

# Se protéger sur Internet - Sécurisé sa navigation

## Introduction

## Quelques définitions

### Pistage

“ Action de guetter quelqu'un et le suivre sans se faire voir.

Larousse

“ Moyen mise en place par divers acteurs [du numérique] pour suivre la navigation de l'internaute à son insu.

Le Poisson Libre

Par définition, le pisteur fait le nécessaire pour que le pisté ne soit pas conscient du pistage !

### Web

“ Le World Wide Web (/ˌwɜːld waɪd 'web/ ; littéralement la « toile (d'araignée) mondiale », abrégé www ou le Web), la toile mondiale ou la toile, est un système hypertexte public fonctionnant sur Internet. Le Web permet de consulter, avec un navigateur, des pages accessibles sur des sites. L'image de la toile d'araignée vient des hyperliens qui lient les pages web entre elles.

Le Web est donc une application du réseau Internet et probablement sont utilisation la plus courante. Par abus de langage, il est courant d'utiliser le mot Internet pour en réalité mentionner le Web.

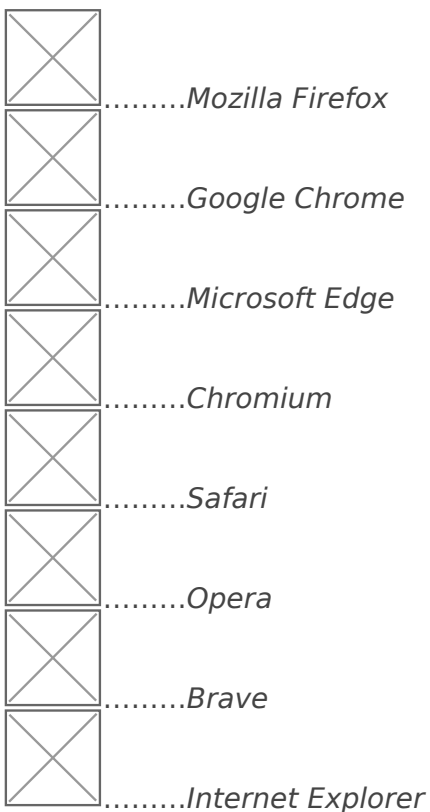
Il convient d'utiliser un navigateur afin de consulter les pages du Web.

## Navigateur

Le navigateur est un logiciel (alias application ou programme) qui permet d'afficher des pages Web.

Techniquement, c'est un client HTTP qui traite les informations reçues des serveurs HTTP afin de présenter un rendu à l'utilisateur.

Il existe une multitude de navigateurs, souvent reconnus par leurs logos.



### “ Attention :

Microsoft Internet Explorer n'a plus de mise à jour de sécurité, l'entreprise Microsoft elle-même déconseille de l'utiliser.

Les navigateurs Web sont majoritairement gratuits mais cela n'est pas systématique.

Ils peuvent être open-source ou propriétaires. C'est-à-dire que le concepteur du navigateur fait le choix de jouer la transparence sur le code informatique nécessaire à l'exécution du programme ou pas. Ce choix est souvent dicté par le modèle économique de l'entreprise derrière la conception du navigateur.

# Le navigateur

## Mozilla Firefox

Mozilla Firefox est un navigateur Web souvent conseillé :

- Gratuit ;
- Open-source ;
- Fiable ;
- Sécurisé ;
- Performant ;
- Extensible...

Il est développé par la [fondation Mozilla](#), un organisme à but non lucratif établi en juillet 2003 qui œuvre pour un Internet libre et neutre.

Son modèle économique repose sur les dons, les subventions. Bien qu'il ait un contrat avec Google pour être le moteur de recherche par défaut, il est simple de le remplacer par un autre plus respectueux de la vie privée (Qwant, DuckDuckGo, etc.).

## Les extensions

“ Une extension de navigateur est un petit module logiciel permettant de personnaliser un navigateur web. Les navigateurs autorisent généralement toute une série d'extensions, notamment des modifications de l'interface utilisateur, la gestion des cookies, le blocage des publicités et la personnalisation des scripts et du style des pages Web.

[Wikipédia \(traduction de l'anglais\)](#)

Les extensions permettent donc d'ajouter des fonctionnalités supplémentaires à un logiciel. On retrouve également les termes anglais : « add-on », « plugins ».

Plus particulièrement, les extensions de Mozilla Firefox sont regroupés sur leur site [addons.mozilla.org](https://addons.mozilla.org). Toute personne ayant des compétences en code informatique peut développer

et y déposer son extension. C'est pourquoi un système de badge permet d'identifier les modules recommandés, vérifiés, créés par Firefox ou les autres, c'est-à-dire sans badge.

## Les cookies

“ Les cookies HTTP (aussi nommés cookies Web, cookies Internet, cookies de navigation, témoin de connexion ou simplement cookies) est un petit fichier texte envoyé par le serveur HTTP (qui envoie la page Web) au client HTTP (l'ordinateur de l'utilisateur).

Lors de la prochaine connexion, le client HTTP renverra au serveur le(s) cookie(s) précédemment reçu(s). Ainsi le serveur pourra automatiquement reconnaître l'utilisateur.

Wikipédia (traduction de l'anglais)

Les cookies permettent entre autres de :

- conserver le panier d'achat lors de la navigation sur un site d'e-commerce ;
- mémoriser les actions réalisées sur un site (pages visitées, boutons cliqués, articles lus...) ;
- conserver la personnalisation souhaitée sur un site (mode sombre par exemple) ;
- mémoriser les coordonnées de l'utilisateur ;
- conserver l'authentification de connexion à un site Web.

Normalement, les cookies déposés depuis un site Web ne sont accessibles que depuis un site ayant le même nom de domaine (pour simplifier : une adresse Web ayant la même fin). Cependant, les sites ont des accords avec d'autres sites afin de déposer des « cookies tiers ». Les plus répandus sont ceux de Google, Facebook ou leurs filiales. Ainsi les cookies permettent également de pister l'utilisateur à travers sa navigation sur différents site Web.

## Les scripts

“ Petits programmes présents sur les sites visités.

Peuvent servir à :

- donner de l'interactivité à la page ;
- analyser des actions de l'internaute ;
- mesurer l'affluence ;
- afficher la publicité ;
- afficher les boutons de partage.

Les scripts sont des instructions sous forme de code informatique. Ces instructions sont directement interprétées par les navigateurs Web. Elles sont de plus en plus nécessaires au rendu visuel et à l'interactivité des pages Web, de nombreux sites ne sont pas en mesure de s'afficher sans ces scripts.

Cependant, les scripts sont massivement utilisés pour pister les usagers et connaître leurs habitudes de navigation Web.

# Installation et configuration de Mozilla Firefox

## Installation de Mozilla Firefox

### Téléchargement

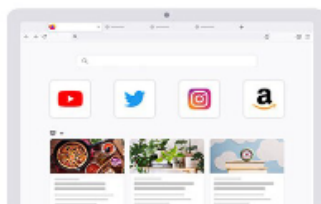
Comme toute application que l'on souhaite installer, il est vivement conseillé de se rendre sur le site officiel, ici : <https://www.mozilla.org/fr/firefox/browsers>. Et ainsi accéder directement à la page des téléchargements de Mozilla Firefox.

#### “ Astuce

Pour trouver le site officiel d'une application, il est possible de se rendre sur le site de Wikipédia. Généralement, un encadré sur la partie latérale droite présente des informations, le dernier élément correspond souvent au site Web.

# Installez les navigateurs qui respectent votre vie privée — et qui l'ont toujours fait

Obtenez la protection de la vie privée qui vous est due. La protection renforcée contre le pistage est automatique pour chaque navigateur Firefox.



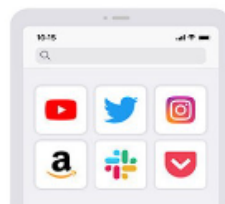
## Ordinateur

La navigation privée prise au sérieux. Firefox empêche automatiquement plus de 2 000 traçage en ligne de collecter des informations sur ce que vous faites en ligne.

Télécharger pour l'ordinateur



[En savoir plus](#)



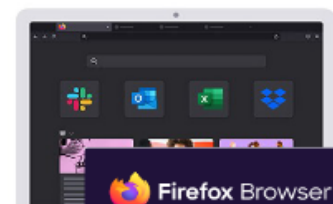
## Mobile

Gardez le même niveau de protection de votre vie privée, ainsi que vos mots de passe, historique, onglets ouverts, etc — toujours avec vous, peu importe où vous êtes.

Télécharger pour mobile



[En savoir plus](#)

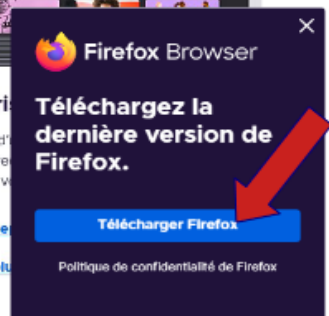


## Entreprise

Bénéficiez d'une protection renforcée de vos données avec Firefox pour entreprise.

[Offres Entreprise](#)

[En savoir plus](#)



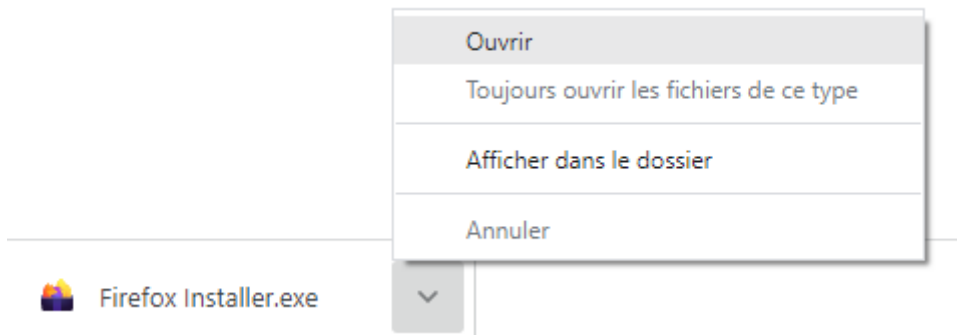
Afin de télécharger le programme d'installation, on clique sur le bouton « Télécharger pour l'ordinateur » à gauche ou bien sur le bouton « Télécharger Firefox » dans la fenêtre apparue par le côté droit. Le site reconduit vers une nouvelle page, suivant le navigateur actuellement utilisé soit il propose d'enregistrer le fichier d'installation, soit il le télécharge directement.

## Installation

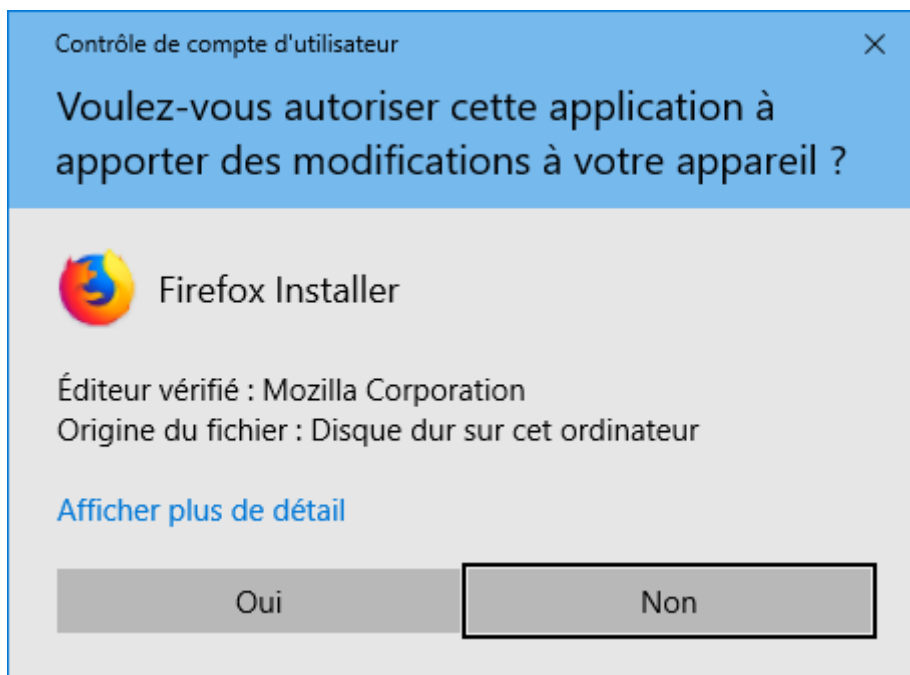
Par défaut, le fichier d'installation est maintenant dans le dossier « Téléchargements » (peut aussi être nommé « Downloads »).

Depuis le navigateur Chrome, il est possible de lancer directement le programme d'installation en cliquant sur « Firefox Installer.exe » en bas à droite.

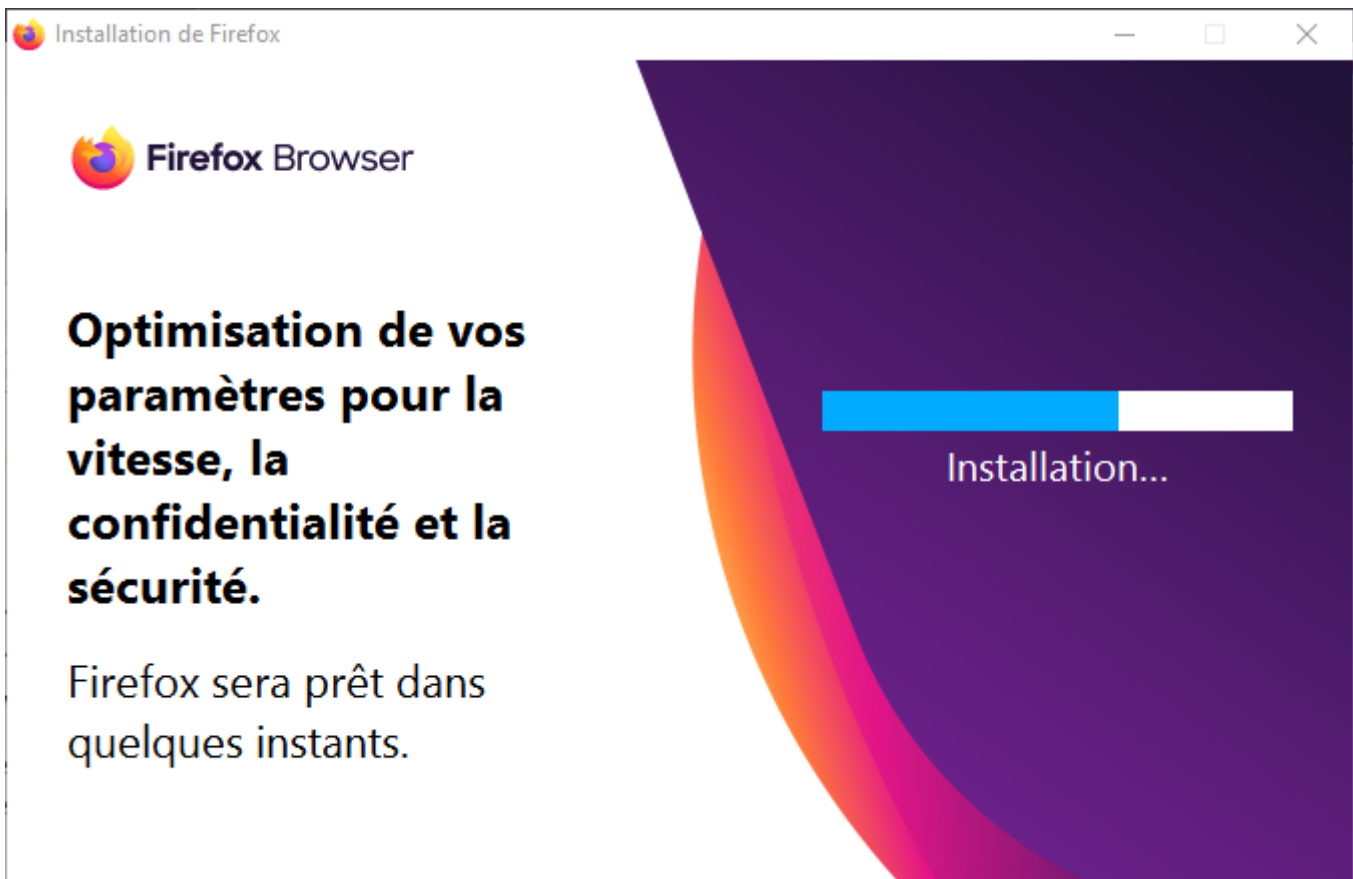
Ou de cliquer sur le chevron vers le haut puis cliquer sur ouvrir.



Ensuite autoriser le programme à apporter des modifications à votre installation de Microsoft Windows en répondant « Oui ».

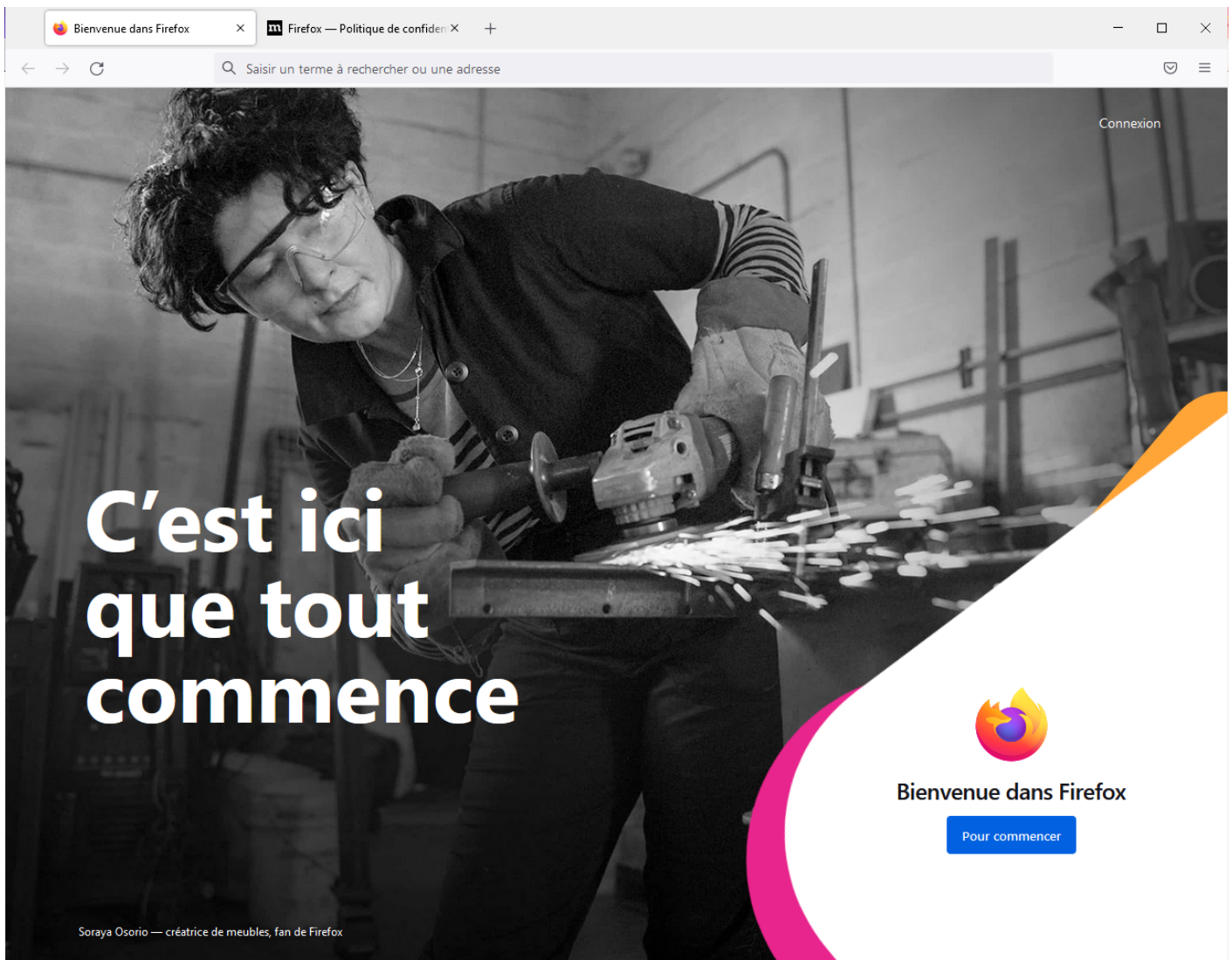


Le programme d'installation va alors continuer.

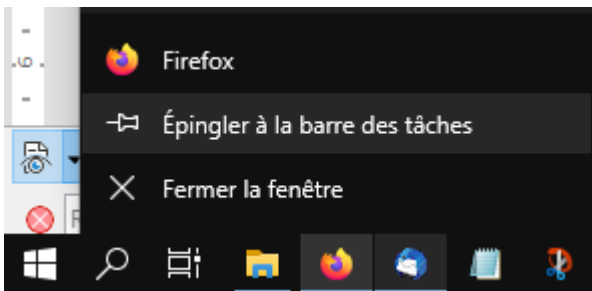


Quand l'installation est terminée, Firefox s'ouvre.





Un raccourci sur le bureau a également dû être créé. Il est aussi possible d'épingler le programme dans la barre des tâches en faisant un clic droit puis choisir « Épingler à la barre des tâches ».



# Configuration de Mozilla Firefox

## Le menu « Paramètres »

Afin de procéder à quelques réglages, il convient d'accéder au menu des réglages, nommé « Paramètres ». Pour ce faire, il suffit de cliquer sur l'icône représentant trois barres horizontales (≡) en haut tout à droite (sous la croix permettant de fermer la fenêtre), puis de cliquer sur

« Paramètres ».

L'onglet ouvert présente, par défaut, la page des paramètres généraux.

Rechercher dans les paramètres

Général

Accueil

Recherche

Vie privée et sécurité

Synchronisation

Extensions et thèmes

Assistance de Firefox

Général

Démarrage

Ouvrir les fenêtres et onglets précédents

Toujours vérifier que Firefox est votre navigateur par défaut

Firefox est votre navigateur par défaut

Onglets

Ctrl+Tab fait défiler vos onglets en les classant selon leur dernière utilisation

Ouvrir les liens dans des onglets au lieu de nouvelles fenêtres

À l'ouverture d'un lien, d'une image ou d'un média dans un nouvel onglet, basculer vers celui-ci immédiatement

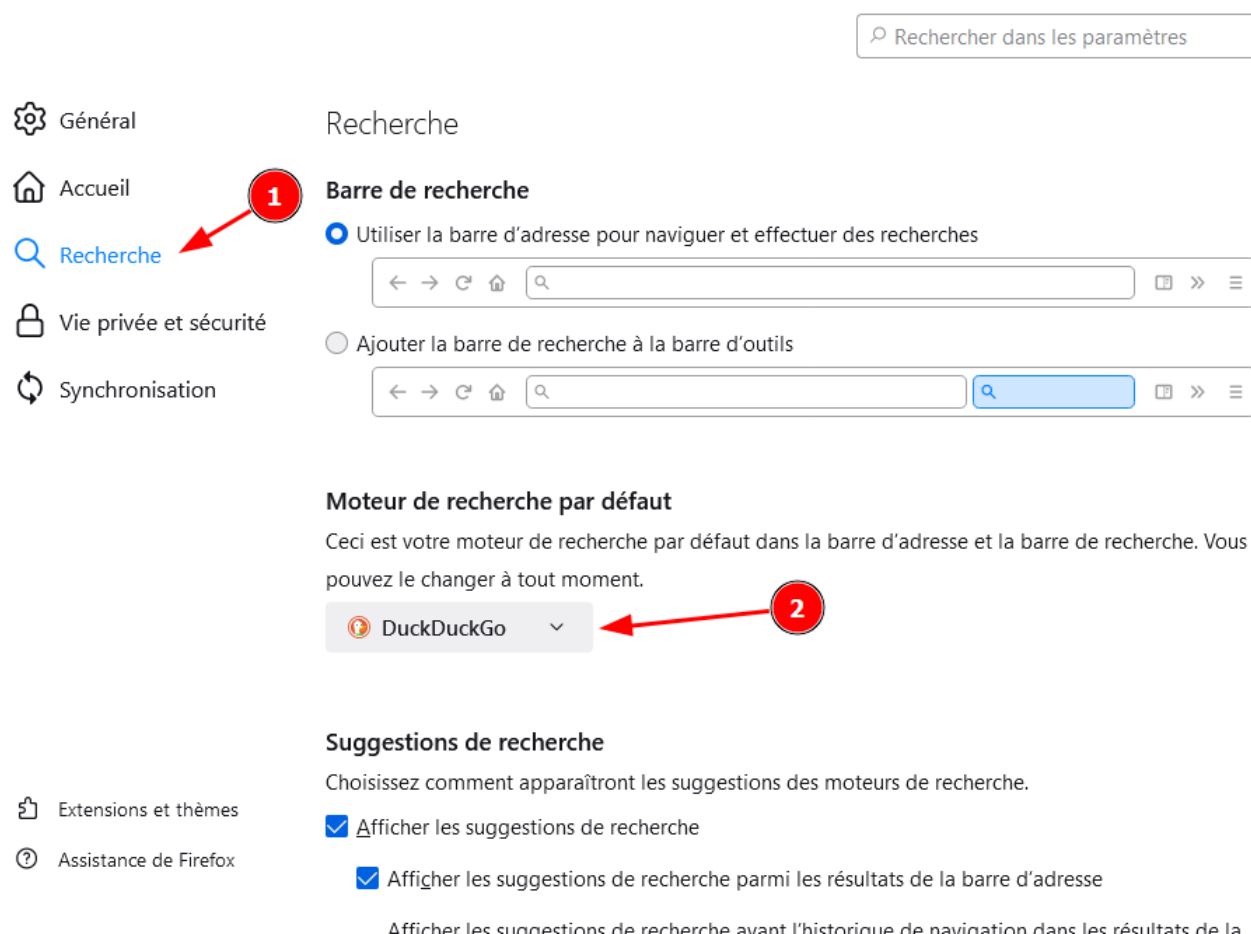
Avertir lors de la fermeture de plusieurs onglets

Afficher les aperçus d'onglets dans la barre des tâches de Windows

## Le moteur de recherche par défaut

Comme mentionné précédemment, Mozilla Firefox reçoit des financements de Google afin d'être le moteur de recherche par défaut. Afin de sécuriser sa confidentialité, il convient de le changer.

Se rendre dans la partie « Recherche », puis déplier le menu déroulant mentionnant le moteur de recherche par défaut (actuellement Google) afin de sélectionner Qwant ou DuckDuckGo.



Qwant (français) et DuckDuckGo (américain) sont des moteurs de recherche alternatif à Google respectueux de la vie privée. Leur modèle économique ne repose pas sur la revente de nos données personnels à des fins publicitaires.

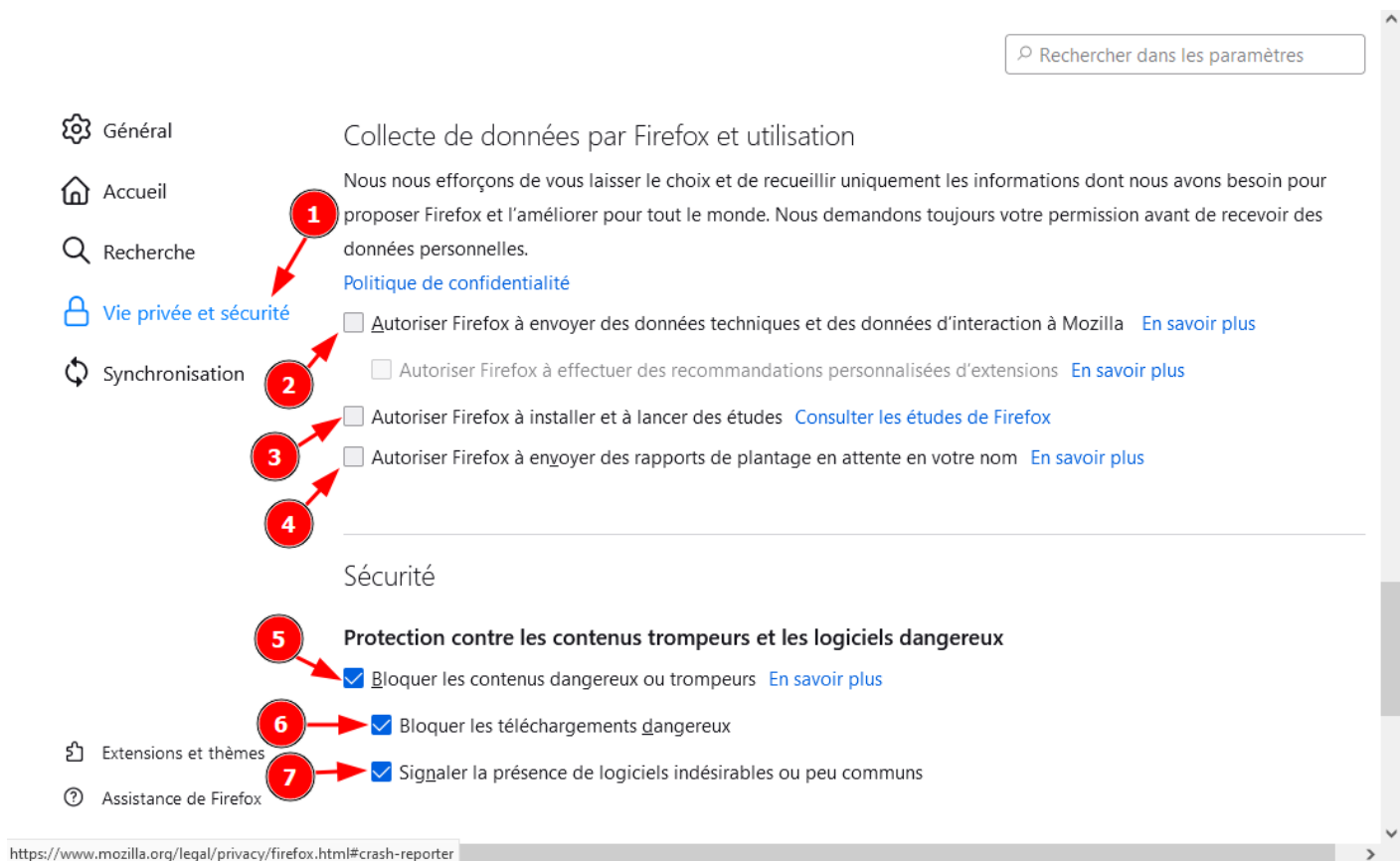
## Vie privée et sécurité

Se rendre dans la partie « Vie privée et sécurité », puis descendre vers le bas de la page afin de personnaliser les options des parties « Collecte de données par Firefox et utilisation » et « Sécurité ».

Bien que Mozilla Firefox soit respectueux de la vie privée, il collecte malgré tout des données afin d'avoir des retours d'utilisation sur leur logiciel. Davantage de détails sont présentés sur [leur page de politique de confidentialité](#).

Par défaut, Mozilla Firefox est autorisé à envoyer des données techniques à la fondation Mozilla, il est souhaitable de décocher toutes les cases de la partie « Collecte de données par Firefox et utilisation » (points 2, 3 et 4 de l'illustration ci-dessous).

Enfin, s'assurer que les trois options « Protection contre les contenus trompeurs et les logiciels dangereux » soient activées (points 5, 6 et 7 de l'illustration ci-dessous). Le cas échéant, il convient de les activer.



## Le mode de navigation privée

“ [...] Le mode de navigation privée n’empêche pas le pistage. Ce mode a pour unique but de permettre de naviguer sur le Web sans que les données de navigation (comme l’historique ou les identifiants et mots de passes) soient conservés lors du prochain lancement du navigateur. Il s’agit de ne pas laisser, dans le navigateur, de traces qu’un utilisateur postérieur pourrait découvrir (par exemple, si vous souhaitez acheter en ligne une surprise pour votre conjoint avec qui vous partagez votre ordinateur). Ouvrir une nouvelle fenêtre de navigation privée n’empêche pas le partage d’informations avec les autres sites : vos informations et données personnelles sont toujours accessibles par les sites web, elles ne le sont plus sur votre ordinateur.

Théo Barnouin pour l’EPN Salle des Rancy.

Entre d'autres termes, la navigation est privée pour l'ordinateur de l'utilisateur mais elle n'est en rien privée pour les sites consultés. **Cela n'empêche pas du tout les traceurs d'opérer.**

## Les extensions

# « Ublock Origin »

## Explication

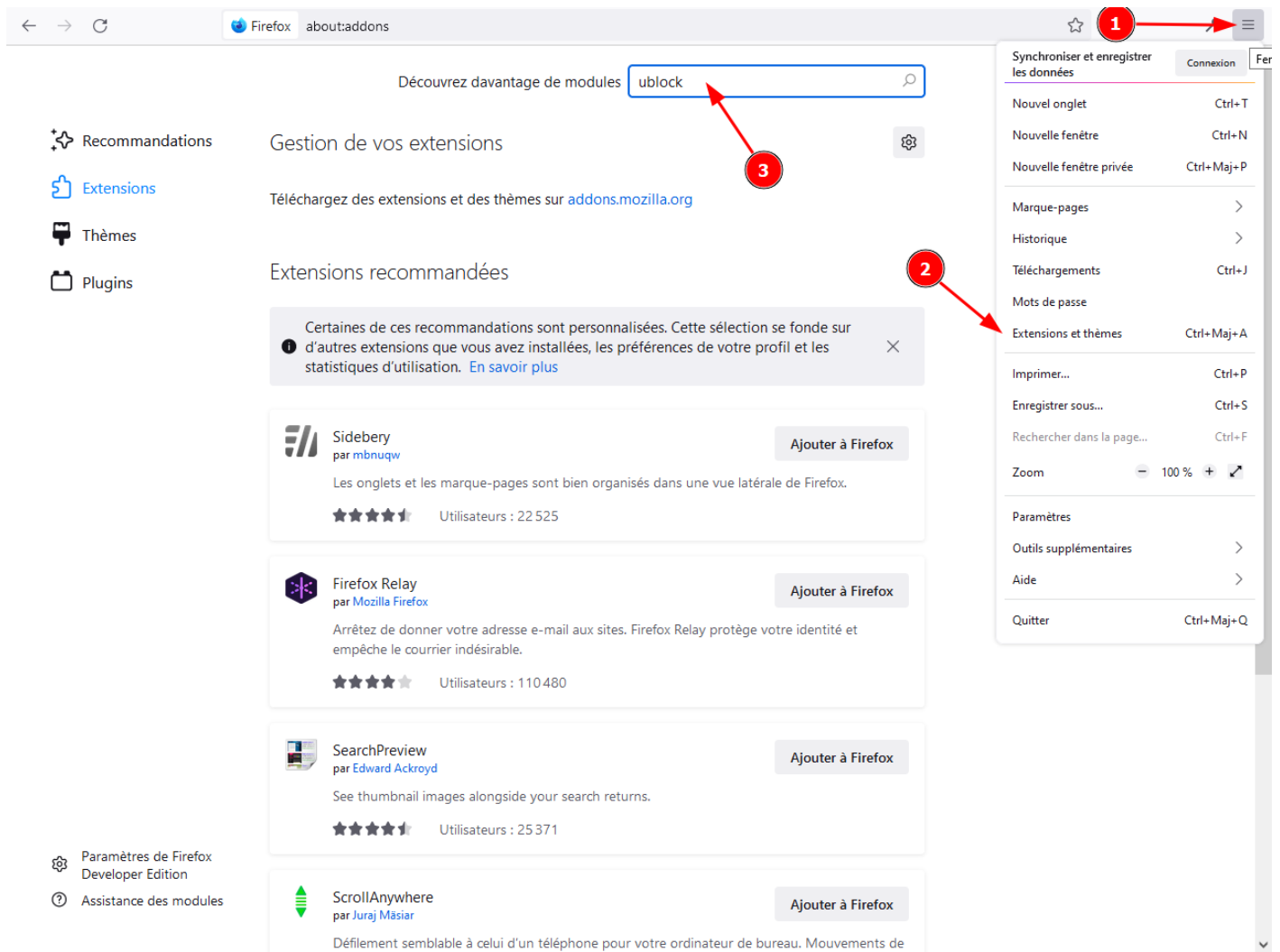
“ Ublock [Origin] est une extension qui bloque les publicités et les pisteurs [...].

uBlock Origin - Adoptez cette extension pour  Firefox

Cette extension est gratuite et open-source (en clair : elle n’a rien à cacher). Son but est d’empêcher le site de charger des données nuisant à la navigation : les publicités et les données de traçage. Bien qu’elle ne puisse pas être efficace à 100 %, elle est très performante.

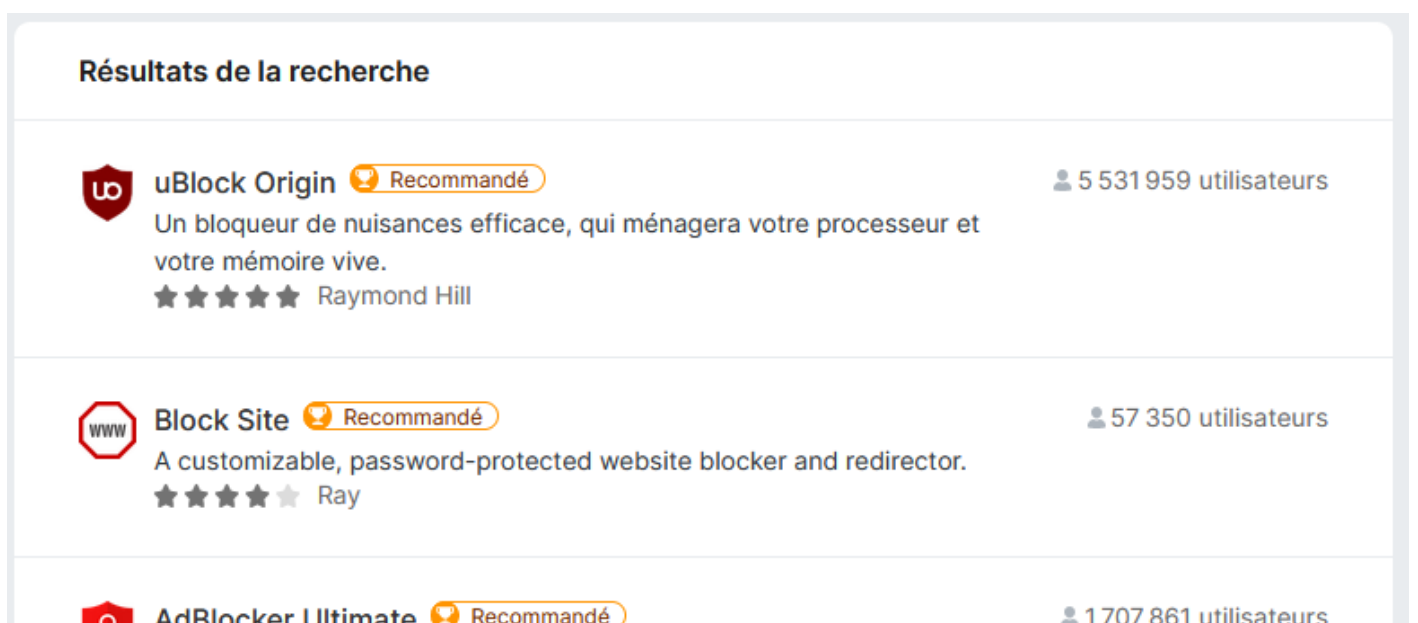
## Installation

Afin de procéder à l’installation de cette extension, il faut se rendre dans le gestionnaire des extensions : cliquer sur l’icône représentant trois barres horizontales (≡) en haut tout à droite (sous la croix permettant de fermer la fenêtre), puis de cliquer sur « Extensions et thèmes ». Ensuite il faut entrer le nom de l’extension voulue (ici « ublock ») dans le champ de recherche, puis valider.



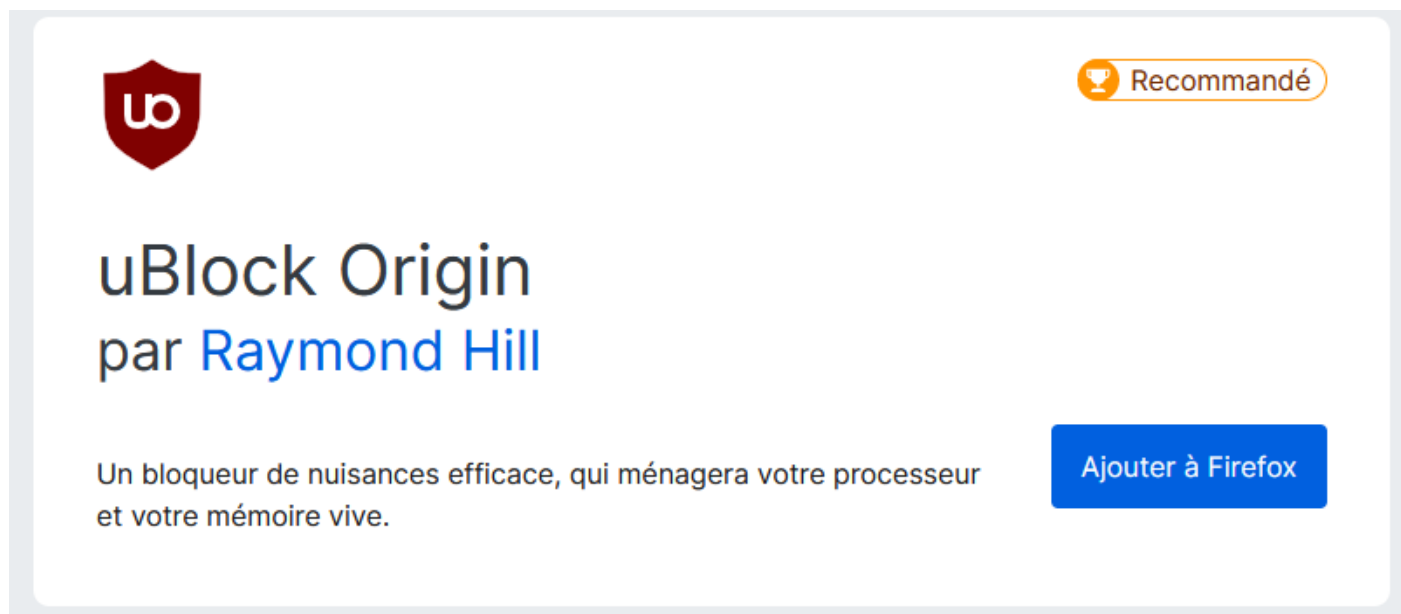
Il est aussi possible d'accéder au catalogue des extensions depuis l'adresse suivante : <https://addons.mozilla.org/fr/firefox>.

Le navigateur va alors ouvrir un nouvel onglet présentant le résultat de la recherche.

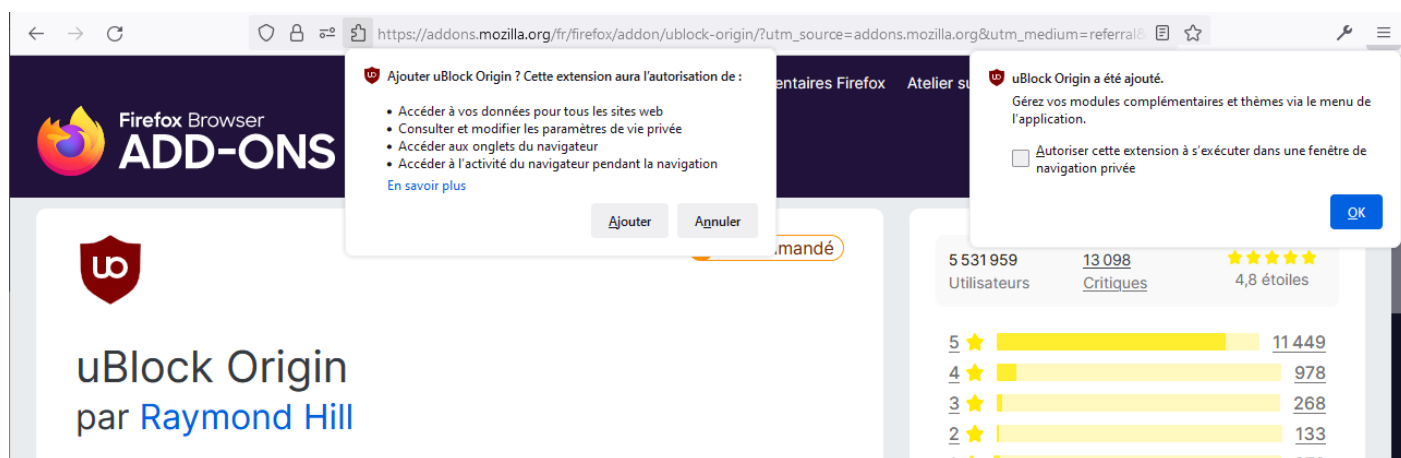


Normalement le premier résultat de la recherche correspond à l'extension souhaitée. On peut noter la présence du badge « Recommandé » indiquant que la fondation Mozilla reconnaît et approuve.

Il faut ensuite cliquer sur la section de uBlock Origin pour se rendre sur sa page, cliquer sur le bouton « Ajouter à Firefox ».



Firefox demande la confirmation de l'installation, pour cela cliquer sur « Ajouter » et ensuite « OK ».



Un badge représentant l'extension est apparu à côté de l'icône de menu, celui-ci peut afficher des nombres indiquant le nom de blocage effectué sur la page en cours d'affichage.

Sur des sites comme YouTube (propriété de Google), le compteur peut vite monter même sans action de l'utilisateur :



## « HTTPS Everywhere »

### Explication

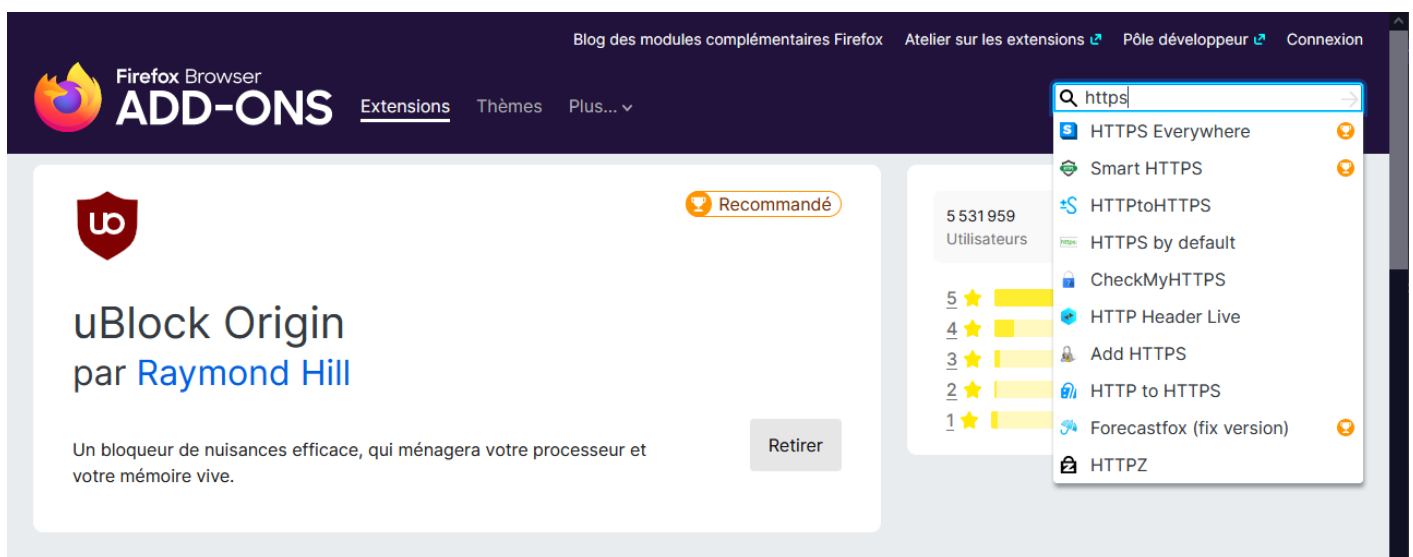
L'extension Firefox HTTPS Everywhere protège vos communications en activant automatiquement le chiffrement HTTPS sur les sites le prenant en charge, même lorsque vous saisissez une URL ou cliquez sur un lien sans préfixe « https: ».

[HTTPS Everywhere - Adoptez cette extension pour ☞ Firefox](#)

Le chiffrement permet de transmettre et recevoir des données entre l'ordinateur de l'utilisateur et le serveur hébergeant le site Web sans qu'une tierce personne présente dans le réseau informatique ne puisse consulter (et interpréter) les données. Bien qu'il s'agisse d'une norme de plus en plus utilisée, certains hébergeurs Web ne font pas systématiquement la redirection vers une communication chiffrée. Cette extension a pour rôle de forcer la connexion chiffrée si celle-ci est proposée par le serveur Web.

## Installation

La recherche peut se faire directement depuis le champ de recherche « Recherche des modules » en inscrivant « https ». Le premier résultat de recherche affiché est normalement celui correspondant, il est alors possible de le valider afin d'afficher la page du module de « HTTPS Everywhere ».



L'installation est identique au module précédent, à savoir cliquer sur le bouton « Ajouter à Firefox ».





# HTTPS Everywhere

par EFF Technologists

Chiffrez le Web ! L'extension Firefox HTTPS Everywhere protège vos communications en activant automatiquement le chiffrement HTTPS sur les sites le prenant en charge, même lorsque vous saisissez une URL ou cliquez sur un lien sans préfixe « https: ».

Ajouter à Firefox

Puis valider l'installation en cliquant sur le bouton « Ajouter », suivi du bouton « OK ».

## « Privacy Badger »

### Explication

“ Privacy Badger est un module complémentaire de navigateur qui empêche les annonceurs et autres trackers [aka pisteurs] tiers de suivre secrètement où vous allez et quelles pages vous regardez sur le Web. Si un annonceur semble vous suivre sur plusieurs sites Web sans votre permission, Privacy Badger empêche automatiquement cet annonceur de charger plus de contenu dans votre navigateur. Pour l'annonceur, c'est comme si vous aviez soudainement disparu.

[Privacy Badger \(traduction depuis le site officiel\)](#)

Privacy Badger et HTTPS Everywhere sont deux modules développés par l'Electronic Frontier Foundation. Il s'agit d'une fondation américaine à but non-lucratif créée en 1990. Elle défend les individus et nouvelles technologies contre les menaces abusives de recours en justice, soutient certaines avancées technologiques qui préservent les libertés individuelles.

### Installation

La recherche peut se faire directement depuis le champ de recherche « Recherche des modules » en inscrivant « privacy ». Le premier résultat de recherche affiché est normalement celui correspondant, il est alors possible de le valider afin d'afficher la page du module de « Privacy

Badger ».



 Recommandé

# Privacy Badger

par EFF Technologists

Automatically learns to block invisible trackers.

Ajouter à Firefox

L'installation est identique au module précédent, à savoir cliquer sur le bouton « Ajouter à Firefox ». Puis valider l'installation en cliquant sur le bouton « Ajouter », suivi du bouton « OK ».

## « Facebook Container »

### Explication

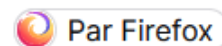
“ Empêchez Facebook de vous suivre partout sur Internet. L'extension Facebook Container pour Firefox vous aide à reprendre le contrôle et à séparer votre activité sur le web de votre profil Facebook.

Facebook Container – Adoptez cette extension pour  Firefox

Cette extension permet d'isoler automatiquement les onglets de Facebook afin de dissocier sa navigation habituelle de la consultation de son compte Facebook.

### Installation

La recherche peut se faire directement depuis le champ de recherche « Recherche des modules » en inscrivant « facebook ». Le premier résultat de recherche affiché est normalement celui correspondant, il est alors possible de le valider afin d'afficher la page du module de « Facebook Container ».



# Facebook Container

## par Mozilla Firefox

Empêchez Facebook de vous suivre partout sur Internet. L'extension Facebook Container pour Firefox vous aide à reprendre le contrôle et à séparer votre activité sur le web de votre profil Facebook.

Ajouter à Firefox

L'installation est identique au module précédent, à savoir cliquer sur le bouton « Ajouter à Firefox ». Puis valider l'installation en cliquant sur le bouton « Ajouter », suivi du bouton « OK ».

## « I don't care about cookies »

### Explication

“ Débarrassez-vous des avertissements de cookies de presque tous les sites Web. Cette extension de navigateur supprime les avertissements de cookies de presque tous les sites Web et vous évite des milliers de clics inutiles ! Dans la plupart des cas, elle se contente de bloquer ou de masquer les fenêtres pop-up relatives aux cookies. Lorsque cela est nécessaire au bon fonctionnement du site Web, elle accepte automatiquement la politique en matière de cookies pour vous (parfois elle accepte toutes les catégories de cookies et parfois seulement les catégories de cookies nécessaires, selon ce qui est le plus facile à faire). Il ne supprime pas les cookies.

[I don't care about cookies \(traduction depuis le site officiel\)](#)

En raison du RGPD (Règlement Général sur la Protection des Données) les sites Web sont dans l'obligation de demander l'accord aux usagers avant de les pister. Raison pour laquelle de nombreux sites demandent d'accepter les cookies. Cette extension permet de supprimer la bannière de demande relative à ces cookies.

### Installation

La recherche peut se faire directement depuis le champ de recherche « Recherche des modules » en inscrivant « care ». Le premier résultat de recherche affiché est normalement celui correspondant, il est alors possible de le valider afin d'afficher la page du module de « I don't care about cookies ».



 **Recommandé**

## I don't care about cookies

par **Kiko**

Get rid of cookie warnings from almost all websites!

Ajouter à Firefox

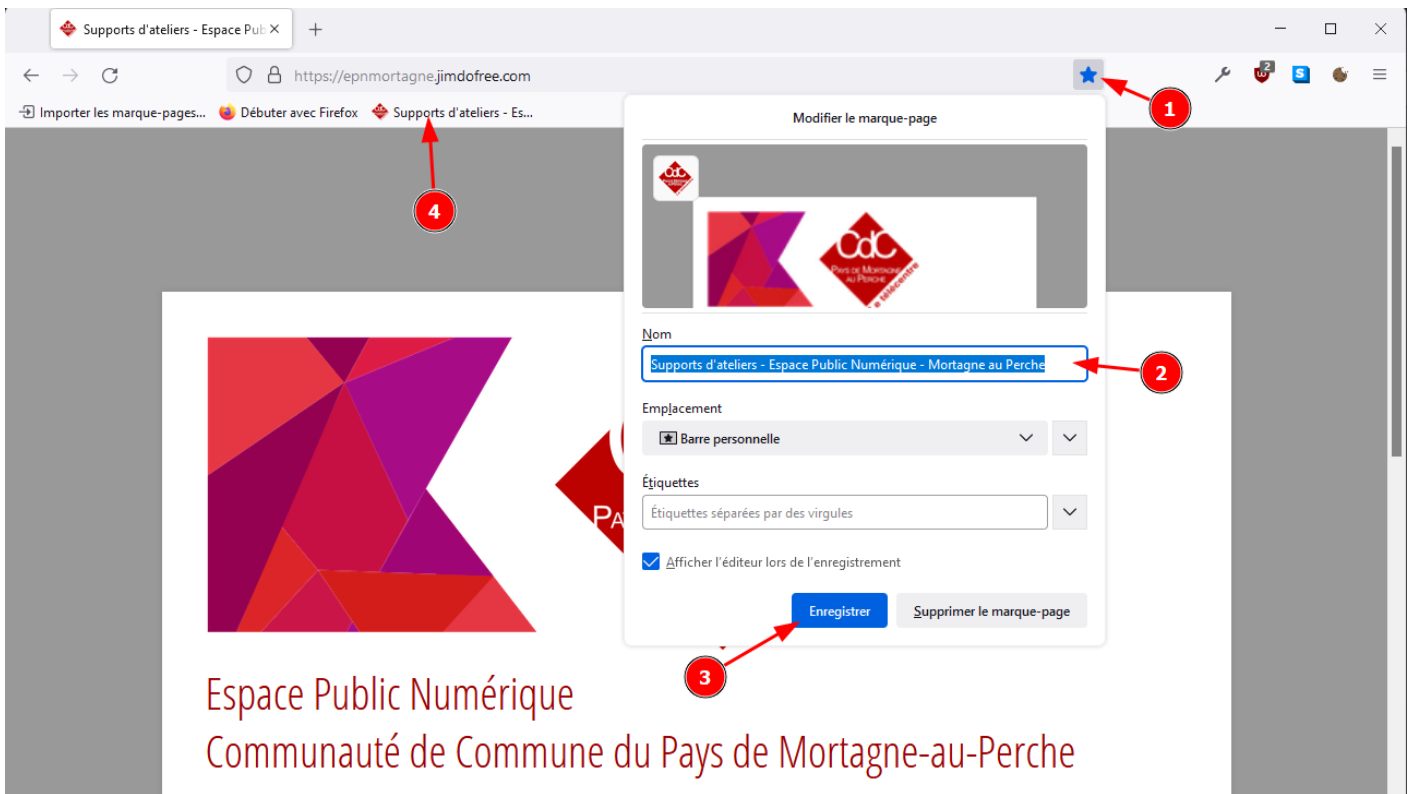
L'installation est identique au module précédent, à savoir cliquer sur le bouton « Ajouter à Firefox ». Puis valider l'installation en cliquant sur le bouton « Ajouter », suivi du bouton « OK ».

## Bonus : Utilisation des marques-pages

“ Nous consultons souvent les mêmes sites internet : la SNCF pour les billets de train, notre boîte mail, le site de notre banque... Pour y accéder, il faut effectuer une recherche, trouver le bon site web dans les résultats de nos recherches puis cliquer dessus. Ça n'est pas forcément très long, mais il existe une méthode bien plus simple que de devoir rechercher chaque fois les mêmes sites : **les marques-pages**.

Un marque-page fonctionne de la même manière qu'un marque-page classique pour un livre. Il va nous permettre de garder un site internet à portée de main, sans avoir à chercher la page à chaque fois que l'on ouvre notre navigateur. Ajouter un marque-page est une procédure assez simple. Il faut tout d'abord cliquer sur l'icône en forme d'étoile [repère 1] présente dans la barre d'adresse en haut de votre navigateur. En appuyant sur celle-ci, il va alors vous proposer d'ajouter ce site à vos marque-pages. Vous pouvez alors décider de lui donner un nom [repère 2] et de le placer dans un dossier spécifique : nous allons choisir

Se protéger sur le web : sécuriser et faciliter sa navigation pour EPN Salle des Rancy par Théo Barnouin.



Il convient d'utiliser les marques-pages pour consulter les sites récurrents (comme sa messagerie, sa banque, etc.). Il est inutile, voire risqué, de consulter un site Web depuis un lien reçu par e-mail.

# Sources

- Protéger-vous du pistage sur le Web ! pour Lyon Café Vie Privée par Le Poisson Libre.
- Se protéger sur le web : sécuriser et faciliter sa navigation pour EPN Salle des Rancy par Théo Barnouin.
- Dictionnaire Larousse en ligne.
- Encyclopédie Wikipédia en ligne.
- Traducteur DeepL en ligne.
- Navigateur Mozilla Firefox.

- Extension Mozilla Firefox.
- 



---

Révision #4

Créé 10 février 2022 16:32:17 par Mickaël G.

Mis à jour 11 février 2022 17:07:24 par Mickaël G.