et merci d'avoir téléchargé ce guide ! Ce que vous avez fait est une première étape essentielle : réaliser l'importance de sa vie privée et de ses données numériques et prendre des actions concrètes comme télécharger ce livret !

Nous allons voir ici, de manière simple et intuitive, comment renforcer votre sécurité en ligne. Dans ce livret, nous allons donc aborder des conseils directement liés à la cybersécurité en général et ensuite à la préservation de votre vie privée numérique. Bonne lecture !

Avant d'aller plus loin, nous allons parler de divers produits, solutions ou marques. Nous ne sommes affiliés à aucune compagnie et nous faisons nos recommandations via des tests, ainsi que des retours utilisateurs et professionnels.

## La cybersécurité et ses outils

- Houston, y a-t-il un problème ? (Les données qui ont déjà "fuité")
- La redondance, il n'y a pas mieux ! (Activation de la double authentification)
- Comment créer un mot de passe fort et s'en souvenir ?
- Les extensions à utiliser

## La protection de sa vie privée

- Comment faire disparaître nos données en ligne ?
- Comment protéger ses comptes en ligne ?
- Quel navigateur et moteur de recherche pour surfer sur le net ?
- Le VPN, l'arme ultime ?
- La zone grise des bloqueurs de pubs
- Les extensions à utiliser

## 1. La cybersécurité et ses outils

Notre but ici est de parler de la protection des données. Avoir une bonne sécurité générale sur Internet va être un avantage crucial. Les cyberattaques sont de plus en plus présentes. Selon le [GIP ACYMA](#) (Groupement d'Intérêt Public Action contre la Cybermalveillance), il y a eu plus de 173 000 demandes d'assistance en 2021, une hausse de 65 % comparée à 2020. Nous allons donc voir comment se prémunir de ces attaques, notamment des trois plus utilisées.

### a. Houston, y a-t-il un problème ? (Les données qui ont déjà "fuité")

Sans le savoir, certaines de vos informations ont peut-être déjà été “leakées” (c'est-à-dire que la base de données d'une entreprise qui possédait vos informations a été piratée et ces données ont été volées).

Pour le savoir, rendez-vous sur le site [Have I Been Pwned ?](https://haveibeenpwned.com) et entrez votre adresse mail sur la page principale.

Si le résultat est vert, tout va bien !

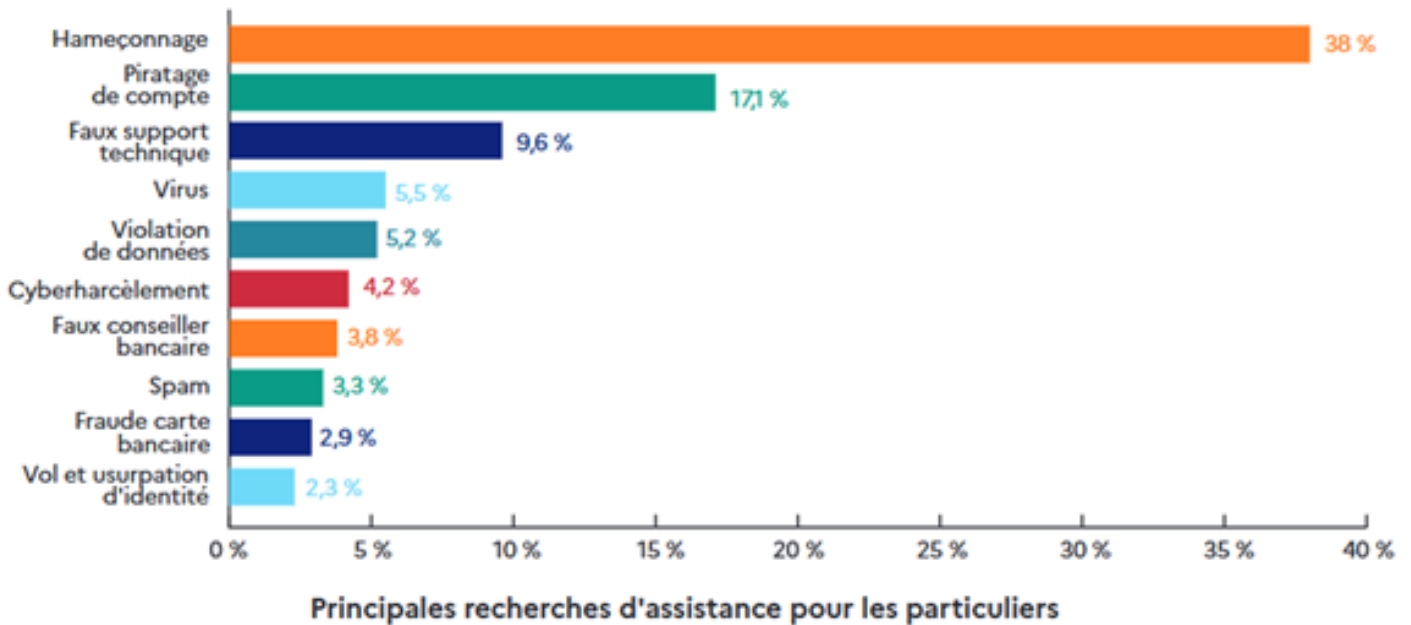
En revanche, si le résultat est négatif, il faut directement prendre les mesures nécessaires en fonction des informations qui ont fuité. Le mieux reste de mettre à jour les informations de connexion de la plateforme ciblée et de vérifier les autres données (comme l'adresse mail !).



The screenshot shows the 'Have I Been Pwned?' website interface. At the top, there is a navigation bar with links: Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. The main heading is 'have i been pwned?' with the subtitle 'Check if your email address is in a data breach'. Below this is a search input field containing 'example@gmail.com' and a 'pwned?' button. The result section is titled 'Oh no — pwned!' and states 'Pwned in 2 data breaches and found no passwords (subscribe to search sensitive breaches)'. It includes social media icons and a 'Donate' button. Under 'Breaches you were pwned in', it lists a breach from LDLC in March 2024, where 1.26M unique email addresses, names, phone numbers, and physical addresses were exposed. The compromised data includes email addresses, names, phone numbers, physical addresses, and salutations.

Ces informations vous permettent également d'être plus vigilant. Les trois attaques les plus utilisées en 2024 sont les suivantes :

## • Particuliers



Plus de 60% des attaques sont soit des attaques de hameçonnage (phishing) dans 38% des cas, du piratage de compte dans 17.1% des cas et pour finir 9.6% des gens sont victimes d'un faux support technique.

La bonne nouvelle est que vous pouvez contre vous même ces trois attaques !! Elles vont toutes nécessiter vos informations privées comme votre mail et votre numéro de téléphone. D'où l'importance de protéger vos données. Mais si vos données sont déjà en vente sur le darknet il vous suffira d'être vigilant sur les mails et les appels que vous allez recevoir avec ces quelques conseils simples :

- Aucun conseiller ou administrateur d'aucun service n'a besoin de votre mot de passe.
- Si vous n'avez pas confiance en un lien que l'on vous a envoyé par mail passer par une recherche internet plutôt que par ce lien.
- Si on vous met la pression pour agir immédiatement c'est le moment de prendre du recul et de bien réfléchir à la situation.
- Si vous devez payer sur un site auxquelles vous n'avez pas confiance passez par un service tiers comme [Paypal](#) ou bien créez [une carte virtuelle](#) via votre banque

Si vous avez été victime d'une attaque, contactez sans tarder l'Assistance et prévention du risque numérique.

Il reste à voir comment se protéger contre les piratages de compte. Ça se passe dans la prochaine section !

## **b. La redondance, il n'y a pas mieux ! (Activation de la double authentification)**

La double authentification est un moyen très sûr de renforcer la sécurité de ses comptes les plus critiques. Nous vous recommandons donc de l'activer sur les sites qui possèdent vos informations bancaires permanentes (Amazon, Fnac ...), les sites qui pourraient permettre d'usurper votre identité (sites gouvernementaux) et surtout l'accès à votre banque et à votre adresse mail.

Sécuriser son adresse mail est très important, car sur quasiment tous les sites, on peut utiliser l'option du "mot de passe oublié". Il suffit alors à l'attaquant d'avoir accès à votre compte mail pour s'introduire dans tous vos autres comptes.

La double authentification ajoute une vérification supplémentaire : lorsque vous vous connectez depuis un nouvel appareil, on va vous demander, en plus de votre mot de passe classique, un mot de passe actualisé toutes les 30 secondes sur un autre appareil (généralement votre téléphone). Cette protection découragera la majeure partie des attaquants de continuer l'attaque !

Pour l'activer, allez dans les paramètres de votre compte et dans l'onglet sécurité, vous y trouverez alors un paramètre lié à la double authentification (ou la validation en deux étapes).

Comme application de double authentification, vous pouvez utiliser [2Fas](#), qui a l'avantage d'être [open source](#) et donc plus transparent sur son fonctionnement. Ils ont d'ailleurs [plusieurs tutoriels vidéo](#) pour vous aider à activer la double authentification.

### **c. Comment créer un mot de passe fort et s'en souvenir ?**

Pour renforcer l'accès à nos comptes, il est préférable d'utiliser un mot de passe fort. Je pense que tout le monde a déjà vu ce genre de schéma, mais je me permets de mettre ici une version traduite du document de la compagnie [Hives Systems](#) sur le temps que mettent chaque type de mot de passe à être trouvé par un attaquant :

# COMBIEN DE TEMPS FAUT-IL À UN PIRATE POUR TROUVER VOTRE MOT DE PASSE 2024

[www.hivesystems.com/password](https://www.hivesystems.com/password)

Nombre de caractères	Nombres seulement	Lettres minuscules	Lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules, symboles
4	Immédiat	Immédiat	3 secs	6 secs	9 secs
5	Immédiat	4 secs	2 mins	6 mins	10 mins
6	Immédiat	2 mins	2 heures	6 heures	12 heures
7	4 secs	50 mins	4 jours	2 semaines	1 mois
8	37 secs	22 heures	8 mois	3 ans	7 ans
9	6 mins	3 semaines	33 ans	161 ans	479 ans
10	1 heure	2 ans	1k ans	9k ans	33k ans
11	10 heures	44 ans	89k ans	618k ans	2M ans
12	4 jours	1k ans	4M ans	38M ans	164M ans
13	1 mois	29k ans	241M ans	2Md ans	11Md ans
14	1 an	766k ans	12Md ans	147Md ans	805Md ans
15	12 ans	19M ans	652Md ans	9Bn ans	56Bn ans
16	119 ans	517M ans	33Bn ans	566Bn ans	3qd ans
17	1k ans	13Md ans	1qd ans	35qd ans	276qd ans
18	11k ans	350Md ans	91qd ans	2qn ans	19qn ans

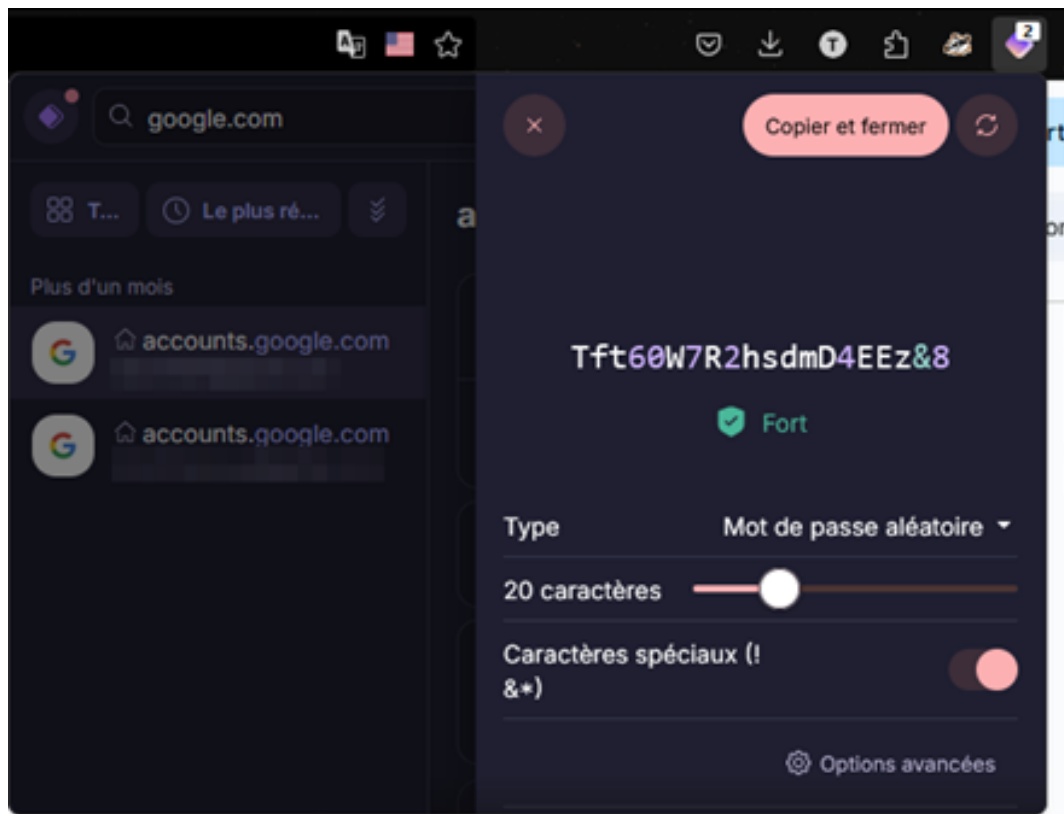


> 12 x RTX 4090 | bcrypt

Nous voyons donc que la complexité et également la longueur du mot de passe ont un impact important sur le temps mis à déchiffrer un mot de passe. Les recommandations de l'ANSSI actuelles sont d'avoir un mot de passe d'au minimum 12 caractères, avec des chiffres, des lettres majuscules, des lettres minuscules et des symboles.

Mais comment créer ce genre de mot de passe complexe lorsque l'on manque d'imagination ? Car il faut bien sûr éviter de s'inspirer de nos données personnelles.

C'est là qu'interviennent les gestionnaires de mots de passe. Ces coffres-forts numériques vont générer des mots de passe très complexes, comme celui-ci, généré via le gestionnaire de mots de passe Proton Pass :



Mot de passe utilisé à titre d'exemple, qui n'est utilisé nulle part.

Maintenant, vient la question de comment mémoriser ce type de mot de passe ? Eh bien, pas besoin ! Le gestionnaire de mots de passe va les retenir et vous les fournir lorsque vous en aurez besoin. Par exemple, si je veux me connecter à myEfrei, la plateforme de l'école, mon gestionnaire de mots de passe va me proposer mon identifiant et mon mot de passe.

 PARIS PANTHÉON-ASSAS UNIVERSITÉ

# Connexion

Utiliser votre compte Efrei

Identifiant ou n° de dossier

Mot de passe

Connexion en tant que...

auth.myefrei.fr  
2022

Identifiants oubliés ? [Contactez-le +33 1 88 289 250](#)

En me connectant, j'accepte les [conditions d'utilisations](#) du service SSO Efrei notamment en matière de données personnelles.

 Protection par reCAPTCHA - [Confidentialité](#) - [Conditions](#)

SE CONNECTER

Le gestionnaire sera protégé par un mot de passe fort que vous seul connaîtrez et qui, pour des raisons de sécurité, ne peut pas être régénéré si vous l'oubliez. Il faut donc s'en souvenir à coup sûr !

Pour choisir votre mot de passe, nous vous conseillons :

De ne pas prendre de gestionnaires multi-appareils gratuits : En effet, si le gestionnaire actualise votre base de mots de passe gratuitement, il doit trouver un moyen de se financer. Et ce sera sûrement par le biais de la vente de données ! Choisissez donc un gestionnaire que vous financez pour vous assurer une bonne protection, comme [BitWarden](#), [1Password](#) ou [ProtonPass](#). La version gratuite de ces gestionnaires est certes très limitée, mais elle permet de vous faire une idée du service ! Si vous ne voulez pas dépenser d'argent, il existe également des solutions hors ligne gratuites comme [KeePass](#). En revanche, tous vos mots de passe ne seront accessibles que sur la machine qui les stocke.

Et enfin, nous allons vous donner un dernier conseil pour créer vous-même un mot de passe fort : créez des phrases ! Une phrase impersonnelle peut faire un mot de passe très efficace tout en restant difficile à trouver pour un ordinateur qui n'utilise pas la logique humaine. Par exemple :

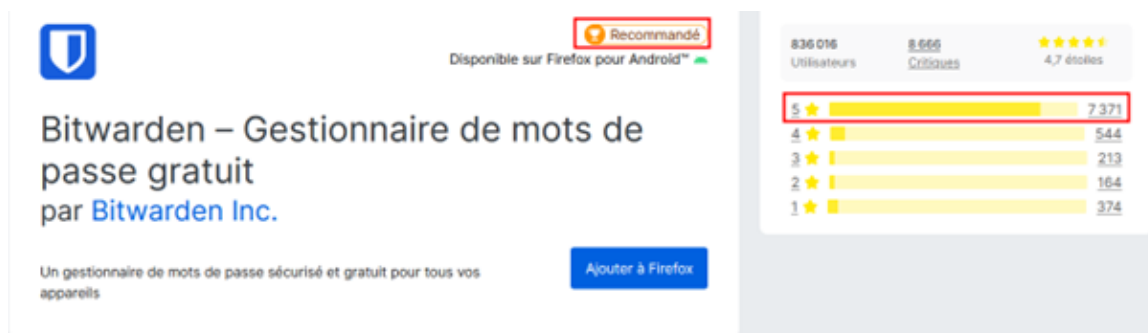
**JeVaisALaPêcheLe8Janvier.** Est un mot de passe fort qui respecte toutes les normes de l'ANSSI et est assez facile à retenir.

#### d. Les extensions à utiliser



Maintenant que vous avez les bons réflexes de sécurité, nous allons vous proposer quelques extensions. Ces extensions sont comme des améliorations que l'on fixe sur notre navigateur. Ici, les extensions recommandées sont pour le navigateur Firefox, mais il en existe d'autres similaires sur les autres navigateurs.

L'extension de votre gestionnaire de mots de passe : Comme vu précédemment, un gestionnaire de mots de passe est un très bon allié. L'avoir intégré à votre navigateur vous facilitera la vie. Tous les gestionnaires cités possèdent leurs propres extensions. Pour ne pas vous faire avoir, vérifiez bien les notes données à l'extension et, voire, si elle est recommandée par le navigateur lui-même.



Extension contre les sites malveillants et leurs scripts : Tous les sites web fonctionnent avec des scripts. Si ces morceaux de code sont inoffensifs la plupart du temps, ils peuvent s'avérer dangereux si vous vous rendez sur des sites malveillants. [NoScript Security Suite](#) vous protégera des scripts qui n'agissent pas de manière normale.

Vous voilà maintenant bien préparé pour affronter la jungle numérique. Mais n'oubliez jamais ce conseil : malgré une excellente protection, le plus important est de rester vigilant. La plupart des attaques aboutissent à cause d'une erreur humaine. Et si vous êtes attentif, aucun hacker ne pourra vous atteindre facilement !

## 2. La protection de sa vie privée

Comment protéger sa vie privée dans le plus grand espace de communication jamais créé par l'homme ? Vaste sujet ! Nous allons commencer simplement par vous dire qu'il n'est pas vraiment possible de complètement "disparaître d'internet". Même si vous n'y avez jamais mis les pieds, vous avez des traces sur le net. Mais ce que nous allons faire ici, c'est vous montrer comment, par des gestes simples, limiter au maximum votre [empreinte numérique](#). Pour qu'une personne lambda, un attaquant ou une entreprise en sache le moins possible.

### a. Comment faire disparaître nos données en ligne ?

Comme nous l'avons dit, nous générons des données lorsque nous sommes en ligne, et les data brokers (les entreprises qui conservent nos données) les gardent comme ressource à utiliser. Il existe une manière de forcer ces géants à supprimer vos données : la voie légale ! Si vous en faites la demande, un data broker est normalement obligé de supprimer vos informations.



[PrivacyRight](#) possède une liste des emails des data brokers à contacter. Mais que mettre dans le mail ? La CNIL propose des modèles d'emails pré-rédigés pour vous aider. [Voici celui destiné à la suppression des données.](#)


Attention toutefois, en fonction de la localisation et de la politique de l'entreprise, il peut être compliqué de forcer la suppression, mais c'est toujours une tentative à envisager.

## b. Comment protéger ses comptes en ligne ?

Nous pouvons, sans le vouloir, laisser des informations visibles sur internet, alors que quelques actions simples peuvent nous protéger. Prenons l'exemple de Strava, un "réseau social pour sportifs" :

Par défaut, un compte Strava est public. Tout le monde peut voir toutes les activités du compte dans les moindres détails.

Pour limiter cela, il faut, comme pour toutes les applications, aller dans les paramètres, puis dans l'onglet confidentialité.



**STRAVA** 🔍 Tableau de bord ▾ Entraînement ▾ Cartes Challenges [Envoyer un cadeau](#) 🔔 9+ 

Mon profil

Mon compte

Mes performances

Préférences d'affichage

**Contrôles de la confidentialité**

Autorisations d'accès aux données

Notifications par e-mail

Mon matériel

Mes applications

Intégrations de partenaires

Mes badges

## Contrôles de la confidentialité

### Emplacements où vous apparaissez

#### Page de profil

Votre page de profil affiche des informations vous concernant, comme votre nom, vos activités, vos abonnés, vos photos et vos statistiques. Certaines parties de votre page de profil seront toujours disponibles publiquement. [En savoir plus.](#)

QUI PEUT VOIR

☒ **Abonnés**

Les membres abonnés à votre profil peuvent voir l'ensemble de votre page de profil. Tout le monde peut rechercher et consulter certaines informations de votre profil, et vous pouvez approuver vos abonnés.

#### Activités

Les activités sont des entraînements, des courses ou des événements que vous enregistrez ou que vous téléchargez sur Strava. Les options que vous choisissez ci-dessous seront vos options **par défaut**, mais vous pouvez modifier les paramètres de chaque activité individuelle. Vous apparaîtrez dans des activités de groupe ou dans les Flybys si vous n'ajustez pas ces options. [En savoir plus.](#)

QUI PEUT VOIR

☒ **Abonnés**

Seuls vos abonnés pourront voir les détails de vos activités. Vos activités n'apparaîtront pas dans les classements des segments ou des challenges, et il se peut qu'elles ne soient pas prises en compte pour certains objectifs de challenge. Les membres qui ne sont pas abonnés à votre profil pourront peut-être voir des résumés de vos activités, en fonction de vos autres paramètres de confidentialité.

#### Activités de groupe

Cette fonctionnalité détecte si des athlètes ont enregistré des activités ensemble. Si c'est le cas, les activités sont groupées et affichées en fonction des options ci-dessous. [En savoir plus.](#)

QUI PEUT VOIR

☒ **Abonnés**

Vos activités de groupe ne seront visibles que par les athlètes abonnés à votre profil et par les athlètes auxquels vous êtes abonné(e).

#### Flyby

Les Flybys fournissent aux utilisateurs Strava ou aux internautes la possibilité de relancer des activités de manière détaillée. Ils vous permettent de regarder à nouveau une activité, minute par minute, de voir les athlètes qui se trouvaient à proximité et le lieu où vous vous êtes croisés. [En savoir plus.](#)

QUI PEUT VOIR

☒ **Personne**

Vos activités ne seront pas visibles dans les Flybys, ni pour vous ni pour personne d'autre.

On peut voir ici une page avec une bonne confidentialité, puisque seules les personnes dont on a accepté l'abonnement peuvent voir nos activités. Ce type de paramètre existe sur la plupart des réseaux sociaux et doit être activé pour renforcer votre vie privée, tout en continuant à profiter de ces plateformes !

### c. Quel navigateur et moteur de recherche pour surfer sur le net ?

Commençons par l'interface qui vous permet d'accéder au web. Ici, il faut bien différencier le navigateur et le moteur de recherche. Le navigateur, c'est l'application qui va être installée sur votre ordinateur, le support. Votre navigateur actuel est probablement Chrome, comme 60 % des Français.

Et ensuite, dans ce navigateur, il y a le moteur de recherche, la fenêtre où vous allez poser votre question. Et là, vous utilisez très probablement Google, qui est le choix de 87 % des Français.

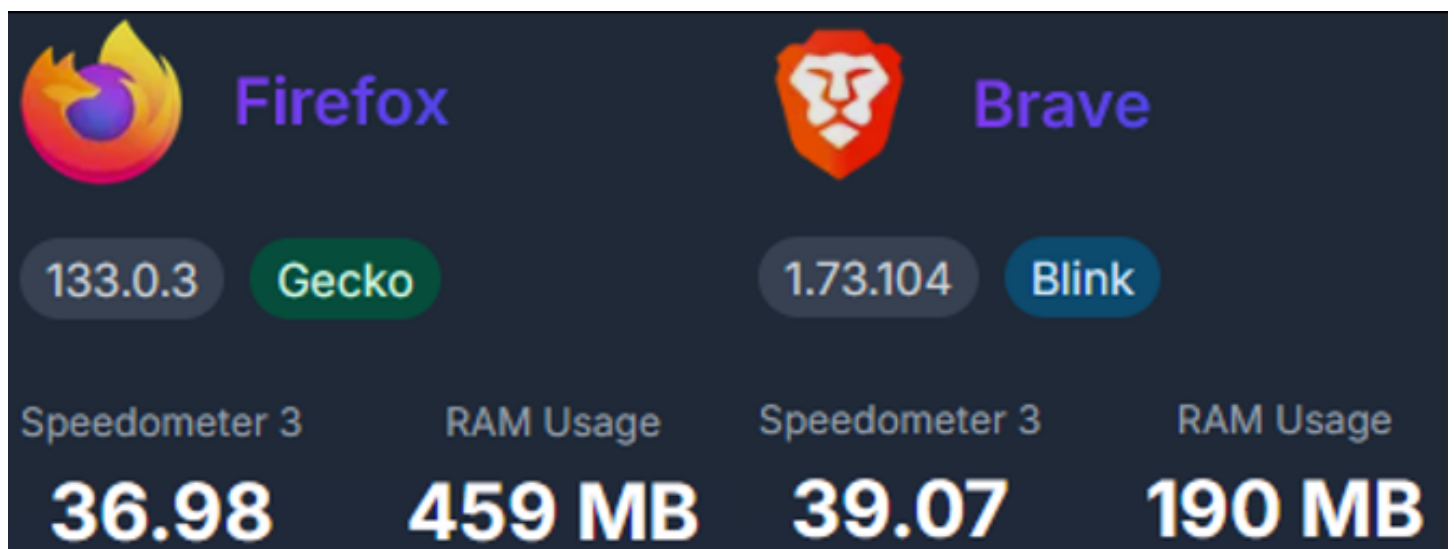
Mais au final, quoi utiliser ? Et quelle est la différence ?

[PrivacyTest.org](https://www.privacytest.org) regroupe un benchmark de plusieurs navigateurs. En le parcourant, on remarque que plusieurs navigateurs se démarquent :

- Brave
- Firefox
- LibreFox
- DuckDuckGo

Ces quatre navigateurs offrent de bonnes protections. Mais LibreFox et DuckDuckGo, étant des navigateurs peu utilisés, sont moins éprouvés et disposent de moins de fonctionnalités. Le choix sera donc plus à faire entre Brave et Firefox.

Pour résumer, entre nos deux navigateurs, Brave sera légèrement plus rapide là où Firefox sera plus gourmand en ressources. Mais Firefox garde l'avantage d'être un organisme à but non lucratif et fait beaucoup avec la Mozilla Foundation pour promouvoir la vie privée en ligne.



Donc, pour résumer, si vous voulez un navigateur sûr et le plus rapide, optez pour [Brave](https://brave.com). Si vous voulez un navigateur également très sûr, qui milite pour la protection de la vie privée de manière libre et indépendante, soutenez [Firefox](https://www.firefox.com) !

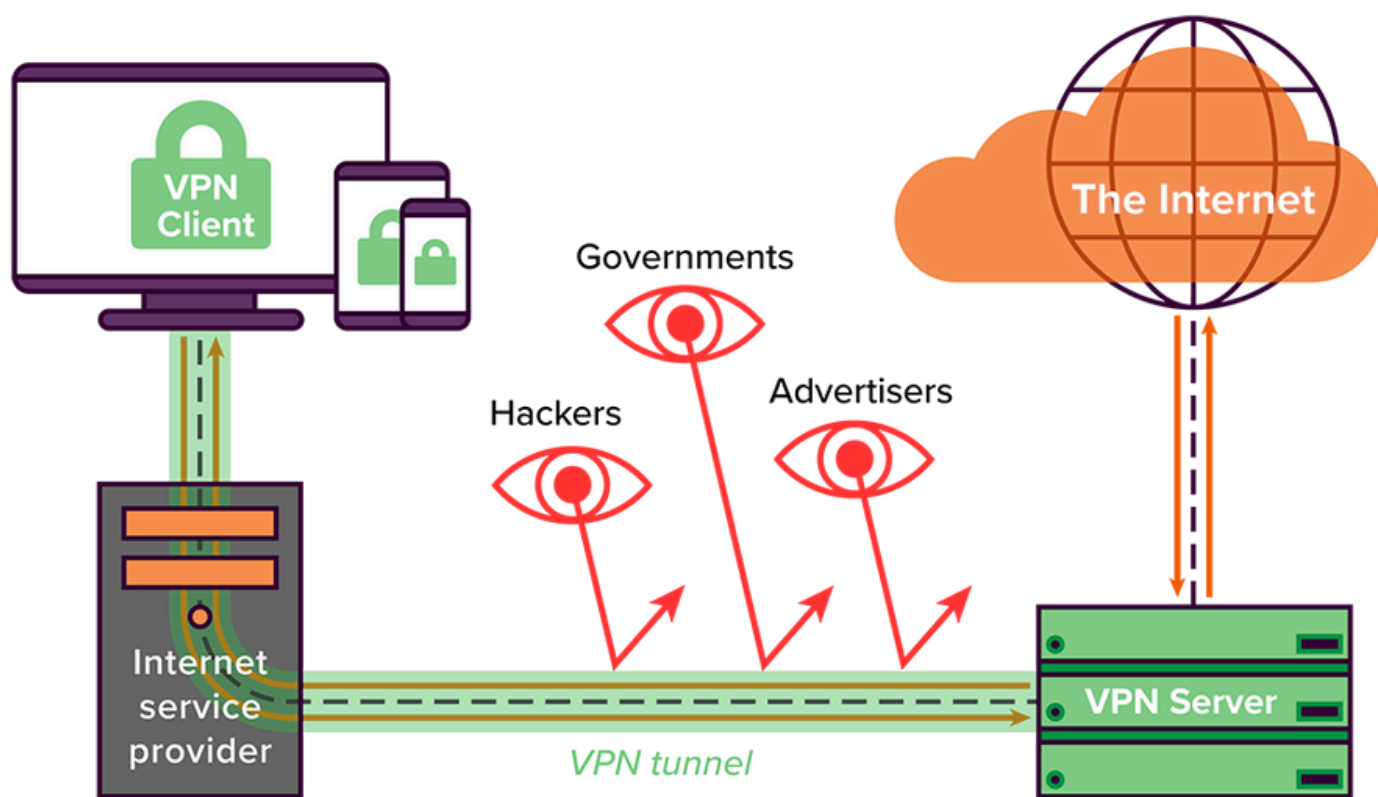
Concernant le moteur de recherche, il n'y a qu'un moteur bien connu qui se concentre sur la

protection de la vie privée : [DuckDuckGo](https://duckduckgo.com/).

#### d. Le VPN, l'arme ultime ?

Si vous êtes sur Internet, vous avez forcément entendu parler des VPN, non ? Depuis cinq ans, on les voit partout dans des publicités qui nous promettent de belles réductions en se localisant partout dans le monde. Mais un VPN, ce n'est pas du tout fait pour ça !

Les VPN (Virtual Private Network) vont créer un tunnel sécurisé entre votre machine et le site web que vous allez consulter. L'avantage principal se situe au niveau de la vie privée ! Toutes les personnes qui cherchent à récupérer vos informations personnelles à votre insu échoueront face au VPN. Vous êtes donc protégé des attaques de type "[homme du milieu](#)" (Man-in-the-Middle).



Attention tout de même, un VPN ne vous protège pas de tout et tout le monde. Votre Fournisseur d'Accès à Internet (FAI) aura toujours des informations sur vous et votre activité en ligne, ainsi que le site web que vous allez consulter.

Donc oui, un VPN va vous protéger de nombreuses attaques en ligne, oui, il va protéger votre vie privée, et oui, vous allez sûrement pouvoir faire des économies en prenant un abonnement quelconque en Argentine (ce qui est une utilisation discutable que nous ne vous recommandons pas). Un VPN peut également, par exemple, vous permettre d'esquiver la censure dans votre pays. Même en France, certains contenus en ligne sont bloqués pour des raisons politiques. Un VPN est donc un bon ajout à votre arsenal numérique, MAIS :

- Il ne vous rend pas invincible. Restez responsable en ligne et faites attention à tout ce que vous faites. La principale faille restera toujours l'utilisateur lui-même !

- Comme pour les solutions vues précédemment, n'utilisez jamais de VPN gratuit ! Pour générer de l'argent, ces services vendront vos données, voire pire. Privilégiez une solution payante de qualité. Dans notre équipe, nous utilisons uniquement le VPN de la firme suisse Proton, qui nous donne entière satisfaction. Mais nous vous invitons à regarder d'autres offres qui pourraient être tout aussi intéressantes, tout en restant vigilant !

## e. La zone grise des bloqueurs de pubs

Les bloqueurs de publicité (ou Adblockers) sont assez connus du grand public, mais seulement [31 % des Français les utilisent](#). Certaines personnes ne les utilisent pas, car elles ne savent pas si ce genre de dispositif est légal ou non.

Les bloqueurs de publicité sont certes controversés, mais l'année dernière, [un tribunal allemand a reconnu légitime leur utilisation](#). Cela crée donc une jurisprudence au niveau européen. Ne vous privez donc pas d'utiliser un bloqueur de publicité pour limiter les données générées par celles-ci et avoir une page web plus agréable !



## f. Les extensions à utiliser

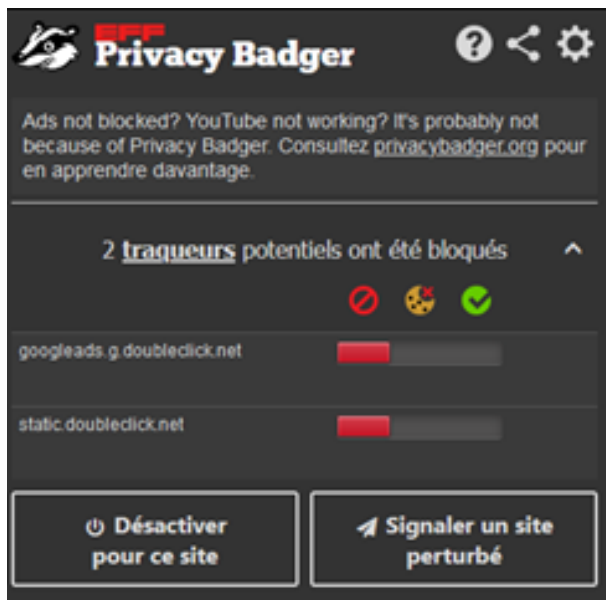
Nous allons ici parler de quelques **extensions** qui vont faciliter la protection de votre vie privée en ligne.

Premièrement, comme dit dans la dernière section, **un bloqueur de publicité est intéressant et légal à installer et à utiliser**. Nous vous conseillons **uBlock Origin**, une solution fiable et

**open source**, disponible sur de nombreux navigateurs.

**Privacy Badger** est une extension qui vous permettra de bloquer automatiquement **les cookies** et **les traqueurs** qui enregistrent votre navigation sur le web.

Il existe d'autres extensions pertinentes pour la sécurité, mais nous vous **recommandons de ne pas trop en ajouter**, car cela risquerait de **nuire à votre expérience globale**.



Si vous avez un abonnement à un VPN, il existe également des extensions permettant d'activer ce VPN directement depuis votre navigateur. Attention toutefois, le flux qui ne passera pas par le navigateur ne sera pas chiffré par le VPN !