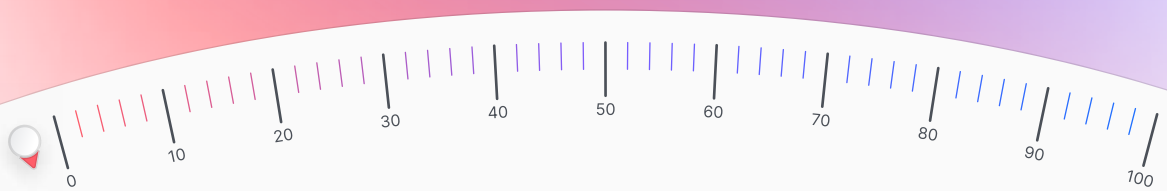
LE guide

Comment protéger votre vie privée sur Internet ?

Qwant, Proton, Olvid et Murena vous donnent les clés pour comprendre et mettre en place des solutions qui vous permettront de protéger vos données personnelles sur le web.



Guide proposé par :

Qwant Proton Olvid murena

À l'ère du numérique plus éthique et responsable, **Qwant, Proton, Olvid et Murena,** acteurs majeurs en Europe proposant des **services numériques éthiques,** sans collecte de données personnelles, vous donnent les clés pour **comprendre pourquoi protéger votre vie privée en ligne et comment garder vos données vraiment privées.** Définitions, conseils et solutions, voici LE guide qui vous accompagnera dans votre transition, vers un univers où vous serez libre et incognito.

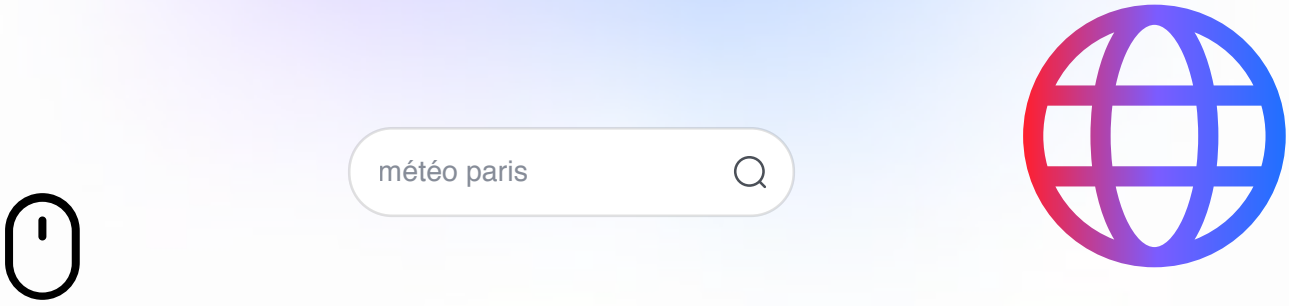
Vous avez déjà eu le sentiment d'accepter machinalement les cookies en arrivant sur un site web ? Vous êtes lassé de retrouver des publicités de baskets, sous prétexte que c'était l'objet de votre dernière recherche ? Vous acceptez systématiquement le partage de votre géolocalisation, même si le site ou l'application ne le nécessite pas ? Vous êtes fatigué de n'avoir d'autres choix que de partager des e-mails, des fichiers et des informations privées avec des entreprises et souhaitez reprendre le contrôle de votre identité en ligne ? Vous avez l'impression que votre smartphone vous écoute ?

Si vous vous reconnaissez dans au moins une de ces situations, alors **ce guide est fait pour vous !** Nous allons vous donner les clés pour mieux comprendre par quel mécanisme, internet sait tout de vous. Nous vous partagerons également des **astuces et solutions,** pour limiter les traces que vous laissez lors de votre navigation sur le web.

1 On révise, on apprend les bases

À chacune de vos connexions sur internet, vous laissez une trace de votre passage : informations recherchées, produits achetés commentaires postés, emails envoyés, posts commentés, connexion sur les sites, utilisation d'une application..., tout est répertorié ! Cela vous semble peut-être sans conséquence, peu importe que l'on connaisse ce que vous aimez. **Mais qu'en est-il des données transmises sans le vouloir ?** Quel usage en font les sites ?

Au fur et à mesure des connexions ou de l'usage d'applications tierces, ces données sont cumulées et dessinent votre **profil numérique.** Votre profil numérique révèle **vos relations, vos opinions, vos habitudes, vos déplacements, toute votre vie privée en somme.** Ce profil numérique est souvent vendu et revendu à de multiples entreprises, qui en tirent un profit. Comment cela est-il possible ? Comment cela fonctionne-t-il ? Voici des explications qui vous aideront à mieux appréhender ce sujet.



Quelle est la différence entre navigateur et moteur de recherche ?

Un navigateur est un logiciel qui permet de consulter des pages web, comme un site e-commerce ou celui de votre média préféré par exemple. Aujourd'hui, les navigateurs les plus utilisés sur le marché sont Firefox, Safari ou encore Chrome.

La barre de recherche présente sur le navigateur permet à la fois d'accéder à une page web via son URL *(www.exemple.com)* mais aussi d'effectuer une recherche via le moteur de recherche défini par défaut, sur le navigateur.

Un **moteur de recherche est un site internet qui permet de rechercher d'autres sites internet.** On accède donc à un moteur de recherche via un navigateur.

Aujourd'hui, les moteurs de recherche les plus utilisés sont Bing, DuckDuckGo, Ecosia, Google, Lilo, Qwant, ou encore Yahoo.

Vous faites une requête, par exemple « météo paris » et le moteur de recherche va vous proposer plusieurs sites qui pourraient répondre à votre demande.

Le moteur de recherche vous guide vers le bon site alors que le navigateur est juste une connexion au monde numérique.

Pour imager la différence entre ces deux termes, le navigateur est le véhicule qui vous transporte alors que le moteur de recherche est le GPS qui vous indique le meilleur chemin pour trouver la meilleure page web correspondant à votre requête.

C'est quoi un cookie ?

Il vous est sûrement déjà arrivé de voir une publicité sur les réseaux sociaux et de vous demander « comment peuvent-ils savoir que j'ai déjà recherché ce produit sur un autre site internet ? » La réponse à la question est … « grâce » aux cookies !

Mais qu'est-ce que c'est un cookie ?

C'est un petit **fichier texte qui est déposé par le navigateur** sur votre ordinateur quand vous visitez un site web. **Ce cookie va traquer votre navigation sur le web.** Ce cookie a une date de péremption, c'est-à-dire qu'il se supprime après un certain délai.

Ce cookie, déposé sur votre ordinateur, peut avoir plusieurs utilités :

Cookies fonctionnels :

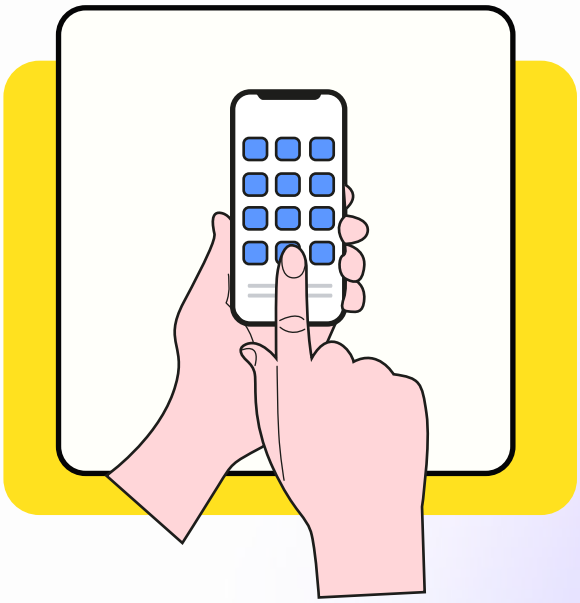
Ils enregistrent vos préférences sur un site internet, à savoir connexion automatique au compte, localisation, langue et autres paramètres choisis. Cela permet d'améliorer votre expérience en tant qu'utilisateur d'un site.

Cookies tiers ou cookies publicitaires :

Ils enregistrent principalement le comportement de l'utilisateur et le chemin du visiteur sur internet afin de créer ultérieurement, un profil utilisateur qui est enrichi au fur et à mesure des connexions. Sur la base de ce **profil utilisateur,** il est alors possible de placer de la publicité personnelle. Ce profil utilisateur peut donc être **revendu à des sites tiers** et aux réseaux sociaux par exemple qui vous présenteront par la suite, des publicités pour des marques ou des produits recherchés précédemment. C'est de cette manière que vous vous retrouvez avec une publicité pour une paire de chaussures recherchée quelques jours ou semaines auparavant, sans que vous n'ayez rien demandé à personne.

C'est quoi un pisteur ?

Non, un pisteur n'a rien à voir avec une station de ski. Ici il s'agit des pisteurs que vous pouvez retrouver **dans les applications mobiles** que vous téléchargez sur votre smartphone. Ces pisteurs sont des **librairies de code** (appelées Software Development Kit ou SDK), **chargées de collecter des informations** sur la personne qui utilise une application, ou bien sur les usages ou l'environnement de cette personne. Ces SDK permettent de gagner du temps dans le développement d'une application en utilisant du code déjà existant. Ils peuvent être utilisés pour analyser l'audience ou le parcours réalisé par l'utilisateur sur l'application, mais également pour le localiser et le profiler. Ce pisteur va donc **collecter des informations sur vous,** vos usages, tout comme les cookies, mais sur votre **smartphone.**



Qu'est-ce que les pixels espions ?

Les pixels espions sont largement utilisés par les entreprises et les spécialistes du marketing, en particulier dans les newsletters et les e-mails promotionnels. Ce sont de simples **images hébergées sur un serveur externe** qui sont insérées dans vos e-mails. Dès lors qu'elles sont chargées pour être affichées dans vos e-mails, ces pixels espions **collectent et partagent des informations personnelles** telles que la date et l'heure d'ouverture, le type d'appareil utilisé et le système d'exploitation ou encore votre adresse IP et position géographique. Ces informations peuvent ensuite être collectées et utilisées pour vous profiler et vous cibler avec des publicités personnalisées. Certains de ces trackers sont presque invisibles - ils se présentent sous la forme de petites images transparentes qui sont uniquement utilisées pour collecter des informations supplémentaires sur vous.

Comment marche la publicité en ligne ?

Des publicités, on en voit tous les jours : que ce soit sur les réseaux sociaux ou à la télévision, aussi bien pour nous proposer des réductions sur notre prochain voyage que pour un produit qui nous fait de l'œil depuis des semaines ! Mais savez-vous comment cela fonctionne vraiment ?

La publicité en ligne fait intervenir 3 acteurs :

- **les annonceurs** qui font la **promotion de leur produit,**
- les **plateformes publicitaires** sur lesquelles sont **affichées les pubs,**
- les **sociétés de traçage** qui **récupèrent toute une série d'informations** sur vous.

Comme nous l'avons vu dans un précédent paragraphe, chaque utilisateur laisse des traces sur internet. Ces traces peuvent être collectées par des sociétés de traçage qui déposent les fameux cookies publicitaires sur nos ordinateurs et smartphones pour récupérer des données. Ces données peuvent être revendues à des plateformes publicitaires.
Les marques font ensuite appel à ces plateformes pour faire la publicité de leurs produits. Le rôle des plateformes publicitaires va être de connecter les utilisateurs au produit à vendre, grâce au profil établi à partir de leurs données personnelles de navigation.

Par exemple, vous avez récemment cherché une enceinte portable. Lors de votre recherche, la société de traçage a déposé des cookies sur votre appareil. Elle sait donc que vous avez cherché ce produit récemment. Elle va revendre cette information aux plateformes publicitaires qui vont ainsi vendre des espaces publicitaires aux marques qui vendent des enceintes. Lors de vos prochaines connexions, des publicités d'enceintes portables vous seront ainsi proposées.

Pas très pratique quand l'achat est personnel, ou quand il s'agit d'un cadeau non ?
Les GAFA (Google, Apple, Facebook, Amazon) sont les plus importantes plateformes publicitaires du marché.

Qu'est-ce qu'un algorithme ?

Si on schématise, un algorithme est un **ensemble d'opérations qui permet de résoudre un problème.** Par exemple, une recette de cuisine, c'est sûrement l'un des algorithmes les plus simples : il s'agit d'une suite d'instructions qui permet d'obtenir un résultat. Il en existe bien évidemment, des plus complexes.

Les **algorithmes de recherche** par exemple : ce sont des **suites d'instructions qui permettent d'obtenir un résultat en fonction d'une requête.** Ce résultat peut être un objet dans une image, un mot dans un texte, ou encore une liste de pages web. On peut voir un algorithme un peu comme une chaîne de production : on fournit des informations en entrée, et on obtient un résultat en sortie. C'est d'ailleurs comme ça que fonctionnent les moteurs de recherche. Vous entrez une requête et le moteur de recherche va utiliser une série d'algorithmes pour aller chercher toutes les pages web susceptibles de répondre à votre question.

Il existe **deux types de moteurs de recherche :**

Ceux dont les résultats de recherche sont influencés par vos informations personnelles, votre géolocalisation, votre culture, votre historique de recherche (recettes recherchées, actualités consultées, sites préférés etc.). C'est le cas de Google par exemple.

Ceux qui n'utilisent pas ces informations car ils ne collectent pas de données personnelles, comme Qwant par exemple.
Les résultats proposés sont donc impartiaux dans le sens où ce sont les mêmes pour tous, peu importe votre profil.

Certains algorithmes ont été conçus de sorte que leur comportement évolue dans le temps, en fonction des données qui leur ont été fournies. Ces algorithmes « auto-apprenants » relèvent du domaine de recherche des systèmes experts et de l'intelligence artificielle. Ils sont utilisés dans un nombre croissant de domaines, allant de la prédiction du trafic routier à l'analyse d'images médicales.

vacances

Qu'est-ce qu'une bulle de filtre ?

La bulle de filtre est le concept dans lequel, **les algorithmes biaisent les opinions des utilisateurs en recommandant du contenu en fonction des préférences des utilisateurs.** Les préférences des utilisateurs sont connues grâce aux cookies déposés par les sites, lors de la navigation sur Internet.

Les contenus qui vous sont alors proposés au fur et à mesure de vos recherches sont sur-personnalisés et peuvent générer une sorte d'enfermement, d'isolement dans une bulle intellectuelle et informationnelle, que l'on appelle une bulle de filtre.

Concrètement, certains moteurs de recherche peuvent montrer des **résultats différents à deux utilisateurs qui font la même requête.**

Par exemple, une recherche de logement de vacances peut donner des résultats d'hôtels 5 étoiles plutôt que de camping ou de bed & breakfast en fonction de l'historique de recherche et de navigation. Cela est également valable pour les actualités qui vous sont proposées ou les prix annoncés. Vos habitudes de lecture vous mettent dans des cases définissant votre profil. Les actualités qui vous sont proposées seront alors en relation avec ce profil, limitant ainsi votre sens critique.

L'internaute se retrouve ainsi **enfermé dans une bulle de filtre.** La seule manière de ne pas être coincé dans cette bulle est de limiter au maximum les traces que vous laissez sur internet, de limiter au maximum la collecte de vos données personnelles numériques.

Qu'est-ce que le chiffrement ? Et le chiffrement de bout en bout ?

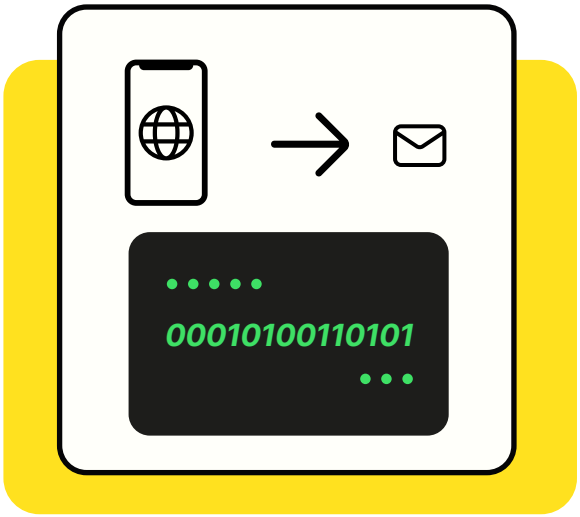
Lorsque vous communiquez sur internet, vos données traversent potentiellement des centaines, voire des milliers de kilomètres avant d'arriver à destination. Des câbles, des routeurs, des serveurs sont nécessaires pour véhiculer vos données. Mais cela signifie-t-il que tous ces éléments ont nécessairement accès à tout ce que vous envoyez, alors qu'ils n'en sont pas les destinataires finaux ? Non ! Il est possible de protéger vos données contre des oreilles indiscrètes grâce à la **cryptographie,** la science des codes secrets, via un procédé que l'on appelle le **« chiffrement ».**

Prenons un exemple : lorsque vous vous connectez au site *https://www.qwant.com/* et que vous y effectuez une recherche, votre requête est automatiquement « chiffrée » par votre navigateur avant d'être envoyée aux serveurs de Qwant, où elle sera « déchiffrée » de manière à permettre à Qwant de préparer une liste de sites pertinents à vous renvoyer. Bien évidemment, cette liste est elle aussi chiffrée par Qwant avant de vous être envoyée. Votre navigateur déchiffre alors ce résultat juste avant de vous l'afficher. Le tour est joué !

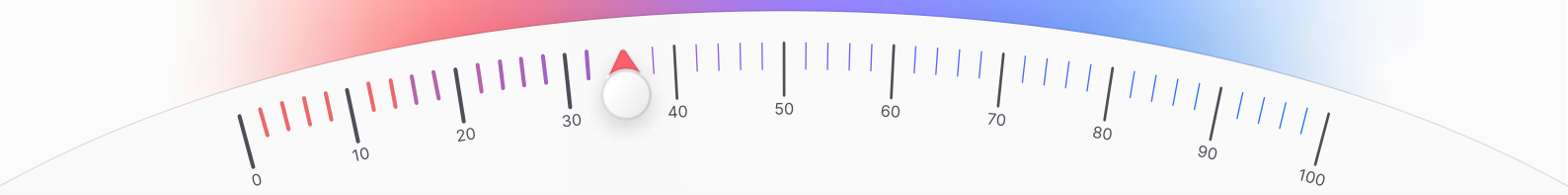
Via le chiffrement, vos recherches ne sont connues que de vous et de Qwant, qui ne sait pas qui se cache derrière la recherche.

Nous avons vu comment le chiffrement permet de sécuriser vos communications avec un serveur proposant un service, comme celui de Qwant. Mais qu'en est-il des communications entre vous et un autre interlocuteur physique ? C'est là qu'intervient le **« chiffrement de bout en bout ».**

Lorsque vous envoyez un message à un correspondant via une messagerie grand public classique, il est généralement chiffré entre votre dispositif (smartphone ou ordinateur) et le serveur de l'opérateur proposant le service de messagerie, qui le déchiffre afin de le stocker « en clair » en attendant que le destinataire viennent le chercher. Ce message est ensuite chiffré entre le serveur et le destinataire final. C'est ce que l'on appelle du **« chiffrement de point à point ».** Le problème ? C'est que le fournisseur du service a accès à tout ce que vous communiquez alors qu'il n'en est pas le destinataire final. Nous voilà revenus au problème précédent… Fort heureusement, une solution existe : le fameux **chiffrement de bout en bout.** Cette technologie permet de **s'assurer que vos messages seront chiffrés sur votre dispositif avant de le quitter et ne seront déchiffrés qu'à un seul endroit :** sur le dispositif de votre destinataire. Entre les deux, vos messages restent chiffrés, y compris lorsqu'ils sont stockés sur le serveur du fournisseur du service. Le tour est à nouveau joué !



Malheureusement, peu de services de messagerie proposent du chiffrement de bout en bout par défaut. Ce n'est par exemple pas le cas de Gmail (pour le mail) ou de Telegram (pour la messagerie instantanée). Cela peut paraître surprenant : finalement, le chiffrement de bout en bout ne fait que **reproduire dans un monde numérique ce que nous faisons depuis des siècles avec nos lettres physiques :** nous les glissons dans des enveloppes avant de les envoyer !



Les bons réflexes à adopter pour maîtriser ses données

« Aujourd'hui c'est décidé ! Je maîtrise les traces que je laisse quand je navigue sur internet » Vous ne savez pas par où commencer ? On vous aide !
Première étape : ménage de printemps. Une fois que tout est nettoyé, on s'équipe.
3, 2, 1 … c'est parti !

2 Faire le ménage

Supprimer les cookies et son historique de navigation

Les cookies enregistrent vos actions, autrement dit votre navigation sur internet. Alors la première chose à faire est de faire le ménage et de **supprimer vos cookies.** Comment vous y prendre ?

Tout dépend votre navigateur !

Si vous utilisez Firefox :

1. Dans la barre des menus en haut ou en bas de l'écran en fonction des appareils, cliquez sur Firefox et sélectionnez *Préférences.*
2. Sélectionnez le panneau *Vie privée et sécurité* et rendez-vous à la section *Cookies et données de sites.*
3. Cliquez sur le bouton *Effacer les données* et la fenêtre du même nom apparaît.
   → Les cases correspondant à *Cookies et données de sites* (pour supprimer les connexions à des sites et les préférences des sites) et *Contenu web en cache* (pour supprimer les images, scripts et autres contenus web en cache) devraient être cochés.
4. Cliquez sur *Effacer.*

   Sur l'application

   1. Rendez-vous dans les *Paramètres* > *Gestion des données*
   2. Cliquez sur > *Effacer mes traces*

Si vous utilisez Safari :

1. Dans l'application Safari sur votre Mac, choisissez *Safari* puis *Réglages,* et cliquez sur *Confidentialité.*
2. Cliquez sur *Gérer les données du site web.*
3. Sélectionnez *un ou plusieurs sites web,* puis cliquez sur *Supprimer ou Tout supprimer.*

Sur iPhone, pour effacer vos cookies, mais conserver votre historique,
1. Accédez à *Réglages* > *Safari* > *Avancé* > *Données de site,*
2. Cliquez sur > *Supprimer les données de sites.*

Si vous utilisez Chrome :

1. Sur votre ordinateur, ouvrez Chrome.

   En haut à droite, cliquez sur *Plus* puis sur *Paramètres.*
2. Cliquez sur *Confidentialité et sécurité* puis sur *Cookies et autres données des sites.*
3. Cliquez sur *Voir toutes les données et autorisations des sites* et ensuite, *Effacer toutes les données.*
4. Pour confirmer, cliquez sur *Effacer.*

   Sur l'application

   1. Allez sur les « … »
   2. Cliquez sur *Effacer les données de navigation.*

Revoir ses paramètres de géolocalisation

Toutes les applications n'ont pas besoin de suivre vos déplacements pour fonctionner. Un petit tour dans les paramètres de localisation est donc nécessaire pour vous assurer que vos paramètres sont définis conformément à vos souhaits et non, systématiquement, par toutes les applications qui vous ont demandé l'autorisation

Pour cela, suivez les procédures suivantes :

Sur Android :

1. Accédez à *Applications*
2. Puis à *Permission d'application*
3. Et choisissez *Localisation*

Sur iPhone :

1. Allez dans les *Réglages*
2. Accédez à la section *Confidentialité*
3. Et choisissez *Services de localisation*

À vous de jouer maintenant, choisissez les applications pour lesquelles vous acceptez ou non la localisation !

Nettoyer ses réseaux sociaux

Vous n'assumez pas toutes les photos de vous ? Vous souhaitez limiter leur accès ? Il est l'heure de vérifier ce que l'on peut savoir ou voir de vous sur les réseaux sociaux.

Sur Instagram, TikTok et Facebook :

↪ **Etape 1 :** Passer votre compte en privé si ce n'est pas déjà le cas.

↪ **Etape 2 :** Faites du tri parmi les personnes abonnées à votre compte. Anciennes connaissances, personnes inconnues, il est temps de trier les personnes avec qui vous souhaitez partager votre contenu.

↪ **Etape 3 :** Votre compte a été créé il y a quelques années ? Il est peut-être temps de faire un tour sur vos anciennes publications pour vérifier si vous êtes toujours à l'aise à l'idée de partager toutes ces photos.

↪ **Etape 4 :** Réfléchissez avant de poster un contenu et avant d'accepter une demande d'abonnement.

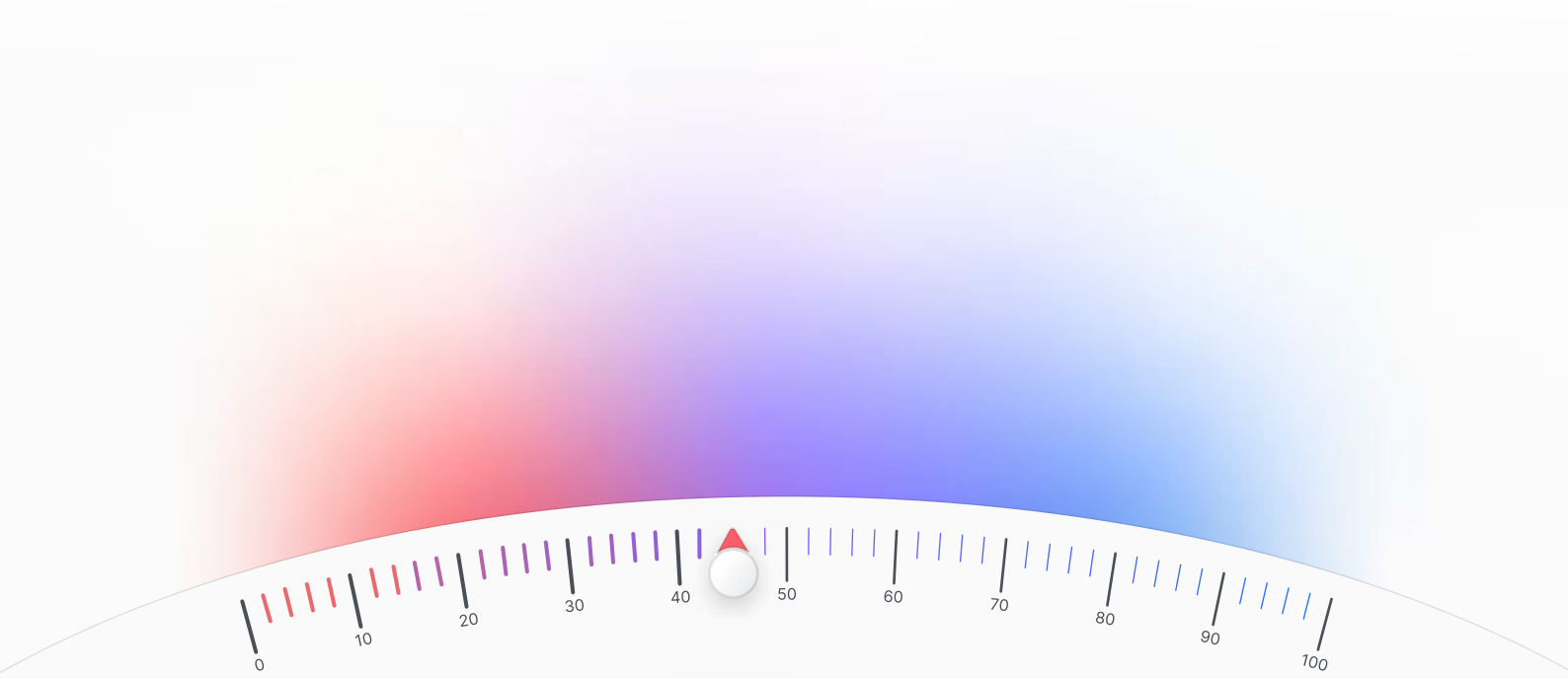
Surveiller sa e-reputation et faire valoir son droit à l'oubli

Publications d'amis, nom associé à des travaux, des événements, des performances sportives, d'anciennes activités… **mais que sait le web sur vous ?**
Pour le savoir, il vous suffit de taper régulièrement sur n'importe quel moteur de recherche, votre prénom et votre nom, votre adresse électronique ou d'autres données que vous pouvez partager en ligne, et qui permettent de vous identifier.

Que faire si un contenu non-souhaité est publié sur Internet ?

Quand cela est possible et s'il ne s'agit pas d'une personne malveillante, vous pouvez demander directement la suppression auprès de la personne à l'origine de la publication.
Si la démarche n'est pas possible ou si la réponse ne vous convient pas, vous pouvez faire valoir votre droit à l'oubli. Le **règlement relatif à la protection des données personnelles (RGPD)** permet à toute personne de demander l'effacement de données la concernant. Pour cela, il faut contacter directement le site internet à l'origine de la publication, en précisant l'URL, les informations à supprimer et la raison qui vous conduit à formuler cette demande. Ces contenus pourront alors être supprimés.

Parallèlement, vous pouvez demander aux moteurs de recherche de ne plus associer un contenu qui peut porter préjudice à votre nom.



3 S'équiper, se protéger

Maintenant que le ménage est fait, voici quelques comportements à adopter.

Activer la localisation uniquement quand l'utilisation du service le nécessite

Toutes les applications, tous les sites que vous visitez n'ont pas besoin de suivre vos déplacements et connaître votre localisation à chaque instant. Prenez le temps de la décision quand le service vous demande l'accès : pourquoi ce site a besoin de suivre mes déplacements ? Est-ce que saisir moi-même ma localisation me permet de bénéficier d'une expérience utilisateur satisfaisante ?
En fonction, adaptez vos réponses !

Utiliser un navigateur et un moteur de recherche plus respectueux de vos données personnelles

Votre porte d'entrée sur le web passe par un navigateur et un moteur de recherche. Alors il faut changer ses habitudes, dès le début de l'expérience.
Pour cela, **choisissez un navigateur et un moteur de recherche plus respectueux de vos données personnelles.** C'est le cas de Firefox en tant que navigateur, ou encore de Brave ou de l'application Qwant.

Pour les moteurs de recherche, testez Qwant (moteur de recherche français) ou encore DuckDuckGo, des moteurs de recherche qui ne font aucune collecte de vos données personnelles et par conséquent, n'en font pas commerce.

Utiliser la navigation privée

La navigation privée est une fonctionnalité disponible sur les navigateurs permettant de **naviguer sans que les données de navigation comme l'historique ou les cookies soient conservées** sur votre appareil.

Avec la navigation privée, une fois votre session fermée, ni votre historique de navigation ni les cookies ne sont sauvegardés. Attention, cela n'empêche pas les sites de déposer des cookies sur votre appareil. Il s'agit donc d'une première étape avant de passer au bloqueur de traqueurs.

Pour naviguer en mode privé, il vous suffit d'aller dans les paramètres de votre navigateur et d'ouvrir une « nouvelle fenêtre de navigation privée ».

Refuser les cookies non essentiels

Si vous n'avez pas de bloqueurs de cookies, les sites vous demanderont la plupart du temps, d'accepter ou de refuser les cookies. Essayez de les refuser systématiquement, ou n'acceptez que ceux essentiels à l'utilisation du service.

Cela est contraignant, c'est pourquoi nous vous suggérons l'étape suivante « installer un bloqueur de traqueurs ».

Installer un bloqueur de traqueurs

Pour naviguer protégé, nous vous conseillons d'installer un **bloqueur de cookies et de traqueurs.** Ce bloqueur permettra de naviguer en toute confidentialité sur le web. Nous vous conseillons d'installer l'extension de navigation **Qwant VIPrivacy,** qui bloquera les cookies et les traqueurs lors de votre navigation, et qui installera Qwant en tant que moteur de recherche par défaut. Vous pouvez également utiliser un outil de protection contre les traqueurs ou **utiliser un service de messagerie qui bloque automatiquement les traqueurs.** La protection de suivi améliorée de **Proton Mail** est activée par défaut pour tous les utilisateurs sur le Web et sur l'application Proton Mail pour iPhone et iPad. Cette fonctionnalité protège votre vie privée contre les tentatives de suivi dans vos emails et vous offre une plus grande tranquillité d'esprit. Une navigation sûre et confidentielle, d'un bout à l'autre de votre recherche !

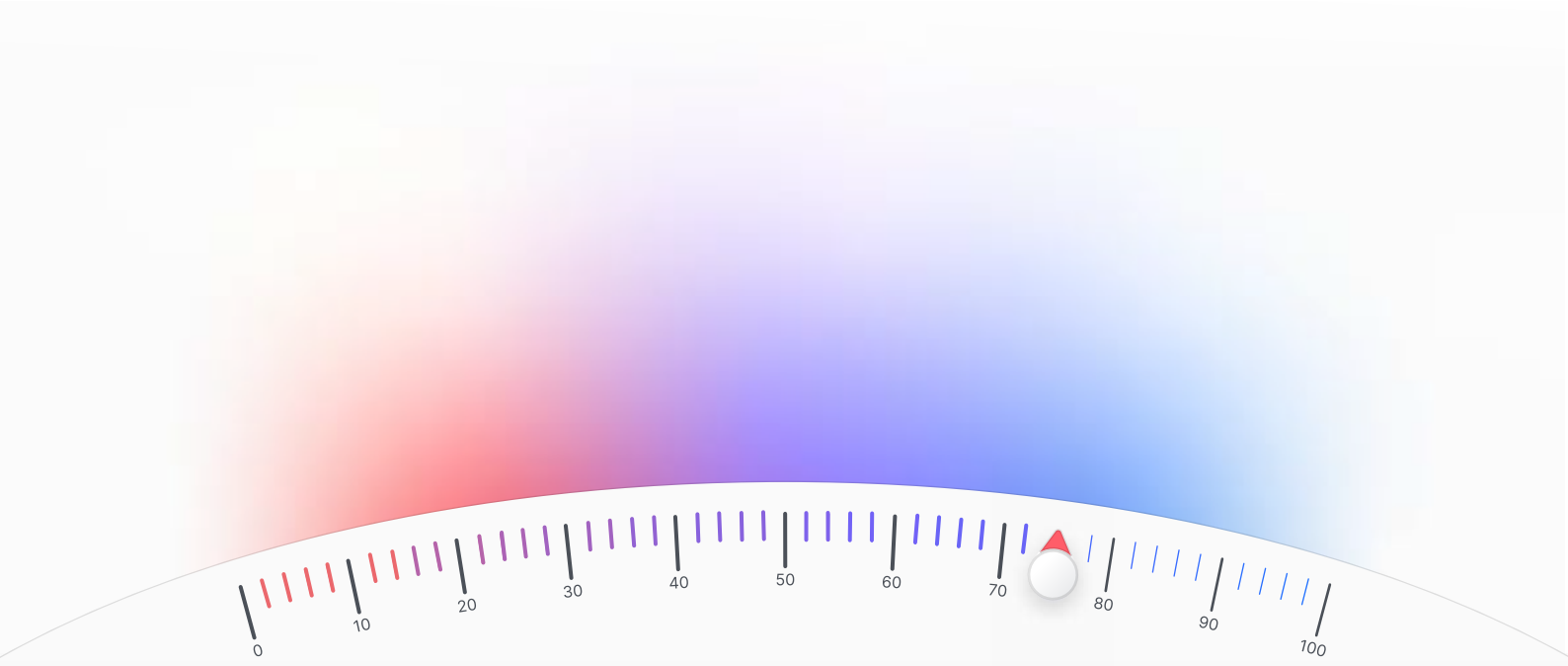
Choisir sa messagerie et sa messagerie instantanée

Afin de sécuriser vos emails, votre calendrier ou encore votre drive, nous vous conseillons de créer un compte sur le site de **Proton.**

Pour votre messagerie instantanée, nous vous recommandons d'installer **Olvid,** la première messagerie privée pour tous, gratuite sur iOS et Android.

Dans les deux cas, la protection de vos données personnelles est une priorité. Dans le cas d'Olvid et de Proton, par exemple, vous n'aurez même pas à communiquer le moindre numéro de téléphone, la moindre adresse, le moindre nom à l'éditeur... Dans le cas d'Olvid, il n'existe même pas de « compte » sur un serveur quelque part sur la planète. Tout simplement parce qu'Olvid ne nécessite **aucune donnée personnelle pour fonctionner !** Vos données (comme votre nom par exemple) ne sont partagées qu'avec les utilisateurs d'Olvid que vous décidez d'inviter.

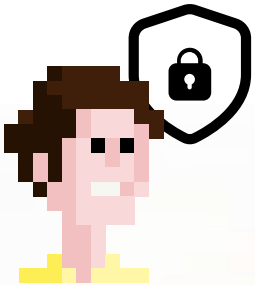
Résultat : Olvid est la seule messagerie qui peut vous garantir que vous ne recevrez jamais de spam. Utiliser des services de messagerie qui garantissent, par conception, qu'ils n'ont pas accès à vos données personnelles est le seul moyen de s'assurer qu'un service qui s'annonce gratuit l'est vraiment. De tels services existent. Pourquoi s'en priver ?



Utiliser un VPN

Un **VPN (Virtual Private Network,** un réseau virtuel privé en français) est un logiciel qui s'installe sur les appareils reliés à Internet et crée **un tunnel sécurisé entre vous, en tant qu'utilisateur, et internet.**

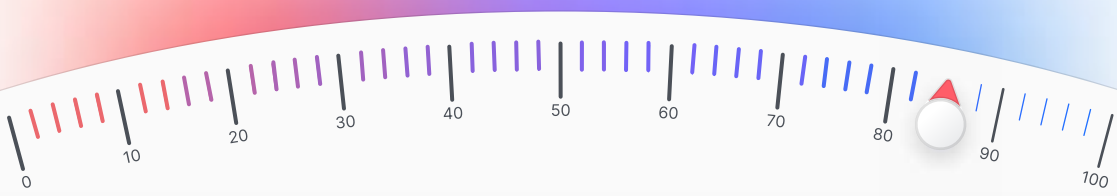
Lorsque vous vous connectez au VPN, l'ensemble de votre trafic internet est redirigé par le serveur VPN avant d'arriver sur le site final. La connexion à un serveur VPN va avoir pour conséquence de cacher votre adresse IP et de la changer au profit de celle du serveur. Finalement, le serveur VPN se place comme un intermédiaire. Ainsi, votre adresse IP d'origine ne sera pas dévoilée au site web que vous consultez et votre vie privée sera respectée.
Voici quelques produits de confiance, que vous pouvez installer aisément sur votre ordinateur ou votre mobile : **Proton VPN,** Express VPN, CyberGhost, Mozilla VPN et NordVPN.



Vous avez désormais toutes les cartes en main pour protéger votre vie privée en ligne : à vous de jouer !

Choisir un smartphone qui n'utilise pas vos données personnelles

Il est fort probable que votre smartphone vous espionne à votre insu. La majorité des smartphones conventionnels collectent un nombre impressionnant de données depuis votre appareil, que ce soit vos contacts, vos usages, vos déplacements, et envoient toutes ces données à des serveurs chez Google, Apple, Facebook et autres géants de la tech.
Les smartphones **Murena** ont été conçus pour proposer une approche différente aux utilisateurs soucieux du respect de leur vie privée et souhaitent se protéger des téléphones avides de données.
Ils se basent sur le système d'exploitation libre "/e/OS" qui est entièrement "déGooglisé" : par défaut, il n'envoie aucune donnée à Google et ni ne collecte vos données d'usage ou votre localisation.
Non seulement /e/OS permet aussi de consulter un « Privacy Score » pour chaque application Android avant de l'installer, il permet aussi de bloquer les pisteurs cachés dans les applications et donc de bloquer le micro-ciblage publicitaire.



Ce guide vous a été proposé par Qwant, Proton, Olvid et Murena ; des acteurs majeurs européens qui proposent des services numériques respectant la vie privée de leurs utilisateurs.

Qwant

À propos de Qwant

Développé en France et leader en Europe, Qwant est le moteur de recherche qui respecte la vie privée de ses utilisateurs en ne collectant aucune donnée personnelle.
Qwant développe sa propre technologie d'indexation du web, conçue pour donner des résultats de recherche impartiaux, exhaustifs et non profilés. Qwant assure ainsi un service de recherche internet avec zéro tracking des recherches, zéro tracking publicitaire et zéro vente de données personnelles.

Au-delà des services Qwant Search, Qwant Maps, offre de cartographie, et Qwant Junior, moteur de recherche dédié aux 6-12 ans, Qwant propose Qwant VIPrivacy, une extension de navigateur permettant de parcourir le web sans subir de tracking publicitaire.
Qwant est disponible sur le web : www.qwant.com, ou grâce aux extensions de navigation. Le navigateur Qwant est disponible sur applications mobiles iOS et Android.
Qwant comptabilise 6 millions d'utilisateurs mensuels.

Qwant ne sait rien sur vous, et ça change tout !
www.qwant.com

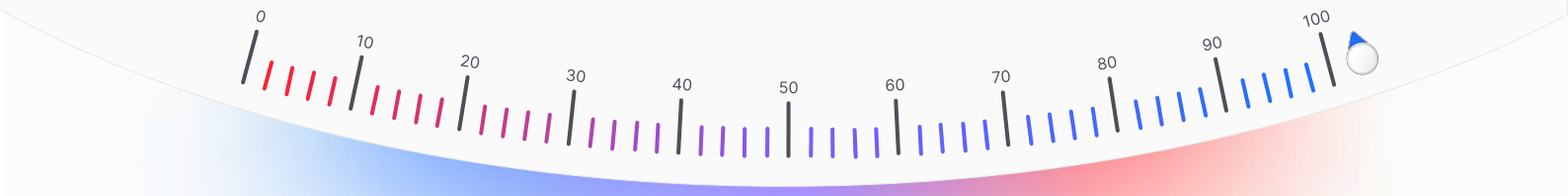
Proton

À propos de Proton

L'entreprise Proton a été fondée en Suisse en 2014 par des scientifiques qui se sont rencontrés à l'Organisation européenne pour la recherche nucléaire (CERN). Notre vision est de créer un internet où la protection de la vie privée est la règle absolue, grâce à un écosystème de services accessibles à tous, partout, tout le temps. Notre premier produit, Proton Mail, est désormais le plus grand service de messagerie chiffrée au monde. Les produits qui ont suivi, Proton VPN, Proton Calendar et Proton Drive s'appuient sur le même chiffrement de bout-en-bout qui permet à nos utilisateurs de contrôler totalement comment et avec qui leurs données sont partagées.

Nos produits sont open source, développés par une équipe de 400 personnes et soutenus par une communauté active dans plus de 180 pays. Aujourd'hui, Proton rend la protection de la vie privée accessible à tous avec plus de 70 millions de comptes utilisateurs, qu'il s'agisse de journalistes, de certaines des plus grandes organisations mondiales ou de personnes du monde entier.

https://proton.me/fr



À propos d'Olvid

Olvid est la première messagerie instantanée privée pour tous, disponible gratuitement pour iOS et Android.

Outre le chiffrement de bout en bout systématique de toutes vos communications, Olvid garantit une authentification de bout en bout de tous vos interlocuteurs. Cela vous protège de toute forme de spam et vous garantit que seuls les utilisateurs que vous choisissez pourront échanger avec vous. Comme Olvid ne nécessite aucune donnée personnelle pour fonctionner (et ne vous en demande donc aucune), elle est fondamentalement gratuite.

Constituez des groupes avec votre famille, vos proches, vos collaborateurs clés. Nul besoin de tisser un réseau virtuel de 5000 « amis ». Olvid a été conçue pour être le meilleur endroit où échanger sur les sujets qui importent, avec ceux qui comptent.

https://olvid.io

À propos de Murena

Fondée en 2018 par le vétéran de l'open source Gaël Duval, fondateur de "Mandrake Linux", Murena est une startup engagée dans la protection de la vie privée avec des produits et des services transparents et de qualité qui aident les citoyens à échapper à la surveillance numérique.

Chez Murena, nous sommes convaincus que les technologies open source sont le seul moyen de tenir cette promesse, car elles restent entièrement auditable pour une transparence maximale. Murena conçoit /e/OS, un système d'exploitation mobile avec des applications préinstallées, et Murena Cloud, un ensemble de services en ligne pour accompagner /e/OS.

Murena développe également les téléphones Murena, avec /e/OS préinstallé, disponibles dès aujourd'hui, livrés aux États-Unis, au Canada, en Europe, au Royaume-Uni et en Suisse.

https://murena.com

Contact : dataprivacyday@qwant.net

Guide Comment protéger votre vie privée sur Internet