

PROTEGER SES DONNEES PERSONNELLES



LES DONNEES PERSONNELLES, DE QUOI S'AGIT-IL ?

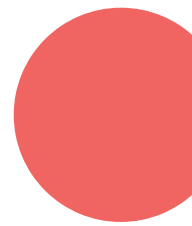
Les données personnelles sont des informations relatives à une personne et permettant de l'identifier. Ces données sont un enjeu important dans l'économie du web puisque de nombreux services gratuits se sont développés à partir du stockage et du traitement, c'est-à-dire de l'exploitation commerciale, de ces données. Ainsi, certaines des plus grandes entreprises du web comme Google et Facebook ont basé leur modèle économique sur la collecte et la vente des données personnelles de leurs utilisateurs. Ainsi, toutes les informations remplies par l'utilisateur lors d'une inscription à un service est une donnée personnelle. Cela peut donc aller de la date de naissance au numéro de carte bancaire.

POURQUOI PROTEGER SES DONNEES PERSONNELLES ?

Si le traitement des données personnelles par les entreprises du web peut avoir des effets positifs, comme l'amélioration des performances des algorithmes de recherche, il peut aussi avoir des effets négatifs pour les utilisateurs :

- Création de « bulles informationnelles ». En collectant les données, les entreprises peuvent en déduire les intérêts des utilisateurs et leur proposer des services en accord avec ceux-ci. Les services de recherche collectant les données proposent donc le même type d'informations, ce qui nuit à la diversité de l'information
- Réception par l'utilisateur de publicités ciblées
- Absence de contrôle de l'utilisateur sur les données conservées par l'entreprise et sur leur localisation.

PROTEGER SES DONNEES PERSONNELLES



QUELQUES ALTERNATIVES

DES MOTEURS DE RECHERCHES QUI N'ENREGISTRENT PAS LES DONNEES



Qwant : <https://www.qwant.com/>



ixquick/startpage : <https://www.startpage.com/>



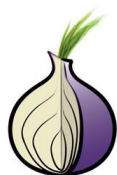
DuckDuckGo

Duckduckgo : <https://duckduckgo.com/>

DES NAVIGATEURS WEB QUI NE COLLECTENT PAS LES DONNEES DE NAVIGATION



Mozilla firefox ne prélève pas de données, toutefois il est possible d'intégrer des applications qui elles peuvent collecter vos données personnelles. Attention donc aux extensions que vous ajoutez : <https://www.mozilla.org/fr/firefox/new/>



Tor browser permet de naviguer sur le réseau Tor. Ce dernier est un réseau virtuel parallèle au réseau internet. Il permet de contourner la surveillance en fournissant une adresse IP différente. Pour être efficace, il faut donc naviguer sans se connecter à des services habituels qui prélèvent les données (comptes mail, de réseaux sociaux, de commerce en ligne, ...) : <https://www.torproject.org/>

PROTEGER SES DONNEES PERSONNELLES

LE SAVIEZ-VOUS ?



NE PAS CONFONDRE DONNEES PERSONNELLES ET DONNEES SENSIBLES

Attention à ne pas confondre les données personnelles avec les données sensibles permettant d'identifier les orientations d'une personne (ex : orientations religieuses, politiques, sexuelles, ...). En effet, la collecte de ces dernières est interdite sauf dans le cadre d'une recherche scientifique.

RENFORCER UN MOT DE PASSE FACILEMENT

Au-delà du traitement des données par les entreprises du web, la protection des données passe aussi par la protection de ses comptes personnels par des mots de passe forts afin d'éviter des intrusions malveillantes. Pour renforcer un mot de passe, la Commission Nationale de l'Informatique et des Libertés (CNIL) préconise qu'il doit contenir au minimum :

- Un nombre,
- Une majuscule,
- Un caractère spécial ou un signe de ponctuation,
- Une douzaine de caractères.

La CNIL propose une méthode mnémotechnique pour créer un mot de passe fiable en utilisant les premières lettres des mots d'une phrase retenue ainsi que la ponctuation, les chiffres et les majuscules qu'elle contient. Ainsi, à partir de la phrase : « Le code postal de la ville de La Riche est 37520 », il est possible de générer selon ce principe le mot de passe suivant : « LcpdlvdLRe37520 » répondant aux critères de sûreté. Pour simplifier cette démarche, la CNIL propose un générateur dans lequel il suffit de rentrer la phrase de son choix : <https://www.cnil.fr/fr/generer-un-mot-de-passe-solide>

Il existe aussi des générateurs de mots de passe afin de créer et de mémoriser des mots de passe sécurisés tels que Keepass, Zenyway ou encore Passwordsafe. La CNIL propose un tutoriel vidéo pour l'utilisation de Keepass, logiciel libre et gratuit qui a passé avec succès la certification de sécurité de premier niveau de l'Agence Nationale de Sécurité des Systèmes d'Information : <https://youtu.be/XTnDKJl1zOQ>

PROTEGER SES DONNEES PERSONNELLES

LE SAVIEZ-VOUS ?



SECURISER SA BOITE MAIL, C'EST ESSENTIEL !



L'adresse mail est souvent utilisée pour l'enregistrement et la création d'espace personnels pour accéder à des services sur internet. Elle permet souvent l'identification sur ces services ainsi que la réception de liens permettant la réinitialisation du mot de passe pour y accéder. Ainsi, plus que tout autre service il est primordial de protéger l'accès à sa boîte mail personnelle par un mot de passe unique et puissant remplissant les critères énoncés auparavant.

QUELQUES SITES UTILES

- Le site de la CNIL : <https://www.cnil.fr/>
- La quadrature du net : <https://www.laquadrature.net/fr/>
- Cartographie de la CNIL des outils permettant de protéger ses données de navigations sr le web : <https://linc.cnil.fr/fr/une-cartographie-des-outils-et-pratiques-de-protection-de-la-vie-privee>