# Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V2.3

7 nov, 2026 · @Gabriel

***Objectif :*** *Remplacer Chrome, Edge ou Safari par un navigateur respectueux de votre vie privée, qui limite la collecte de vos données de navigation, bloque le pistage d'un site à l'autre et les publicités intrusives. Cette fiche présente aussi des réglages avancés contre le fingerprinting (empreinte numérique) et explique ce que font – et ne font pas – les outils « anti-DPI ».*

- ***Public visé :*** *Intermédiaire / Avancé (quelques réglages avancés)*
- ***Temps estimé :*** *30 à 45 minutes*
- ***Difficulté :*** *★★★☆☆ (Moyen)*
- ***Prérequis :*** *savoir installer un logiciel et une extension de navigateur*
- ***Fiches associées :*** *N°14a (nettoyer vos liens), N°14b (cas particuliers du nettoyage de liens), N°13 (passer à Linux)*

## 1. Pourquoi quitter Chrome, Edge ou Safari ? (Le problème)

| Navigateur | Problème principal |
|---|---|
| **Google Chrome** | Navigateur d'un groupe dont le modèle repose sur la publicité ciblée, synchronisation poussée avec le compte Google. Chrome n'exécute plus aucune extension Manifest V2 depuis Chrome 139 (2025), et Google a retiré les dernières extensions MV2 du Chrome Web Store le 31 août 2026 : les bloqueurs les plus puissants n'y fonctionnent plus. |
| **Microsoft Edge** | Basé sur Chromium (mêmes limites d'extensions), services cloud Microsoft intégrés par défaut, télémétrie difficile à désactiver complètement. |
| **Safari (Apple)** | Protections de base correctes, mais logiciel propriétaire, synchronisé avec iCloud (serveurs d'Apple), disponible uniquement sur les appareils Apple. |

**Ce qu'il faut comprendre :**

- Le navigateur voit tous les sites que vous visitez, quand et combien de temps.
- Les régies publicitaires construisent des profils de centres d'intérêt (politique, santé, achats…).
- Les sites et les traqueurs tiers vous suivent d'un site à l'autre (cookies tiers, fingerprinting).

**Le bénéfice :** un navigateur qui bloque les traqueurs et les publicités, et qui ne fait pas de votre navigation un produit.


gabriel.ananda@mailo.com
CC BY SA

# Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V2.3

## 2. Les solutions : navigateurs open source et/ou axés vie privée

| Navigateur | Moteur | Open source | Blocage natif | Extensions recommandées | Idéal pour |
|---|---|---|---|---|---|
| **Firefox** | Gecko | ✓ Oui | Protection renforcée contre le pistage (mode Standard ou Strict) | **uBlock Origin seul** | Usage quotidien (ordinateur et Android) |
| **Brave** | Chromium | ✓ Oui | Boucliers (Shields) : moteur de blocage maison, compatible avec les listes de filtres de type uBlock Origin | Aucune nécessaire | Usage quotidien (mobile et ordinateur) |
| **LibreWolf** | Gecko (Firefox) | ✓ Oui | Très strict, uBlock Origin préinstallé | Déjà configuré | Utilisateurs avancés / exigeants (ordinateur uniquement) |
| **Chromium (sans modification)** | Chromium | ✓ Oui | Aucun | uBlock Origin Lite uniquement (Manifest V2 retiré aussi de Chromium) | Puristes open source (peu protégé par défaut) |
| **Tor Browser** | Gecko (Firefox) | ✓ Oui | Très élevé (réseau Tor + navigateur durci) | **Aucune** : le Tor Project déconseille fortement d'en ajouter | Anonymat fort (lanceurs d'alerte, contournement de la censure) |


gabriel.ananda@mailo.com
CC BY SA

# Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V2.3

## 3. Le changement majeur : la fin de Manifest V2 sur Chrome

### 3.1 Ce qui a changé

Google a supprimé progressivement les extensions « Manifest V2 » (MV2), dont fait partie **uBlock Origin** (version complète) :

- **Juillet 2025 – Chrome 138** : les extensions MV2 sont désactivées sur tous les canaux, sans possibilité de les réactiver. Chrome 138 est la dernière version qui pouvait encore les faire tourner (via une stratégie d'entreprise).
- **Chrome 139 et suivants** : les extensions MV2 ne fonctionnent plus du tout.
- **31 août 2026** : toutes les extensions MV2 restantes sont retirées du Chrome Web Store. Une copie déjà installée sur Chrome 138 ou antérieur reste en place, mais ne reçoit plus de mise à jour et ne peut plus être réinstallée.
- **uBlock Origin Lite** est la version proposée pour Chrome. Elle repose sur l'API déclarative de Manifest V3 et **est moins puissante** : pas de filtrage dynamique, contrôles par site limités (polices distantes, scripts, gros médias).

### 3.2 Qui permet encore uBlock Origin complet ?

**Firefox** conserve Manifest V2 à côté de Manifest V3 et continue d'accepter uBlock Origin complet, sur **ordinateur et Android**. Mozilla a répété en 2024 et en 2025 qu'elle n'avait pas de projet de suppression de MV2, sans donner de durée garantie.

**Brave** s'est engagé à continuer de prendre en charge quelques extensions MV2 : **uBlock Origin, NoScript, uMatrix et AdGuard**. Ses Boucliers intégrés suffisent toutefois dans la plupart des cas.

⚠️ **À savoir sur Brave :** Brave Software est une entreprise américaine (soumise au Cloud Act). Elle se finance notamment par sa propre publicité, affichée seulement si vous l'activez (Brave Rewards), et par ses services. En 2020, Brave a reconnu avoir ajouté à tort des codes d'affiliation à certaines adresses tapées par ses utilisateurs, puis a corrigé. Firefox est lui aussi américain, mais édité par une filiale de la fondation Mozilla, à but non lucratif.

**LibreWolf**, dérivé de Firefox, fonctionne comme Firefox et fournit uBlock Origin préinstallé.

### 3.3 Ce que cela implique pour vos choix

| Navigateur | uBlock Origin complet | uBlock Origin Lite | Recommandation |
|---|---|---|---|
| **Chrome** | ✗ Non (depuis Chrome 139) | ✓ Seule option | Éviter pour la protection avancée |
| **Edge** | ✗ Non (mêmes règles Chromium) | ✓ Disponible | Éviter pour la protection avancée |
| **Firefox** | ✓ Oui | ✓ Disponible | **Recommandé** |


gabriel.ananda@mailo.com
CC BY SA

# Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V2.3

| Navigateur | uBlock Origin complet | uBlock Origin Lite | Recommandation |
|---|---|---|---|
| **Brave** | ✓ Oui (prise en charge annoncée par Brave) | ✓ Disponible | **Recommandé** (Boucliers suffisants) |
| **LibreWolf** | ✓ Préinstallé | Sans objet | **Recommandé (avancé)** |

## 4. Pourquoi ne pas empiler les extensions de protection

### 4.1 Chaque extension est une trace de plus

Un principe simple : **chaque extension ajoutée modifie le comportement du navigateur, donc peut le rendre plus reconnaissable**. Un site peut détecter une extension de trois manières :

1. **Ressources accessibles** : l'extension expose des fichiers à des adresses identifiables.
2. **Modifications de la page** : un bloqueur retire des éléments, ce qui laisse des traces.
3. **Comportement ajouté** : une extension qui modifie *navigator* ou *canvas* peut être repérée.

Plusieurs extensions de confidentialité peuvent aussi **se contredire** : deux composants qui modifient les mêmes valeurs créent des incohérences, plus faciles à détecter.

### 4.2 Le cas de Privacy Badger

En 2020, l'EFF (qui développe Privacy Badger) a reconnu que l'**apprentissage local** de l'extension pouvait servir à créer un identifiant propre à chaque utilisateur. Elle a donc **désactivé cet apprentissage par défaut** : tous les utilisateurs partagent désormais la même liste préétablie. Le risque principal a donc été corrigé, mais Privacy Badger fait doublon avec uBlock Origin.

### 4.3 La règle à retenir

**Une seule extension de blocage suffit : uBlock Origin.** Inutile d'ajouter Privacy Badger, NoScript ou d'autres extensions de « protection » par-dessus.

**Exceptions :**

- Sur Firefox, **Multi-Account Containers** est une extension d'isolement (pas de blocage), complémentaire d'uBlock Origin.
- Dans **Tor Browser**, n'ajoutez **aucune** extension, pas même uBlock Origin : le Tor Project le déconseille fortement, car cela peut compromettre votre anonymat et votre sécurité.


gabriel.ananda@mailo.com
CC BY SA

# Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V2.3

## 5. Focus sur LibreWolf : le Firefox durci pour les exigeants

### 5.1 Qu'est-ce que LibreWolf ?

LibreWolf est un **dérivé indépendant de Firefox**, orienté confidentialité et sécurité. Il utilise le même moteur Gecko, avec une philosophie différente : **confidentialité maximale par défaut, sans configuration manuelle**.

Par défaut, LibreWolf, c'est :

- **Télémétrie entièrement désactivée** (y compris rapports de plantage et études).
- **uBlock Origin préinstallé**, avec la protection contre le pistage en mode strict.
- **Protection anti-fingerprinting RFP (Resist Fingerprinting)** activée, issue du projet Tor Uplift.
- **Cookies et données des sites effacés à la fermeture**, sauf exceptions que vous créez.
- **DRM désactivés** : Netflix, Disney+ et autres services de streaming protégés ne fonctionnent pas sans réactivation.
- **WebGL désactivé** : certaines cartes 3D et applications web interactives peuvent ne pas fonctionner.

### 5.2 Les contraintes à connaître

| Contrainte | Explication |
|---|---|
| **Ordinateur uniquement** | Pas de version Android ni iOS. Sur Android, LibreWolf conseille IronFox ; sinon Firefox ou Brave. |
| **Synchronisation désactivée par défaut** | Firefox Sync peut être activé dans les réglages de LibreWolf (données chiffrées localement avant envoi). |
| **DRM désactivés** | À réactiver dans **Paramètres › Général › Contenu protégé par des DRM**, uniquement pour les sites qui en ont besoin. |
| **WebGL désactivé** | À n'activer que pour les sites qui en ont besoin. |
| **Cookies effacés à la fermeture** | Vous devez vous reconnecter à chaque session, sauf exceptions site par site. |
| **Effets de RFP** | Fuseau horaire présenté comme UTC, thème clair forcé, taille de fenêtre arrondie : c'est voulu. LibreWolf déconseille de modifier ces réglages. |

### 5.3 Pour qui ?

LibreWolf est **idéal sur ordinateur quand la confidentialité prime** : banque, recherches sensibles, données confidentielles.

Il est **déconseillé** sur un ordinateur familial, sur un média center, ou pour quelqu'un qui n'est pas prêt à gérer des exceptions site par site.


gabriel.ananda@mailo.com
CC BY SA

# Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V2.3

## 6. Firefox Multi-Account Containers – Isolez vos identités en ligne

### 6.1 Qu'est-ce que c'est ?

Multi-Account Containers est une extension développée par Mozilla. Elle répartit votre navigation dans des conteneurs isolés (onglets colorés), chacun avec ses propres cookies, son propre cache et ses propres connexions.

### 6.2 En quoi cela améliore-t-il votre vie privée ?

| Problème | Solution apportée |
|---|---|
| Les traqueurs vous suivent d'un site à l'autre via les cookies | Chaque conteneur est isolé : les cookies du conteneur « Réseaux sociaux » ne sont pas lisibles depuis un site d'actualité ouvert dans un autre conteneur. |
| Vous devez vous déconnecter d'un compte pour vous connecter à un autre | Vous pouvez être connecté aux deux comptes en même temps, dans deux conteneurs. |
| Vous mélangez travail et personnel | Créez un conteneur « Travail » et un conteneur « Personnel » ; la couleur de l'onglet rappelle le contexte. |

### 6.3 Limites importantes

| Limite | Explication |
|---|---|
| Ne bloque pas le fingerprinting | Les conteneurs isolent les cookies, pas l'empreinte numérique. |
| Installation manuelle | C'est une extension à ajouter, pas une fonction intégrée. |
| Synchronisation via compte Mozilla | Pratique, mais cela ajoute un compte en ligne. |
| Ne remplace pas uBlock Origin | Les conteneurs gèrent les cookies, pas le blocage des publicités. |

## 7. L'empreinte numérique (fingerprinting) – Pourquoi rien n'est parfait

Le fingerprinting est une technique de pistage qui ne repose pas sur les cookies. Elle combine des caractéristiques de votre navigateur et de votre ordinateur :

- Résolution de l'écran
- Polices installées
- Navigateur et version
- Système d'exploitation
- Matériel (carte graphique, carte son…)


gabriel.ananda@mailo.com
CC BY SA

Combinés, ces éléments peuvent former une empreinte presque unique. Même sans cookies, un site peut alors vous reconnaître.

**Que faire pour mieux résister ?**

- **LibreWolf** : RFP actif par défaut.
- **Brave** : protection contre l'empreinte activée par défaut dans les Boucliers (ajout d'un peu d'aléatoire aux caractéristiques mesurées).
- **Firefox** : *privacy.resistFingerprinting = true* dans *about:config* (approche radicale).
- **Tor Browser** : tous les utilisateurs présentent volontairement la même empreinte (plus lent, pas pour le quotidien).

**Limite :** rien n'est parfait. Utilisez amiunique.org pour mesurer votre propre empreinte.

## 8. Aller plus loin : anti-DPI et anti-fingerprinting avancé

### 8.1 Les outils « anti-DPI » : à quoi servent-ils vraiment ?

Le DPI (Deep Packet Inspection, inspection approfondie des paquets) est utilisé par certains fournisseurs d'accès ou États pour **bloquer ou ralentir** des sites. Les outils anti-DPI modifient la forme de vos paquets (fragmentation, faux paquets) pour que ce filtrage ne se déclenche pas.

⚠️ **Ce qu'ils ne font pas :** ils ne chiffrent rien de plus et **ne cachent pas** à votre fournisseur d'accès les sites que vous visitez. Ce sont des outils de **contournement de la censure**, pas de confidentialité. Pour masquer votre trafic à votre fournisseur d'accès, il faut un VPN de confiance ou Tor.

**Sur Windows :**

- **GoodbyeDPI** (Windows 7 à 11, droits administrateur) : scripts fournis pour l'installer comme service (par exemple *service_install_russia_blacklist.cmd*, conçus pour la Russie). Le projet recommande aussi d'activer le DNS sécurisé (DNS over HTTPS) dans le navigateur.
- **zapret** (via son composant *winws*, droits administrateur).

**Sur Linux :**

- **zapret** (cible principale : Linux et routeurs OpenWrt).
- **SpoofDPI** (proxy local ; pas disponible sur iOS ni Android). Téléchargez-le uniquement depuis son dépôt officiel ou un gestionnaire de paquets officiel.

En France, ces outils n'ont en général pas d'utilité au quotidien : ils servent surtout dans les pays qui pratiquent un blocage par DPI.

### 8.2 Anti-fingerprinting : durcir LibreWolf, Brave ou Firefox

**LibreWolf :** déjà configuré. Rien à faire.

**Brave :**

1. Cliquez sur l'icône **Boucliers** (lion) dans la barre d'adresse.


gabriel.ananda@mailo.com
CC BY SA

2. Vérifiez que la protection contre l'empreinte numérique est **activée** (réglage par défaut).
3. Pour bloquer davantage, réglez le blocage des traqueurs et publicités sur **Agressif** (bloque aussi les publicités propres au site).
4. Pour appliquer ces réglages partout, ouvrez **Paramètres par défaut globaux** depuis le panneau des Boucliers.

Note : l'ancien mode « Strict » contre l'empreinte a été retiré par Brave en 2024 (version 1.64), car il cassait trop de sites.

**Firefox :**

1. Tapez *about:config* dans la barre d'adresse.
2. Recherchez *privacy.resistFingerprinting*.
3. Passez la valeur à *true*.
4. ⚠️ Ce réglage peut casser certains sites (fuseau horaire, taille de fenêtre, thème).

## 9. Tableau récapitulatif des niveaux de protection

| Niveau | Actions à mener | Navigateur recommandé |
|---|---|---|
| **Base** | **uBlock Origin seul** (ou LibreWolf) | Firefox + uBlock Origin, Brave, ou LibreWolf |
| **Anti-fingerprinting renforcé** | RFP (LibreWolf) ou *privacy.resistFingerprinting* (Firefox) | LibreWolf (déjà fait) ou Firefox (radical) |
| **Masquer sa navigation au fournisseur d'accès** | VPN de confiance ou Tor (les outils anti-DPI ne le font pas) | Tous |
| **Contourner une censure par DPI** | GoodbyeDPI (Windows), zapret, SpoofDPI | Tous (outil externe) |

| Navigateur | Bloqueur pubs/traqueurs | Anti-fingerprinting | Open source | Usage quotidien | Recommandé débutant |
|---|---|---|---|---|---|
| **Firefox + uBlock Origin seul** | Bon | Moyen | Oui | Oui | Oui |
| **Brave (Boucliers)** | Excellent | Bon | Oui | Oui (surtout mobile) | Oui |
| **LibreWolf** | Excellent | Très bon | Oui | Oui (ordinateur) | Non (avancé) |


gabriel.ananda@mailo.com
CC BY SA

# Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V2.3

| Navigateur | Bloqueur pubs/traqueurs | Anti-fingerprinting | Open source | Usage quotidien | Recommandé débutant |
|---|---|---|---|---|---|
| **Chromium sans modification** | Aucun | Aucun | Oui | Partiel | Non |
| **Tor Browser** | Très élevé | Très élevé | Oui | Non (lent, parfois bloqué) | Non |

## 10. À savoir avant de se lancer

| Crainte / question fréquente | La réalité |
|---|---|
| « Firefox est-il vraiment mieux que Chrome ? » | Pour la vie privée, oui : sa protection renforcée contre le pistage isole les cookies de chaque site par défaut (Protection totale des cookies) et Firefox accepte toujours uBlock Origin complet. Notez qu'en 2025 Mozilla a retiré de sa FAQ la promesse de « ne jamais vendre vos données » en introduisant des conditions d'utilisation : LibreWolf évite cette question. |
| « Pourquoi ne pas installer Privacy Badger en plus d'uBlock ? » | Il fait doublon avec uBlock Origin, et chaque extension supplémentaire peut rendre votre navigateur plus reconnaissable. |
| « Qu'est-ce que Multi-Account Containers apporte ? » | Il sépare vos identités (travail, perso, banque) en isolant les cookies. C'est complémentaire d'uBlock Origin. |
| « LibreWolf, c'est compliqué ? » | Non, tout est préconfiguré. Certains sites (streaming, WebGL) demandent des réglages manuels. |
| « Puis-je utiliser LibreWolf sur mobile ? » | Non. Sur Android : IronFox (conseillé par LibreWolf), Firefox ou Brave. |
| « Est-ce que les sites vont me bloquer parce que j'utilise LibreWolf ? » | Parfois. Les sites de streaming (DRM) ou très dépendants du fingerprinting peuvent mal fonctionner. |
| « Tor Browser, est-ce légal ? » | Oui, son usage est légal en France. |
| « Les outils anti-DPI cachent-ils ma navigation ? » | Non. Ils contournent un blocage, ils ne cachent pas les sites visités à votre fournisseur d'accès. |


gabriel.ananda@mailo.com
CC BY SA

# Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V2.3

## 11. Challenge 15 jours

**Challenge :** pendant 15 jours, utilisez votre navigateur avec les protections avancées. Ne rouvrez ni Chrome, ni Edge, ni Safari.

**À faire :**

- **Jour 1-2 :** installez Firefox, Brave ou LibreWolf et configurez les protections.
- **Jour 3 :** installez **uBlock Origin seul** (inutile sur Brave et LibreWolf).
- **Jour 4 :** créez vos conteneurs (Travail, Personnel, Banque, Réseaux sociaux) si vous utilisez Firefox.
- **Jour 5 :** assignez vos sites principaux aux bons conteneurs.
- **Jour 6 :** désinstallez Chrome de votre ordinateur.
- **Jour 7 :** allez sur amiunique.org pour mesurer votre empreinte.
- **Jour 8-15 :** naviguez normalement et notez les sites à mettre en exception.

**Vous allez constater :**

- Beaucoup moins de publicités (y compris sur YouTube).
- Des pages souvent plus rapides à charger.
- Moins de bannières de cookies (selon vos listes de filtres).
- La fin de la confusion entre comptes professionnels et personnels.
- Les traqueurs ne vous suivent plus d'un site à l'autre.

## 12. Alternatives et approfondissements

| **Si vous avez besoin de…** | **Essayez plutôt…** |
|---|---|
| Navigateur léger (vieux PC sous Linux) | Falkon (KDE, moteur QtWebEngine) |
| Navigateur open source avec blocage maximal sans réglage | **LibreWolf** ou Tor Browser |
| Navigateur sur iPhone | Brave ou Firefox Focus |
| Navigateur durci sur Android | IronFox, Brave ou Firefox + uBlock Origin |
| Mieux résister au fingerprinting | **LibreWolf** (déjà fait) ou *privacy.resistFingerprinting = true* (Firefox) |
| Naviguer sans laisser de traces sur un ordinateur partagé | Tor Browser (à la fermeture, tout est effacé) |
| Contourner une censure par DPI | GoodbyeDPI (Windows), zapret ou SpoofDPI |


gabriel.ananda@mailo.com
CC BY SA

# Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V2.3

## 13. En résumé (ce que vous gagnez)

| Action | Gagné | Renvoi |
|---|---|---|
| **Remplacer Chrome par Firefox + uBlock Origin seul** | Navigation sans publicités ciblées, sans collecte Google, uBlock Origin complet | § 3 |
| **Utiliser LibreWolf sur ordinateur** | Protection maximale sans réglage, télémétrie désactivée, anti-fingerprinting par défaut | § 5 |
| **Ne pas empiler les extensions** | Navigateur moins reconnaissable | § 4 |
| **Ajouter Multi-Account Containers** | Identités séparées : travail, perso, banque, réseaux sociaux | § 6 |
| **Utiliser Brave sur mobile** | Blocage intégré, aucune extension nécessaire | § 2 |
| **Vérifier sur amiunique.org** | Comprendre ce que votre navigateur révèle | § 7 |
| **Utiliser Tor Browser pour certains besoins** | Anonymat fort (plus lent) | § 2 |
| **Connaître les limites des outils anti-DPI** | Ne pas croire à une protection qu'ils n'offrent pas | § 8 |

## 14. Conclusion générale

| Si vous êtes… | Choisissez… |
|---|---|
| **Ordinateur, usage quotidien** | Firefox + **uBlock Origin seul** + Multi-Account Containers |
| **Mobile au quotidien (surtout Android)** | Brave (Boucliers intégrés) |
| **Utilisateur avancé / exigeant sur ordinateur** | **LibreWolf** (protection maximale, télémétrie désactivée, anti-fingerprinting par défaut) |
| **Anonymat fort ou contournement de la censure** | Tor Browser (usage ponctuel) |

## À retenir absolument

- **Chrome n'exécute plus uBlock Origin complet** (depuis Chrome 139) ; Firefox, LibreWolf et Brave le permettent encore.
- **Une seule extension de blocage suffit : uBlock Origin.** Et aucune extension dans Tor Browser.


gabriel.ananda@mailo.com
CC BY SA

# Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V2.3

- **LibreWolf est le meilleur compromis sur ordinateur** pour une protection maximale sans réglage.
- **Les outils anti-DPI contournent la censure, ils ne cachent pas votre navigation.**

**Test final :**

1. Installez Firefox ou Brave (ou LibreWolf sur ordinateur).
2. Installez **uBlock Origin seul** sur Firefox (rien à ajouter sur Brave ou LibreWolf).
3. Créez au moins 3 conteneurs (Firefox) ou vérifiez les Boucliers (Brave).
4. Assignez vos sites principaux (messagerie pro dans Travail, messagerie perso dans Personnel, réseaux sociaux à part).
5. Vérifiez que la protection renforcée contre le pistage est active.
6. Allez sur amiunique.org pour mesurer votre empreinte.
7. Si tout fonctionne : vous avez nettement amélioré votre vie privée en ligne ✅

## Références


- Chrome for Developers – Calendrier de fin de Manifest V2
- CyberInsider – Google retire uBlock Origin du Chrome Web Store (31 août 2026)
- uBlock Origin Lite – FAQ officielle)
- BleepingComputer – Firefox conserve Manifest V2 (février 2025)
- Brave – Que faire si votre extension n'est plus prise en charge
- Brave – Utiliser les Boucliers (Shields)
- Brave – adblock-rust, moteur de blocage des Boucliers
- TechSpot – Brave abandonne le mode « Strict » anti-empreinte
- EFF – Privacy Badger change pour mieux vous protéger (2020)
- Forum du Tor Project – Faut-il installer des extensions dans Tor Browser ?
- LibreWolf – Fonctionnalités
- LibreWolf – FAQ
- GoodbyeDPI – dépôt officiel
- zapret – documentation
- SpoofDPI – dépôt officiel
- The Register – Mozilla introduit des conditions d'utilisation pour Firefox (mars 2025)
- It's FOSS – Midori 11 (désormais basé sur Firefox)
- AmIUnique
- Brave – Publicités Brave sur option (opt-in)
- Engadget – Brave ajoutait des liens d'affiliation à certaines adresses (juin 2020)



gabriel.ananda@mailo.com
CC BY SA