

Installer Firefox et le paramétrer pour se protéger contre le pistage.

1 – Sommaire

1 – Sommaire.....	1
2 – Installation de Firefox.....	2
3 – Paramétrer Firefox.....	2
3.1 – Onglet “général”.....	3
3.2 – Onglet “Recherche”.....	3
3.3 – Onglet “Vie privée et sécurité”.....	6
4 – Les modules complémentaires.....	9

Note :

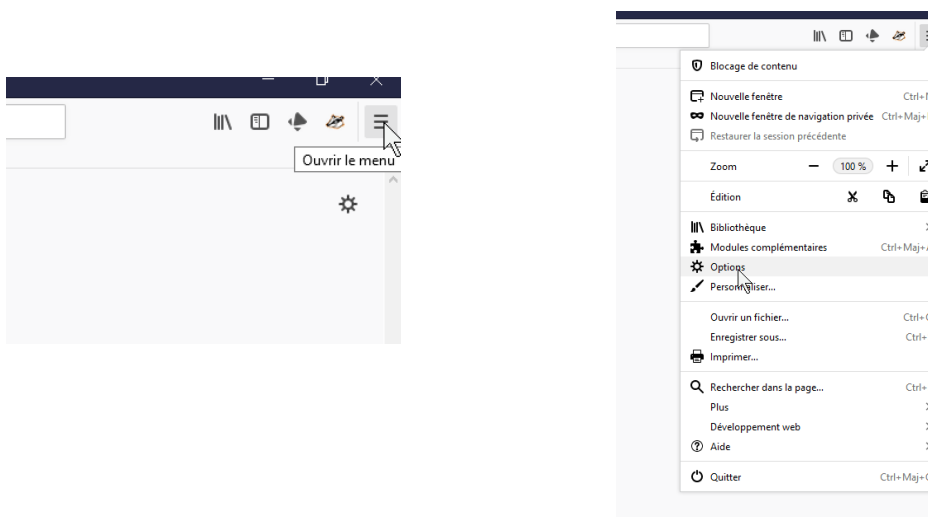
Note : Damien Quinton – Ce support est sous licence libre copyleft CC-BY-SA, ce qui signifie que vous pouvez le modifier et le redistribuer comme bon vous semble, à la condition qu'il soit distribué sous la même licence, donc avec les mêmes libertés et en citant son auteur. – https://fr.wikipedia.org/wiki/Licence_Creative_Commons
<https://creativecommons.org/licenses/by-sa/2.0/deed.fr>

2 – Installation de Firefox

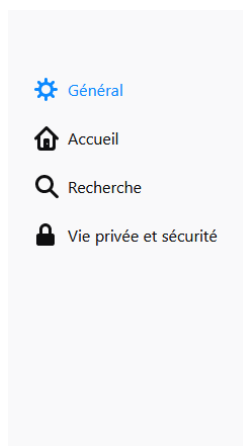
1. Après avoir ouvert votre navigateur (Google chrome, internet explorer etc.), taper dans la barre d'adresse « firefox.com »
2. Cliquer sur « Télécharger firefox »
3. Une fois le fichier téléchargé, ouvrez le et suivez les instructions (faire « suivant »)
4. Une fois l'installation terminée, ouvrez Firefox.

3 – Paramétrer Firefox

Pour accéder aux paramètres de Firefox, cliquer sur le menu, puis “options” :

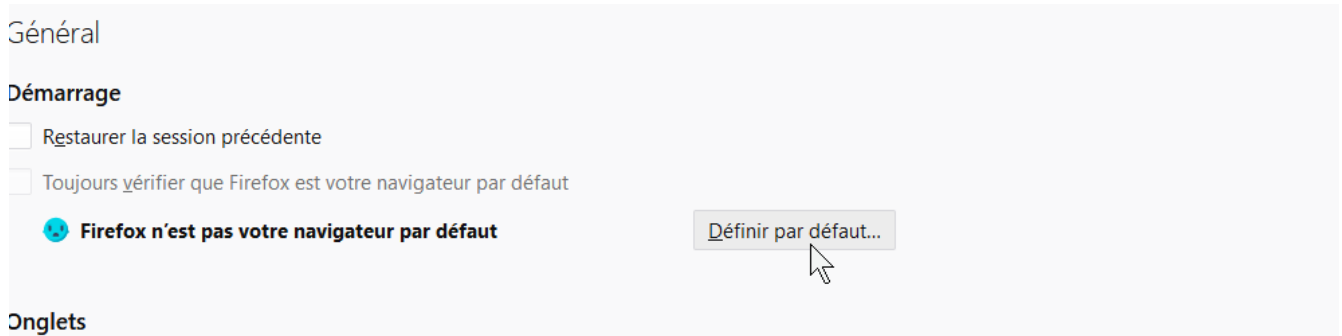


On a alors sur la gauche plusieurs onglets :



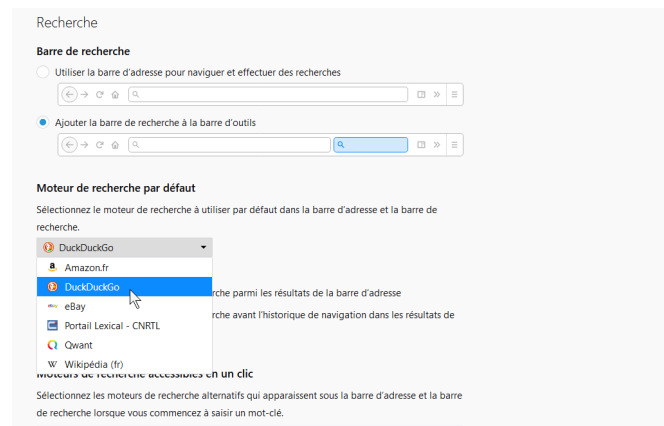
3.1 – Onglet “général”

Dans l'onglet “général”, on peut définir Firefox comme étant notre navigateur par défaut en cliquant sur “définir par défaut” :

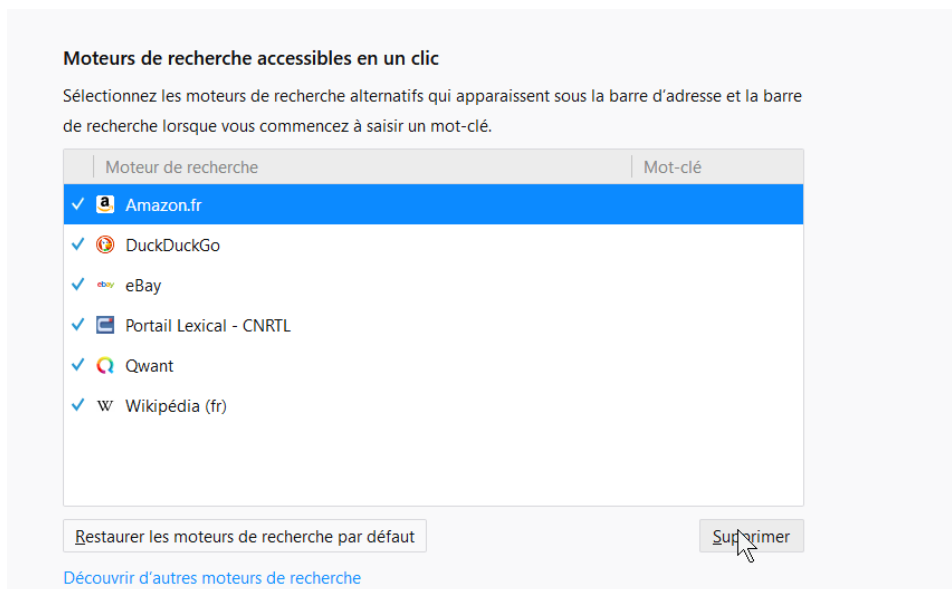


3.2 – Onglet “Recherche”

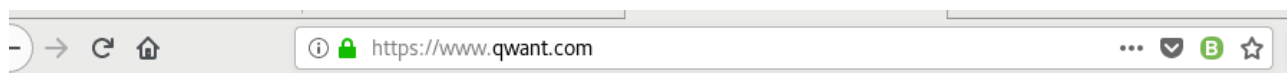
On peut modifier le moteur de recherche par défaut. Par exemple, avec duckduckgo :



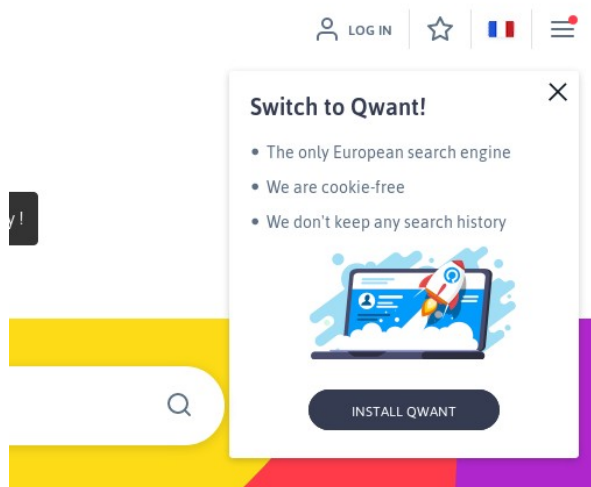
On peut ensuite supprimer certains moteurs de recherche dans la liste en dessous :



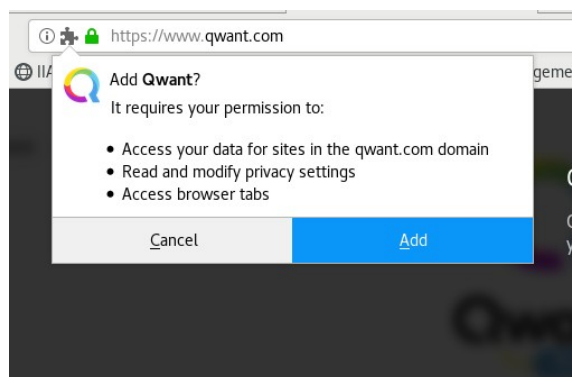
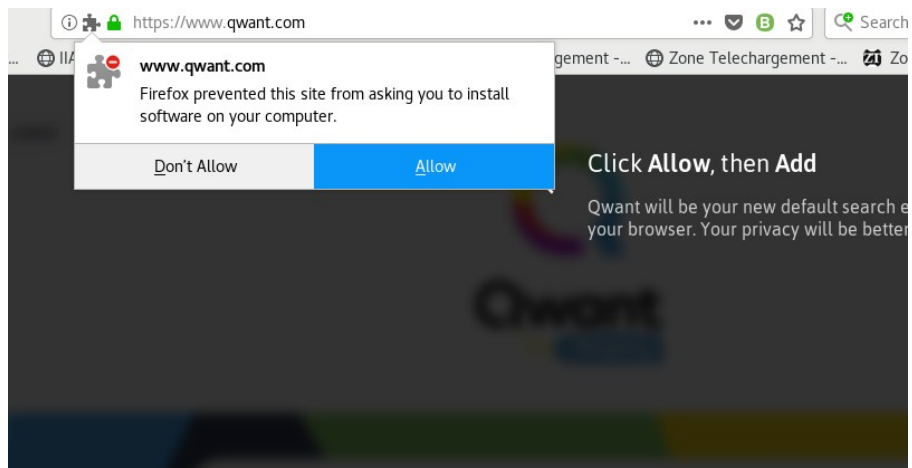
Note : pour ajouter des moteurs de recherche, il suffit d'aller sur le moteur en question :



Et la plupart du temps, le moteur de recherche détecte qu'il n'est pas installé sur votre navigateur. Il vous propose donc de l'installer.



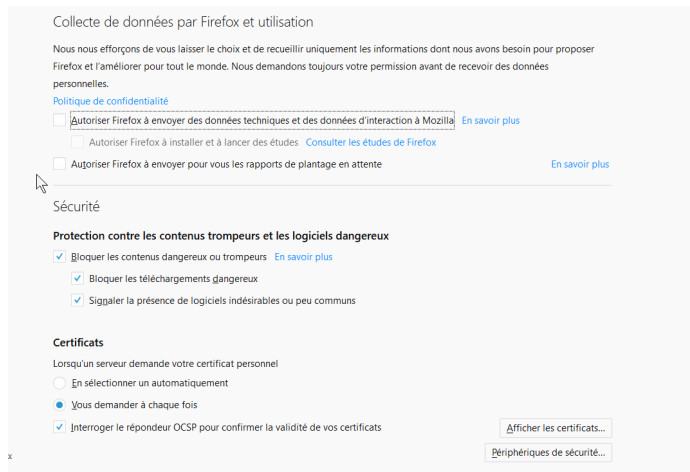
Il vous suffit donc de cliquer sur « installer », puis « autoriser » et « ajouter », comme sur les captures suivantes :



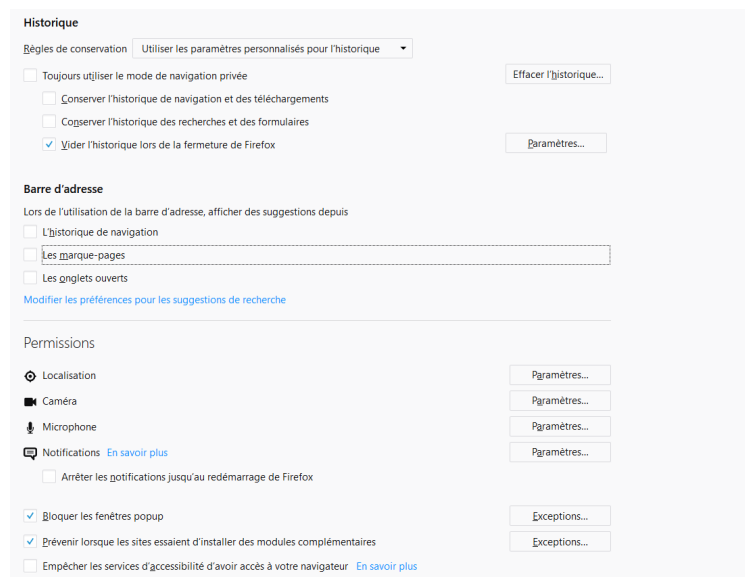
3.3 – Onglet “Vie privée et sécurité”:

Pour cette partie, mettre les paramètres tels qu'ils sont sur les captures d'écran :

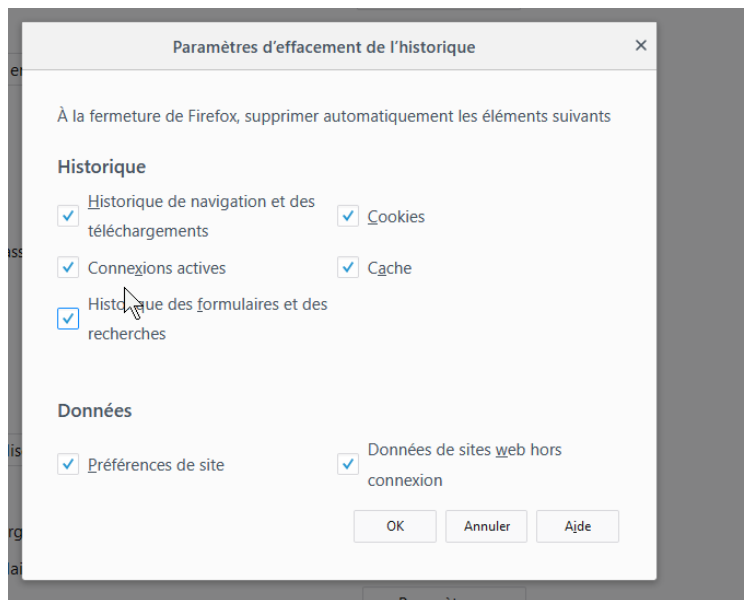
On commence par le bas de la page, puis on remonte au fur-et-à-mesure : descendre tout en bas :



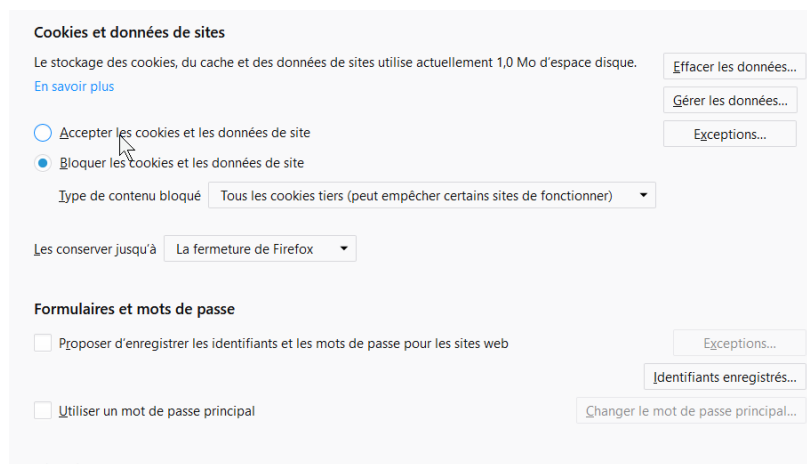
Ci-dessous, commencer par modifier “règles de conservation”. Les paramètres juste en dessous s'afficheront.



Dans la catégorie “historique”, on clique sur “paramètres” en face de “vider l'historique lors de la fermeture de firefox” :

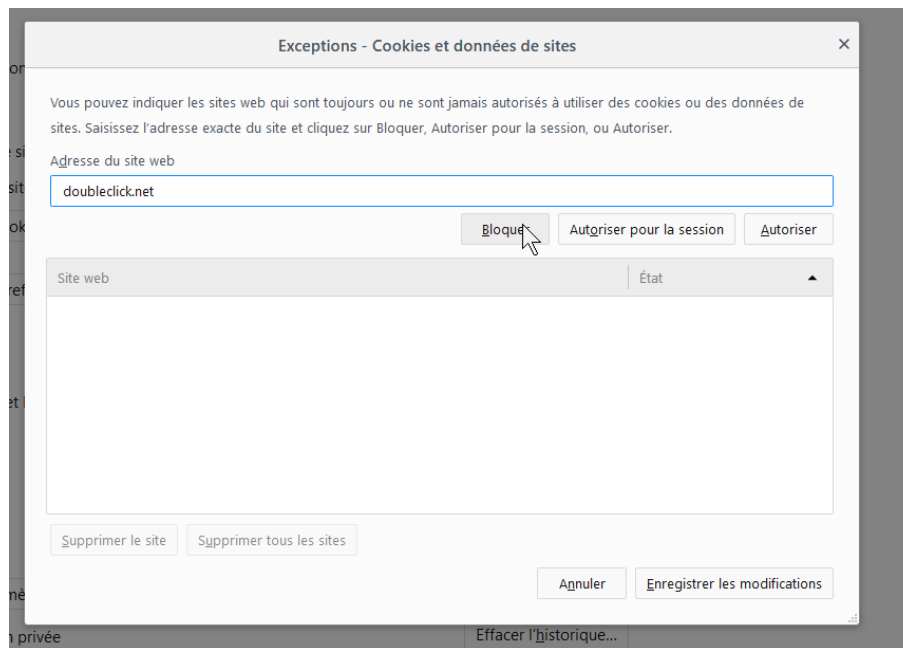


On remonte un peu...

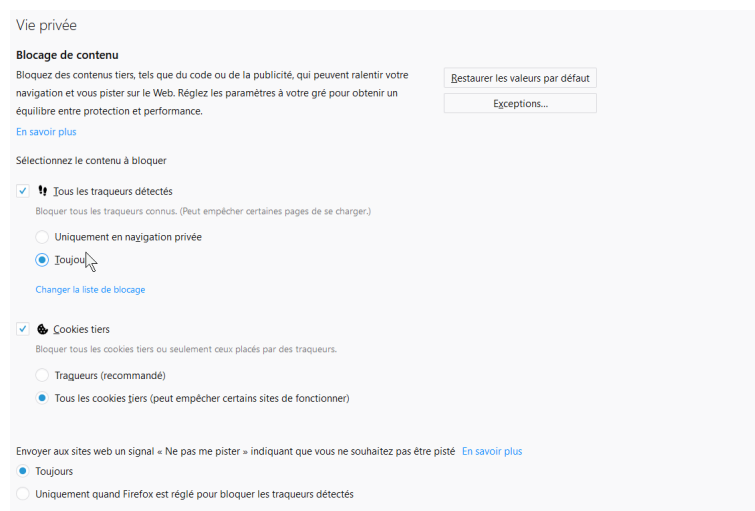


Ci-dessus, on clique sur “exceptions...”

Et on bloque doubleclick.net, qui est une régie publicitaire de google qui permet de faire du ciblage comportemental :



On enregistre les modifications, puis on continue :



Avec ces paramètres, lorsque l'on ferme Firefox pour le rouvrir par la suite, on ne retrouvera aucune trace à part les marque page. De plus, certains cookies, traqueurs et contenus dangereux seront bloqués, mais pas tout.

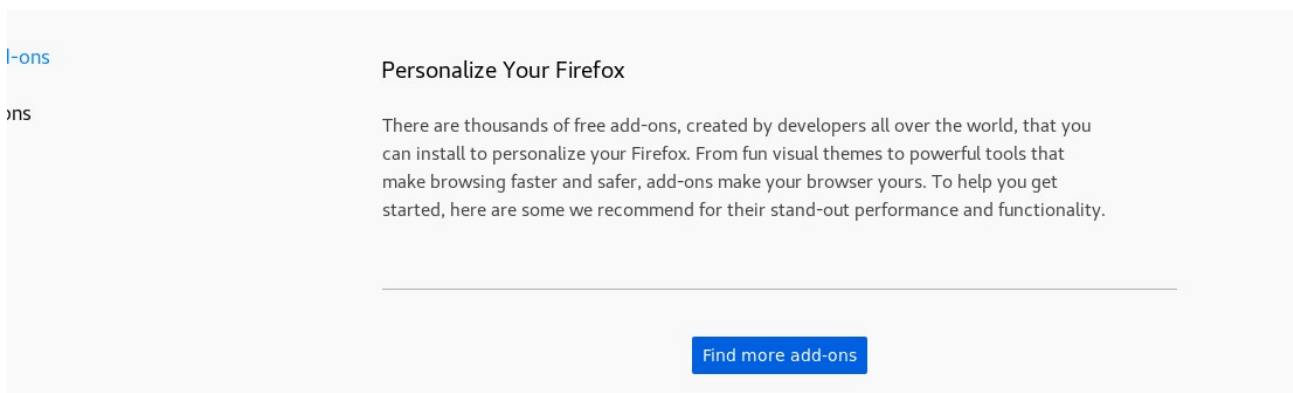
ATTENTION : Il est recommandé de checker régulièrement ces paramètres au cas où ils aient changé ou soient rétablis par défaut (dans le cas d'une mise à jour par exemple)

4 – Les modules complémentaires

Un module complémentaires est un logiciel que l'on vient installer sur son navigateur afin de lui ajouter des fonctionnalités supplémentaires. On a pour cela à notre disposition une boutique directement dans le navigateur qui va nous permettre d'en installer très simplement. Sur Firefox, c'est ici que ça se passe :



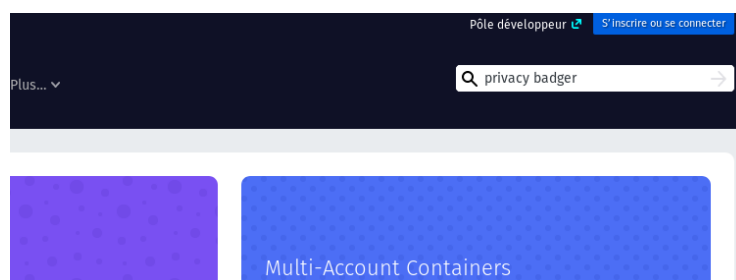
On ensuite aller dans le catalogue et commencer à rechercher des extensions :



Cliquez sur « trouver plus d'extensions »

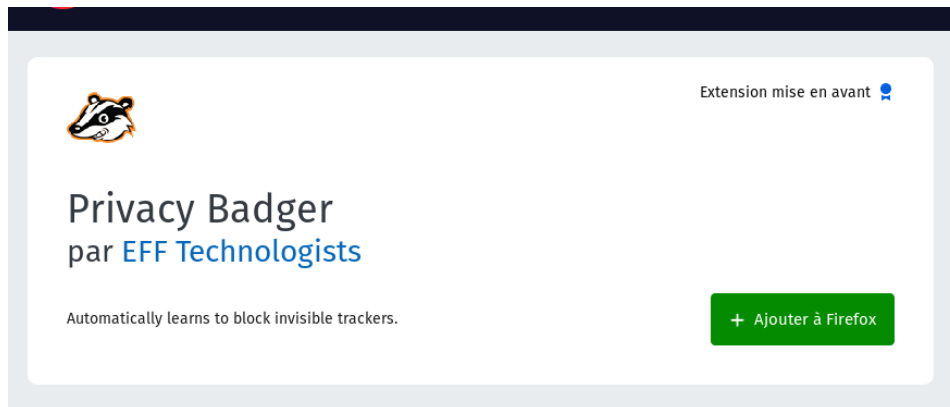
Nous allons prendre l'exemple de Privacy badger pour voir comment installer des extensions (=module complémentaire).

Privacy Badger est une extension libre (c'est à dire qu'elle respecte des valeurs éthiques et sociales et que chacun peut l'utiliser et la modifier comme il le souhaite). Elle « tracke les trackeurs », c'est à dire qu'au fur et à mesure de votre navigation, elle va regarder les traceurs qui vous suivent, et va les bloquer en fonction. Pour l'installer, on recherche « privacy badger » dans la barre de recherche :

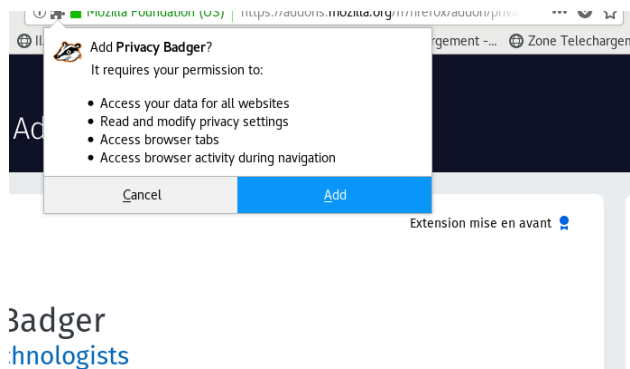




On clique sur l'application, puis sur « ajouter à firefox » :



Firefox nous demande confirmation, on clique donc sur « ajouter » :



Et là, ça y'est, Privacy Badger commence son boulot !

Cette extension est très utile à elle toute seule, car elle apprend d'elle même les nouveaux traqueurs en fonction de votre navigation. Néanmoins, on peut l'utiliser en complémentarité avec d'autres bloqueurs, qui eux se réfèrent à une liste déjà existante de traceurs (pour les installer, faire de même qu'avec privacy badger) :



HTTPS Everywhere est une extension permettant de forcer le passage en HTTPS sur les sites qui ne le sont pas par défaut (mais qui le supporte quand même)

(Note: Toutes les extensions présentées ici sont libres).

ATTENTION : Il est conseillé de ne pas installer Adblock plus, qui a des contrats avec certaines régies publicitaires afin de laisser passer certaines publicités. Privilégiez Ublock Origin. Plus d'infos sur <https://bloquerlapub.net>

Une fois que l'on a bien paramétré son navigateur et que l'on a installé les extensions ci-dessus, on commence déjà à être mieux protégé contre les traqueurs et les publicités intrusives. Mais évidemment nous avons encore du chemin à faire...