

Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V2.1

Objectif

Remplacer Chrome, Edge ou Safari par un navigateur respectueux de votre vie privée, qui ne collecte pas vos données de navigation, ne vous trace pas d'un site à l'autre, et vous protège contre les publicités intrusives. Cette fiche vous guide également vers des techniques avancées pour contrer le fingerprinting (empreinte numérique) et le DPI (Deep Packet Inspection), afin d'atteindre un niveau de protection maximal.

• **Public visé** : Intermédiaire / Avancé (quelques lignes de commande et réglages avancés sont nécessaires)

• **Temps estimé** : 30 à 45 minutes

• **Niveau de difficulté** : ★★★☆☆ (Moyen)

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

Navigateur Problème principal

Google Chrome	Collecte massive de données de navigation, synchronisation forcée avec votre compte Google, historique analysé pour le profilage publicitaire, intégration de technos de tracking propriétaires. Depuis le 31 août 2026, Chrome ne supporte plus les extensions Manifest V2, ce qui limite considérablement les bloqueurs puissants .
Microsoft Edge	Envoie votre historique à Microsoft, intègre des services cloud par défaut, synchronisation invasive, télémétrie difficile à désactiver complètement.
Safari (Apple)	Moins mauvais que Chrome, mais reste propriétaire, synchronisé avec iCloud (serveurs US), et Apple peut techniquement accéder à vos données de navigation.

Ce qu'ils font vraiment :

- Ils savent quels sites vous visitez, quand, pendant combien de temps.
- Ils construisent un profil de centres d'intérêt (politique, santé, shopping, etc.).

Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V2.1

- Ils revendent ce profil aux régies publicitaires.
- Ils permettent aux sites de vous tracer d'un site à l'autre (cookies tiers, fingerprinting).

Le bénéfice : Un navigateur qui ne vous connaît pas. Qui bloque les traqueurs, les publicités, et ne vous transforme pas en produit.

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

Navigateur	Moteur	Open source	Blocage natif	Extensions recommandées	Idéal pour
Firefox	Gecko	✓ Oui	Mode protection renforcée	uBlock Origin seul (pas de Privacy Badger)	Usage quotidien (ordinateur)
Brave	Chromium	✓ Oui	uBlock Origin intégré + Shields	Pas besoin (déjà intégré)	Usage quotidien (mobile & desktop)
LibreWolf	Gecko (Firefox)	✓ Oui	Très strict (uBlock intégré)	Déjà configuré	Utilisateurs avancés / exigeants (ordinateur uniquement)
Chromium (vanilla)	Chromium	✓ Oui	Aucun	uBlock Origin (si support MV2)	Puristes open source (mais moins protégé par défaut)
Tor Browser	Gecko (Firefox)	✓ Oui	Extrême (tout bloqué)	Interdit par sécurité	Anonymat fort (whistleblower, contournement censure)

Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V2.1

3. Le changement majeur du 31 août 2026 : Manifest V2 et les extensions

3.1 Ce qui a changé

Le **31 août 2026**, Google a retiré **toutes les extensions Manifest V2 restantes** du Chrome Web Store . Concrètement :

- **uBlock Origin (version complète)** ne fonctionne plus sur Chrome. Les installations existantes sur Chrome 138 ou antérieur continuent de fonctionner, mais ne reçoivent plus de mises à jour et ne peuvent pas être réinstallées .
- **Chrome 139 et versions ultérieures** ne supportent plus du tout les extensions MV2 .
- **uBlock Origin Lite** est la seule version disponible pour Chrome. Elle utilise les API déclaratives de Manifest V3 et **est moins puissante** que la version complète : pas de filtrage dynamique, pas de journal de requêtes, pas de contrôle avancé par site .

3.2 Qui supporte encore uBlock Origin complet ?

Firefox continue de supporter les extensions Manifest V2 et uBlock Origin complet, sur **desktop et Android** . Firefox a confirmé qu'il n'a pas l'intention d'abandonner MV2, et préviendra les développeurs au moins 12 mois à l'avance si cela change .

Brave a choisi de **conserver uBlock Origin et d'autres extensions MV2** en les hébergeant sur ses propres serveurs . Brave continue de supporter AdGuard, uBlock Origin, uMatrix et NoScript .

LibreWolf, en tant que fork de Firefox, bénéficie du même support que Firefox pour uBlock Origin complet.

Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V2.1

3.3 Ce que cela implique pour vos choix

Navigateur	uBlock Origin complet	uBlock Origin Lite	Recommandation
Chrome	× Non supporté	✓ Seule option	Éviter Chrome pour la protection avancée
Edge	× Non supporté	✓ Seule option	Éviter Edge pour la protection avancée
Firefox	✓ Support complet	✓ Disponible	Recommandé
Brave	✓ Support complet (hébergé par Brave)	✓ Disponible	Recommandé
LibreWolf	✓ Intégré par défaut	N/A	Recommandé (avancé)

4. Pourquoi ne pas installer Privacy Badger

4.1 Le problème du fingerprinting

Les recherches montrent que **Privacy Badger augmente significativement l'empreinte numérique** et peut rendre votre navigateur **unique**. Dans certaines configurations testées, Privacy Badger rendait l'utilisateur identifiable de manière unique.

À l'inverse, **uBlock Origin seul réduit légèrement l'empreinte** ou la maintient stable. La recommandation explicite du Tor Project est : « **Utilisez uBlock Origin seul. N'installez pas d'autres extensions au-delà d'uBlock.** »

4.2 Le paradoxe des extensions de confidentialité

Un principe fondamental : **chaque extension ajoutée est une surface d'empreinte supplémentaire** . Un site peut détecter une extension de trois manières :

1. **Ressources accessibles** : l'extension expose des fichiers à des URL identifiables.
2. **Modifications de la page** : un bloqueur supprime des éléments, laisse des traces.
3. **Comportement ajouté** : une extension qui modifie navigator ou canvas laisse des traces détectables.

Quand vous ajoutez **plusieurs extensions de confidentialité**, elles peuvent **se contredire** : deux composants qui essaient de définir les mêmes valeurs créent des incohérences, plus faciles à détecter qu'une seule réponse .

4.3 La règle à retenir

Une seule extension de blocage suffit : uBlock Origin. N'ajoutez pas Privacy Badger, NoScript, ou d'autres extensions de « protection » — elles augmentent votre empreinte au lieu de la réduire.

Exception : Sur Firefox, **Multi-Account Containers** est une extension d'isolation (pas de blocage) qui reste recommandée. Elle isole les cookies entre conteneurs, ce qui est complémentaire à uBlock Origin.

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

5.1 Qu'est-ce que LibreWolf ?

LibreWolf est un **fork indépendant de Firefox**, orienté vers la confidentialité et la sécurité maximales. Il utilise le même moteur Gecko, mais avec une philosophie

Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V2.1

radicalement différente : **confidentialité maximale par défaut, sans configuration manuelle.**

Concrètement, LibreWolf, c'est :

- **Zéro télémétrie** : aucune donnée n'est envoyée à Mozilla.
- **uBlock Origin préinstallé** : dès le premier démarrage, vous bénéficiez d'un des meilleurs bloqueurs, sans avoir à l'installer.
- **Protection anti-fingerprinting par défaut** : la technologie RFP (Resist Fingerprinting), issue du projet Tor, rend votre navigateur aussi « générique » que possible.
- **Cookies effacés à la fermeture** : les sites ne vous gardent pas connecté entre deux sessions, sauf si vous créez des exceptions.
- **DRM désactivés** : Netflix, Spotify et autres services de streaming ne fonctionneront pas sans configuration supplémentaire.
- **WebGL restreint** : Google Earth et certaines applications web interactives peuvent ne pas fonctionner.

5.2 Les contraintes à connaître

Contrainte	Explication
Ordinateur uniquement	Pas de version Android ni iOS. Sur mobile, utilisez Brave ou Firefox.
Pas de synchronisation native	Firefox Sync est désactivé par défaut. Il faut passer par un gestionnaire de mots de passe et un outil de synchronisation de favoris tiers.
DRM désactivés	Netflix, Spotify, Disney+ et autres services de streaming ne fonctionnent pas sans réactivation manuelle.
WebGL restreint	Google Earth, certains jeux en ligne et applications web interactives peuvent ne pas fonctionner.
Cookies effacés à la fermeture	Vous devez vous reconnecter à vos comptes à chaque session, sauf si vous créez des exceptions site par site.

Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V2.1

Contrainte	Explication
Certains sites cassés	La protection stricte peut casser des sites mal codés ou dépendants du fingerprinting.

5.3 Pour qui ?

LibreWolf est **idéal pour un usage desktop où la confidentialité prime** : ordinateur personnel, banque, recherches sensibles, travail sur des données confidentielles.

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

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 permet de diviser votre navigation en conteneurs isolés (onglets colorés), chacun ayant ses propres cookies, son propre cache et ses propres identifiants de connexion.

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 de Facebook dans le conteneur « Réseaux sociaux » ne peuvent pas être lus quand vous visitez un site d'actualité dans un autre

Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V2.1

Problème	Solution apportée
	conteneur.
Vous devez vous déconnecter d'un compte pour vous connecter à un autre	Vous pouvez être connecté aux deux comptes simultanément dans deux conteneurs différents.
Vous mélangez travail et personnel	Créez un conteneur « Travail » et un conteneur « Personnel ». Les couleurs des onglets vous rappellent le contexte.

6.3 Limites importantes

Limite	Explication
Ne bloque pas le fingerprinting	Les conteneurs isolent les cookies, mais pas l'empreinte numérique.
Nécessite une installation manuelle	Ce n'est pas une fonction intégrée par défaut, c'est une extension à ajouter.
La synchronisation nécessite un compte Mozilla	Cela peut réduire légèrement l'anonymat.
Ne remplace pas uBlock Origin	Les conteneurs gèrent les cookies, mais pas la suppression des publicités.

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

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

- Résolution de l'écran
- Polices installées

Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V2.1

- Navigateur et sa version
- Système d'exploitation
- Configuration matérielle (GPU, carte son, etc.)

Ces éléments combinés forment une empreinte unique. Même sans cookies, un site peut vous reconnaître à chaque visite.

Que faire pour mieux résister ?

- LibreWolf** : protection anti-fingerprinting active par défaut (RFP).
- Brave** : Shields → Strict fingerprinting.
- Firefox** : `privacy.resistFingerprinting = true` dans `about:config` (approche radicale).
- Tor Browser** : tous les utilisateurs Tor ont une empreinte volontairement identique (mais lent, pas pour le quotidien).

Limite : Rien n'est parfait. Les sites très motivés (Google, Meta) contournent souvent les protections. Utilisez amiunique.org pour vérifier votre propre empreinte.

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

8.1 Anti-DPI : contourner l'analyse de votre FAI

LibreWolf, Brave et Firefox n'intègrent pas de fonction anti-DPI. Il faut installer un outil complémentaire :

Sur Windows :

- GoodbyeDPI (avec interface graphique)** : installez en tant que service pour un démarrage automatique.
- SpoofDPI** : lancez en tant qu'administrateur.

Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V2.1

Sur Linux :

- **Zapret** (script automatisé)
- **GoodbyeDPI-Linux**
- **SpoofDPI**

8.2 Anti-fingerprinting : durcir LibreWolf, Brave ou Firefox

LibreWolf : déjà configuré. Rien à faire.

Brave :

1. brave://flags
2. Recherchez brave-show-strict-fingerprinting-mode
3. Activez, redémarrez.
4. Dans Brave Shields & Privacy, réglez le blocage des traqueurs sur « Aggressif ».

Firefox :

1. about:config
2. Recherchez privacy.resistFingerprinting
3. Passez à true.
4. **Attention** : ce paramètre peut casser certains sites.

9. Tableau récapitulatif des niveaux de protection

Niveau	Actions à mener	Navigateur recommandé
Base	uBlock Origin seul (ou LibreWolf)	Firefox + uBlock Origin, ou LibreWolf
Anti-fingerprinting renforcé	RFP (LibreWolf) ou privacy.resistFingerprinting (Firefox)	LibreWolf (déjà fait) ou Firefox (radical)
Anti-DPI	Installer GoodbyeDPI, SpoofDPI ou	Les deux (outil externe)

Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V2.1

Niveau	Actions à mener	Navigateur recommandé
	Zapret	
Niveau maximal	Coupler anti-DPI + anti-fingerprinting + VPN	LibreWolf (configuré) + outil externe + VPN

Navigateur	Bloqueur pubs/traqueurs	Anti-fingerprinting	Open source	Usage quotidien	Recommandé débutant
Firefox + uBlock Origin seul	Bon	Moyen	Oui	Oui	Oui
Brave (Shields max)	Excellent	Bon	Oui	Oui (surtout mobile)	Oui
LibreWolf	Excellent	Très bon	Oui	Oui (léger)	Non (avancé)
Chromium nu	Aucun	Aucun	Oui	Partiel	Non
Tor Browser	Extrême	Extrême	Oui	Non (lent, bloqué)	Non

10. À savoir avant de se lancer

Crainte / question fréquente

La réalité

« Firefox est-il vraiment mieux que Chrome ? »

Oui — Firefox bloque par défaut les traqueurs sociaux, les cookies tiers, et ne vend pas vos données. De plus, Firefox supporte uBlock Origin complet, contrairement à Chrome .

« Pourquoi ne pas installer Privacy Badger en plus de uBlock ? »

Parce que Privacy Badger augmente votre empreinte numérique au lieu de la réduire. uBlock Origin seul est plus efficace pour la discrétion .

Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V2.1

Crainte / question fréquente

La réalité

- « Qu'est-ce que Multi-Account Containers apporte ? » Il isole vos identités (travail, perso, banque) en séparant les cookies. C'est complémentaire à uBlock Origin, et ça ne pose pas de problème de fingerprinting.
- « LibreWolf, c'est compliqué ? » Non, tout est préconfiguré. Mais certains sites (streaming, WebGL) demanderont des réglages manuels.
- « Puis-je utiliser LibreWolf sur mobile ? » Non — LibreWolf n'existe que sur ordinateur. Sur mobile, utilisez Brave ou Firefox.
- « Est-ce que les sites vont me bloquer parce que j'utilise LibreWolf ? » Parfois. Les sites très « DRM » (streaming) ou dépendants du fingerprinting peuvent mal fonctionner.
- « Tor Browser, est-ce légal ? » Oui — Totalement légal en France et dans la plupart des démocraties.
- « L'outil anti-DPI est-il légal ? » Oui — ils contournent l'analyse du trafic, pas le chiffrement.
-

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** (pas de Privacy Badger).
- **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.

Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V2.1

•**Jour 7** : Allez sur amiunique.org pour vérifier votre empreinte numérique.

•**Jour 8-15** : (Optionnel) Installez un outil anti-DPI si nécessaire.

Vous allez constater :

- Beaucoup moins de publicités (y compris sur YouTube).
 - Chargement des sites plus rapide.
 - Moins de bannières « Acceptez les cookies ».
 - 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...

Navigateur ultra-léger (vieux PC)

Navigateur open source avec blocage maximal sans config

Navigateur sur iOS (iPhone)

Éviter le fingerprinting plus efficacement

Naviguer sans laisser de traces sur un ordinateur partagé

Contourner la censure ou l'analyse de votre FAI

Essayez plutôt...

Falkon (KDE) ou Midori (basés QtWebEngine)

LibreWolf ou Tor Browser

Brave ou Firefox Focus

LibreWolf (déjà fait) ou `privacy.resistFingerprinting = true` (Firefox)

Tor Browser (fermeture = tout disparaît)

GoodbyeDPI, SpoofDPI ou Zapret

Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V2.1

13. En résumé (ce que vous gagnez)

Action	Gagné
Remplacer Chrome par Firefox + uBlock Origin seul	Navigation sans publicités ciblées, sans collecte Google, open source. uBlock Origin complet fonctionne sur Firefox, contrairement à Chrome .
Utiliser LibreWolf sur ordinateur	Protection maximale sans configuration, zéro télémétrie, anti-fingerprinting par défaut
Ne pas installer Privacy Badger	Empreinte numérique réduite, meilleure discrétion
Ajouter Multi-Account Containers	Isolation des identités : travail, perso, banque, réseaux sociaux séparés
Utiliser Brave sur mobile	Blocage intégré, navigation rapide, respectueuse de la vie privée. Brave supporte uBlock Origin complet .
Activer la protection stricte	Moins de fingerprinting (sans garantie absolue)
Consulter amiunique.org	Comprendre que votre navigateur vous identifie, même avec des blocages
Utiliser Tor Browser pour certains besoins	Anonymat presque total (lent, mais efficace)
Installer un outil anti-DPI	Contourner l'analyse de votre FAI

14. Conclusion générale

Si vous êtes...	Choisissez...
Ordinateur quotidien	Firefox + uBlock Origin seul + Multi-Account Containers
Mobile quotidien (surtout Android)	Brave (bloqueur intégré Shields, support uBlock

Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V2.1

Si vous êtes...

Choisissez...

Origin)

Utilisateur avancé / exigeant sur ordinateur

LibreWolf (protection maximale, zéro télémétrie, anti-fingerprinting par défaut)

Anonymat extrême ou contournement de censure

Tor Browser (usage ponctuel uniquement)

Ce qu'il faut retenir :

- **Depuis le 31 août 2026**, Chrome ne supporte plus uBlock Origin complet. **Firefox et Brave sont les seuls navigateurs majeurs à le supporter .**
- **N'installez pas Privacy Badger** : il augmente votre empreinte numérique au lieu de la réduire. **Une seule extension de blocage suffit : uBlock Origin .**
- **LibreWolf est le meilleur compromis sur ordinateur** pour qui veut une protection maximale sans configuration.
- **Multi-Account Containers** reste recommandé sur Firefox : il isole les cookies sans augmenter le fingerprinting.
- **À tester absolument** : amiunique.org — vous serez surpris de voir à quel point votre navigateur vous identifie, même avec des protections actives.

Test final

1. Installez Firefox ou Brave (ou LibreWolf si vous êtes sur ordinateur et exigeant).
2. Installez **uBlock Origin seul** (pas de Privacy Badger).
3. Créez au moins 3 conteneurs (si Firefox) ou activez Shields Strict (si Brave).
4. Assignez vos sites principaux (Gmail pro dans Travail, Gmail perso dans Personnel, Facebook dans Réseaux sociaux).
5. Activez la protection stricte contre le pistage.
6. (Optionnel) Installez un outil anti-DPI si nécessaire.
7. Allez sur amiunique.org pour mesurer votre empreinte.

Si tout fonctionne : vous avez considérablement amélioré votre vie privée en ligne.