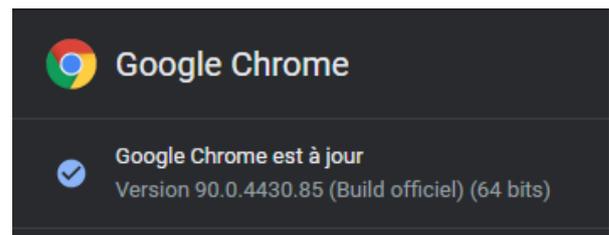
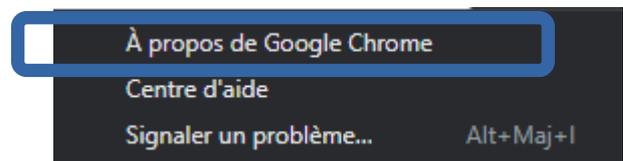
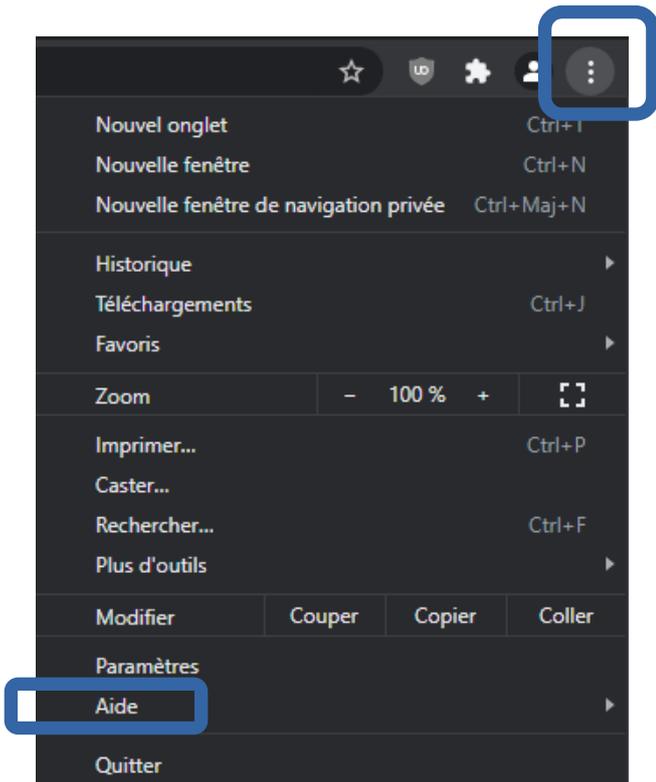


Sécuriser son navigateur et ses données sur Internet (Chrome)



Mettre à jour son navigateur

Si Chrome ne vous signale pas qu'une mise à jour est disponible, il faut ouvrir le menu , puis "Aide" / "À propos de Google Chrome" et "Mettre à jour"



Même si votre navigateur fonctionne très bien sans être à jour, des failles de sécurité peuvent être exploitées par des personnes malveillantes. Les mises à jour intègrent les correctifs nécessaires.

D'autre part, certains sites ou certains outils en ligne (notamment de visio et de classes virtuelles) ont besoin de navigateurs mis à jour pour fonctionner correctement.

Enfin les mises à jours intègrent de nouvelles fonctionnalités dont vous pourriez trouver une utilité un jour !



Installer les extensions essentielles

- **Rendez-vous sur la page des "extensions"**

C'est dans ce champs de recherche que vous indiquerez le nom de l'extension

- **Si vous ne deviez installer qu'une extension : uBlock Origin**

uBlock Origin

Proposé par : Raymond Hill (gorhill)

Un bloqueur de nuisances efficace, qui ménagera votre processeur et votre mémoire vive.

★★★★★ 24 227 Productivité

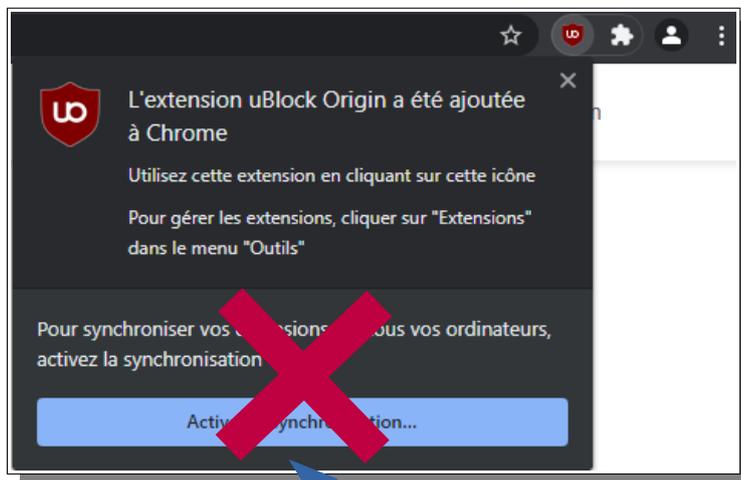
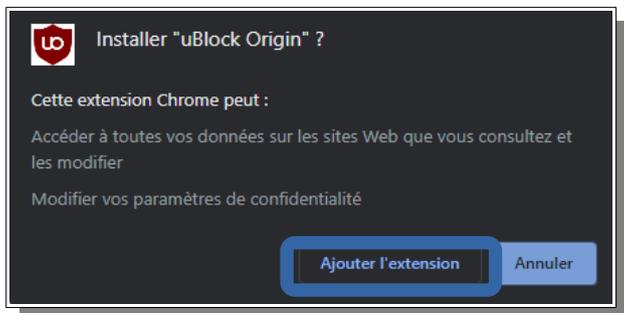
Accueil > Extensions > uBlock Origin

uBlock Origin

Proposé par : Raymond Hill (gorhill)

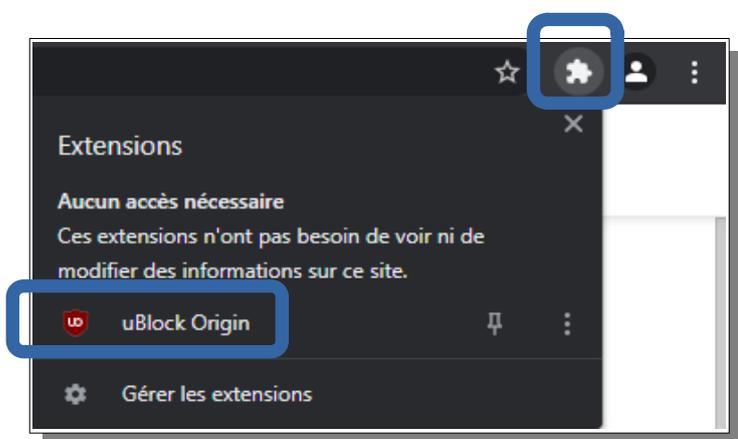
★★★★★ 24 227 | Productivité | 10 000 000+ utilisateurs

Ajouter à Chrome

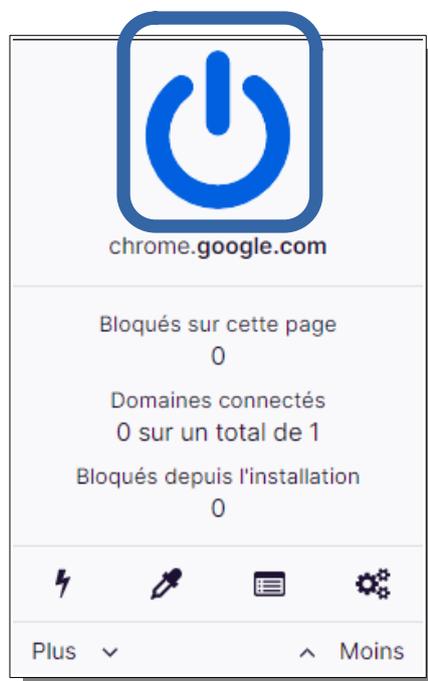


"Activer la synchronisation" n'est pas nécessaire...

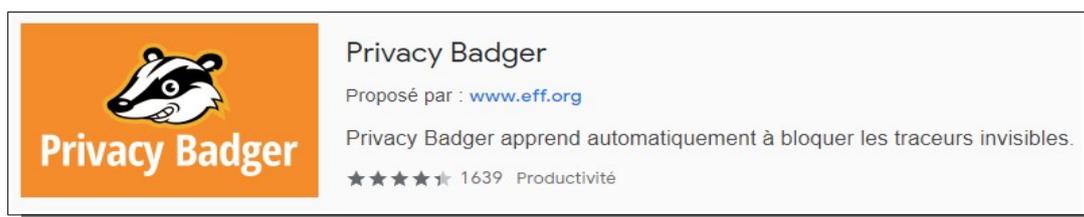
- Pour paramétrer l'extension :



Un clic sur l'extension et vous pourrez désactiver uBlock Origin (le bouton ON/OFF bleu) si vous naviguez sur un site qui vous bloque sous prétexte d'utiliser un bloqueur de publicité !



- Si vous deviez installer une deuxième extension : **Privacy Badger**



Cette extension empêche les annonceurs publicitaires et autres opérateurs de pistage et de surveillance des internautes, quelle que soit la méthode de pistage utilisée, de pratiquer ce pistage et cette surveillance.

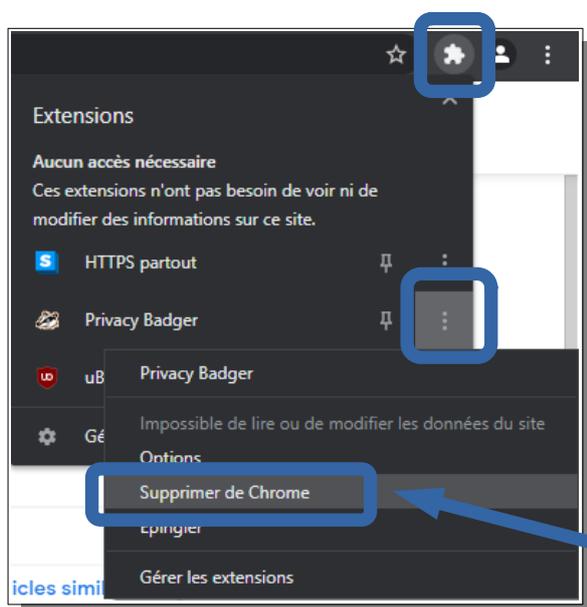
La procédure d'installation est identique à la précédente... et vous pourrez, une fois installée, l'activer ou la désactiver en cliquant sur le logo présent en haut à droite de votre navigateur.

- Si vous deviez en installer une troisième : **HTTPS partout**



Cette extension force les sites que vous visitez à vous proposer une version sécurisée de leur site afin que les données qui transitent entre celui-ci et votre ordinateur soient cryptées et ne puissent pas être interceptées (ex. formulaires, coordonnées bancaires, mots de passe,...)

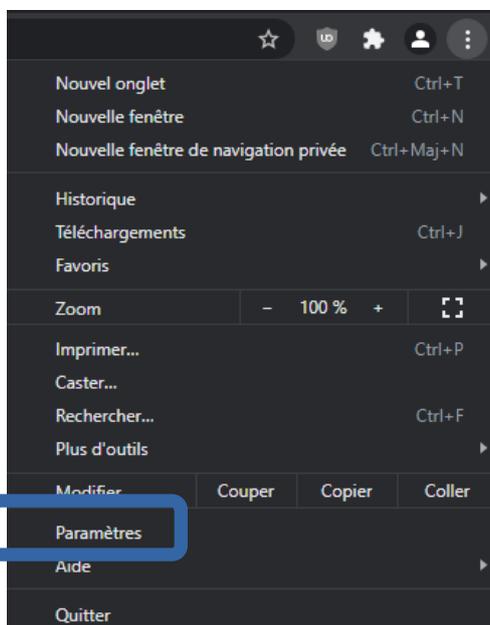
Désactiver/désinstaller une extension



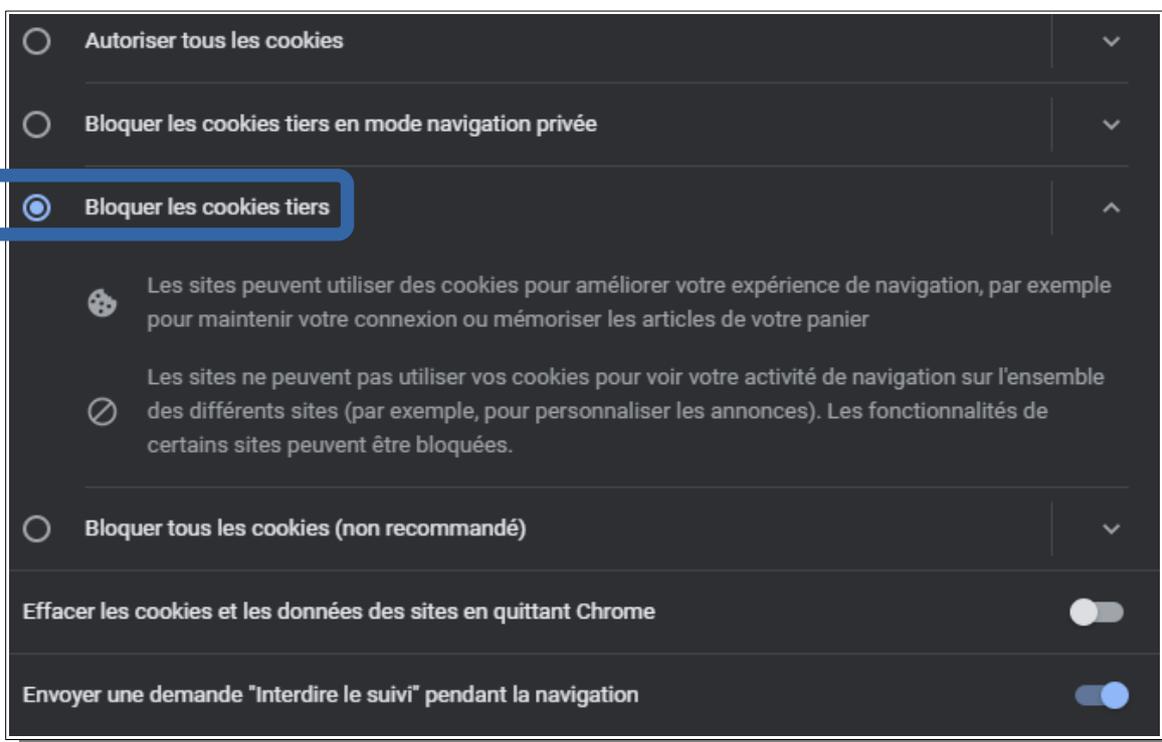
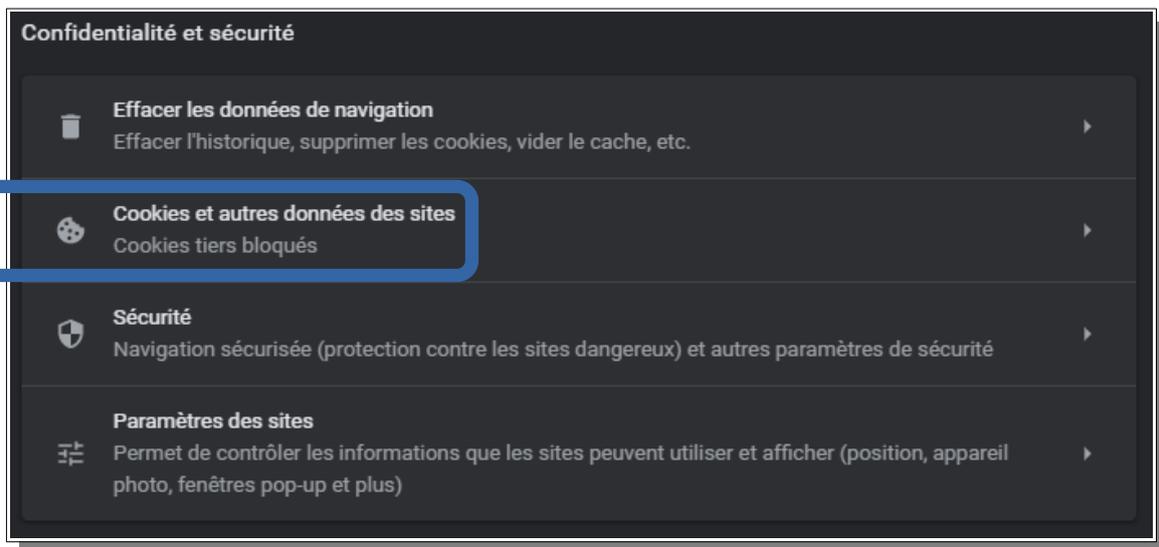
Pour désinstaller définitivement l'extension



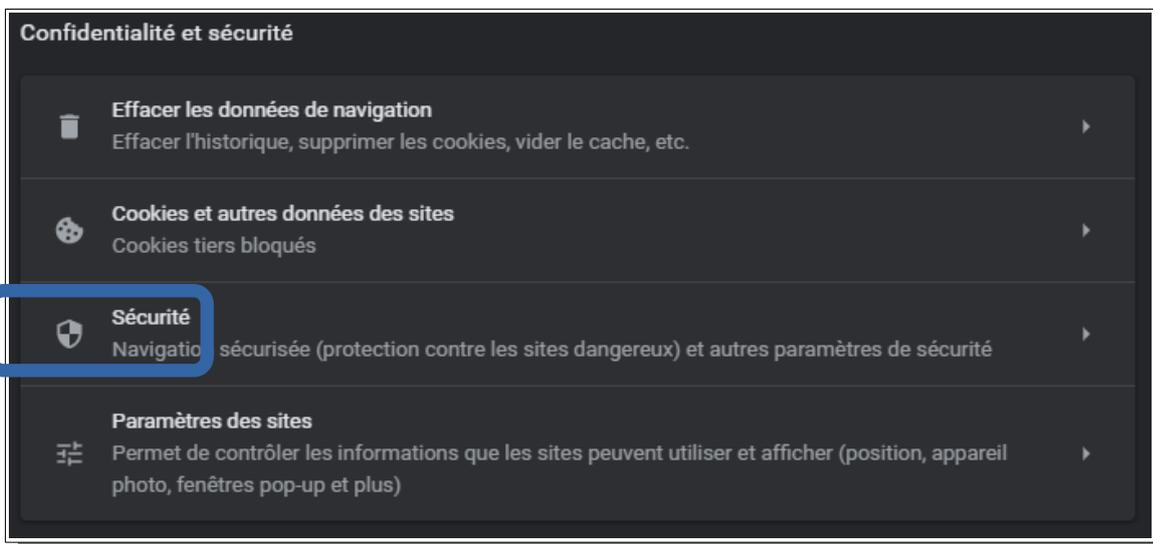
Effectuer quelques réglages dans les options du navigateur



- Menu "Confidentialité et sécurité" / "Cookies et autres données des sites"



- Menu "Confidentialité et sécurité" / "Sécurité"



Protection standard

- Ce mode offre une protection standard contre les téléchargements, les extensions et les sites web connus pour être dangereux.

Il détecte les événements dangereux et vous en informe lorsqu'ils surviennent

Il vérifie les URL d'après une liste de sites dangereux stockée dans Chrome. Si un site tente de voler votre mot de passe ou si vous téléchargez un fichier dangereux, Chrome peut également envoyer les URL concernées, y compris des extraits du contenu de pages, à la fonctionnalité de navigation sécurisée.

Pour information, La protection renforcée est plus intéressante en ce qui concerne la sécurisation de vos données **mais** elle implique d'envoyer des informations à Google et elle associe temporairement Chrome à votre compte Google. Si ça n'est pas déjà le cas, à vous de voir...

Protection renforcée

- Ce mode offre une protection proactive et plus rapide contre les téléchargements, les extensions et les sites Web dangereux. Il vous permet d'être averti en cas de piratage de mots de passe et nécessite d'envoyer les données de navigation à Google.

Prédit les événements dangereux et vous en informe avant qu'ils ne surviennent

Ce mode assure votre sécurité dans Chrome et peut être utilisé pour améliorer votre sécurité dans d'autres applications Google lorsque vous êtes connecté

Renforce votre sécurité et celle de tous les utilisateurs sur le Web

Vous alerte si des mots de passe sont compromis lors d'une violation des données

Il envoie des URL à la navigation sécurisée pour les vérifier. Il transmet également un petit échantillon de pages, de téléchargements, d'informations système et de l'activité des extensions afin d'identifier de nouvelles menaces. De même, pour vous protéger dans l'ensemble des applications Google, il associe temporairement ces données à votre compte Google lorsque vous êtes connecté.

- Menu "Moteur de recherche"

Dans le menu "Moteur de recherche", profitez-en pour choisir un moteur de recherche par défaut qui soit plus respectueux de vos données personnelles que Google, comme **Qwant** par exemple

