5 EXTENSIONS POUR PROTÉGER MA VIE PRIVÉE

Crédit : Numérique & moi

87% DES FRANÇAIS SE DÉCLARENT AUJOURD'HUI SENSIBLES À L'ENJEU DE LA PROTECTION DES DONNÉES.

Sources : cnil.fr, rapport d'activité 2019.

Une **donnée personnelle** est une **information** me concernant : mon nom, mon prénom, ma date de naissance, mais aussi mon numéro de téléphone, mon adresse mail, une publication, une recherche sur le web, etc.

Les extensions qui suivent ne suffisent pas à protéger ma vie privée, elles sont un complément à ma vigilance et à d'autres outils comme : les paramètres de confidentialité, la navigation privée, les VPN, les mots de passe, ou encore les pseudonymes.

LA CNIL

est l'autorité administrative indépendante chargée de faire respecter, notamment, mon **droit à une vie privée**. Elle met également à disposition de nombreuses **ressources** et **informations pratiques** sur son site, notamment des **modèles de courrier** pour faire valoir mes droits.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

www.cnil.fr

AJOUTER DES EXTENSIONS

Le navigateur web Firefox* permet d'ajouter de nombreuses extensions pour améliorer la qualité de ma navigation et notamment la protection de ma vie privée. Elles ne sont pas payantes, mais **faire un don** permet de péreniser leur existence et leur amélioration.

Pour ajouter des extensions et faire des dons :
www.addons.mozilla.org/fr

***Pourquoi Firefox ?** Il existe de nombreux navigateurs web qui autorisent l'installation d'extension (cf. Chrome via le chrome web store) et qui protègent la vie privée (cf. TOR). Tous ont des avantages et des inconvénients. Firefox est facile à utiliser et surtout il appartient à une **fondation à but non lucratif** qui porte des valeurs plus **éthiques** que certains de ses concurrents.

1. BLOQUER LES PUBS

uBlock Origin est une extension qui bloque les publicités et les pisteurs*.

2. BLOQUER LES TRACEURS

Privacy Badger est une extension qui bloque les sites tiers qui cherchent à collecter des informations sur les internautes pendant leur navigation sur le web.

***Les cookies sont régulièrement comparés à des "traceurs", mais à quoi servent-ils ?** Depuis l'entrée en vigueur du Règlement Général sur la Protection des Données (**RGPD**) en **2018**, les sites web doivent demander le consentement de leurs visiteurs avant de déposer des cookies sur leurs équipements. **Ces messages d'avertissements existent donc pour nous protéger**. Les cookies permettent notamment aux sites web de générer des recettes financières grâce à la publicité et donc de rester accessibles gratuitement. L'inconvénient est que cette gratuité se fait au détriment de la vie privée.

3. SUPPRIMER LES INTERMÉDIAIRES

Decentraleyes est une extension qui supprime les intermédiaires entre moi et le site web auquel je veux accéder. Cela permet également de naviguer plus rapidement.

Crédit : Numérique & moi

4. CONTENIR FACEBOOK*

Facebook Container est une extension qui permet d'isoler Facebook pour éviter que le réseau et ses pisteurs n'espionnent mes faits et gestes sur le web.

*L'entreprise Facebook propriétaire d'Instagram, WhatsApp, Messenger, ou encore Oculus VR s'appelle désormais "Meta". Ce mot vient de "métaverse" (méta univers), c'est-à-dire un monde virtuel.

Meta

5. CHIFFRER SA NAVIGATION

HTTPS Everywhere est une extension qui permet d'activer le chiffrement HTTPS* sur les sites le prenant en charge.

*__HTTPS__ (Hyper Text Transfer Protocol Secure) est un **protocole de sécurité** qui permet de c**hiffrer** les communications entre le site web et l'internaute. Son rôle est de protéger la confidentialité et le contenu des données échangées entre mon équipement et le serveur. En revanche, **ça seule présence ne doit pas me dispenser de rester vigilant** sur les sites web que je visite.

PRÊT.E À VOUS PROTÉGER ?

POUR ALLER PLUS LOIN :
www.cnil.fr
www.foundation.mozilla.org
www.idfrights.org

Edward Snowden, Mémoires vives, Seuil, 2019.
Anne-Sophie Jacques et Maxime Guedj, Declic, les arènes, 2020.

@NUMERIQUE_ET_MOI