

## Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V1.1

**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.

**Public visé** : Débutant à Intermédiaire

**Temps estimé** : 15 minutes

**Niveau de difficulté** : ★★☆☆☆ (Facile)

---

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


Navigateur	Problème principal
------------	--------------------

<b>Google Chrome</b>	Collecte massive de données de navigation, synchronisation forcée avec votre compte Google, historique analysé pour le profilage publicitaire, intégration de technos de tracking propriétaires.
<b>Microsoft Edge</b>	Envoie votre historique à Microsoft, intègre des services cloud par défaut, synchronisation invasive, télémétrie difficile à désactiver complètement.
<b>Safari (Apple)</b>	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.)
- Ils revendent ce profil aux régies publicitaires

---

1  Vous débutez ? Commencez par la fiche N°2, plus courte et plus simple. Revenez ici quand vous voulez comprendre les limites de la protection.

## Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V1.1

•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
<b>Firefox</b>	Gecko (maison)	✓ Oui	Mode protection renforcée	uBlock Origin + Privacy Badger + <b>Multi-Account Containers</b>	Usage quotidien (ordinateur)
<b>Brave</b>	Chromium	✓ Oui	Bloqueur intégré (Shields)	X Pas besoin (déjà intégré)	Usage quotidien (mobile & desktop)
<b>Chromium (vanilla)</b>	Chromium	✓ Oui	✗ Aucun	uBlock Origin + Privacy Badger	Puristes open source (mais moins protégé par défaut)
<b>LibreWolf</b>	Gecko (Firefox)	✓ Oui	Très strict (uBlock intégré)	✗ Déjà configuré	Utilisateurs avancés / exigeants
<b>Tor Browser</b>	Gecko (Firefox)	✓ Oui	Extrême (tout bloqué)sécurité	✗ Interdit par	Anonymat fort (whistleblower, contournement censure)

## Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V1.1

### Notre recommandation selon votre profil :

Si vous êtes...	Choisissez...
Débutant / usage quotidien (ordinateur)	<b>Firefox</b> + uBlock Origin + Privacy Badger + <b>Multi-Account Containers</b>
Débutant / usage quotidien (mobile)	<b>Brave</b> (bloqueur intégré, plus simple)
Exigeant mais simple sur mobile	<b>Brave</b> (excellent sur Android/iOS)
Puriste open source (ordinateur)	<b>LibreWolf</b> (Firefox durci)
Vous voulez absolument du Chromium sans Google	Chromium (vanilla) + extensions (mais moins recommandé)
Vous avez besoin d'un anonymat extrême	<b>Tor Browser</b> (pas pour le quotidien)
<p><b>⚠ Attention :</b> Aucun navigateur n'est une panacée (solution magique). Même avec Firefox, Brave ou Tor, il existe des techniques avancées de <b>fingerprinting</b> (empreinte numérique) qui permettent de vous identifier. Nous y reviendrons.</p>	

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

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

**Multi-Account Containers** est une extension développée par **Mozilla** elle-même . 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 .

Concrètement, les données d'un conteneur ne peuvent **pas** être lues par un autre conteneur . Vous pouvez ainsi :

## Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V1.1

- Être connecté à **deux comptes Gmail différents** en même temps (un dans le conteneur "Personnel", l'autre dans "Travail") .
- Empêcher Facebook de traquer votre navigation sur d'autres sites, en l'isolant dans son propre conteneur .
- Séparer vos activités professionnelles, bancaires, shopping et personnelles en un coup d'œil grâce aux **couleurs** des onglets .

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

Problème	Solution apportée par Multi-Account Containers
Les traqueurs (Facebook, Google, etc.) vous suivent d'un site à l'autre via les cookies	Chaque conteneur est <b>isolé</b> . Les cookies de Facebook dans le conteneur "Réseaux sociaux" ne peuvent pas être lus quand vous visitez un site d'actualité dans un autre conteneur .
Vous devez vous déconnecter d'un compte pour vous connecter à un autre (ex: deux Gmail)	Vous pouvez être connecté aux <b>deux comptes simultanément</b> dans deux conteneurs différents .
Vous mélangez travail et personnel, avec des risques de confusion	Créez un conteneur "Travail" et un conteneur "Personnel". Les couleurs des onglets vous rappellent en permanence dans quel contexte vous êtes .
Vous êtes vulnérable aux attaques via des liens malveillants	Un clic malveillant reste <b>confiné</b> dans son conteneur et ne peut pas compromettre vos autres identifiants .

### 3.3 Installation étape par étape

#### Étape 1 : Installez l'extension

1. Ouvrez **Firefox**.
2. Cliquez sur le menu (trois traits en haut à droite) → **Extensions et thèmes** .
3. Recherchez "**Firefox Multi-Account Containers**".

## Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V1.1

4. Cliquez sur "**Ajouter à Firefox**" puis sur "**Ajouter**".

5. L'icône de l'extension (trois carrés avec un +) apparaît dans la barre d'outils.

### Étape 2 : Découvrez les conteneurs par défaut

Par défaut, l'extension crée plusieurs conteneurs :

- **Personnel**
- **Travail**
- **Banque**
- **Shopping**

### Étape 3 : Ouvrez un nouvel onglet dans un conteneur

- Cliquez sur l'icône **Multi-Account Containers** dans la barre d'outils.
- Sélectionnez le conteneur souhaité (ex: "Shopping").
- Un nouvel onglet **coloré** s'ouvre. Tout ce que vous faites dans cet onglet reste isolé.

💡 **Astuce** : Vous pouvez aussi faire un **clic droit** sur le bouton "Nouvel onglet" (+) pour choisir directement le conteneur.

## 3.4 Configurer des conteneurs personnalisés

### Créer un nouveau conteneur :

1. Cliquez sur l'icône Multi-Account Containers.
2. Cliquez sur "**Gérer les conteneurs**" (Manage Containers).
3. Cliquez sur "**Nouveau conteneur**" (New Container).
4. Donnez-lui un **nom** (ex: "Réseaux sociaux"), choisissez une **couleur** et une **icône**.
5. Cliquez sur "**OK**".

### Affecter un site à un conteneur (automatisation) :

Pour qu'un site s'ouvre **toujours** dans le même conteneur :

1. Ouvrez le site dans le conteneur souhaité.
2. Cliquez sur l'icône Multi-Account Containers dans la barre d'outils.

## Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V1.1

3. Cochez "**Toujours ouvrir ce site dans...**" (Always Open This Site in...) et sélectionnez le conteneur .

💡 **Option avancée** : Vous pouvez aussi **limiter un conteneur aux seuls sites qui lui sont assignés** (Limit to Designated Sites). Cela empêche d'y ouvrir accidentellement un autre site .

### 3.5 Utilisation avancée

#### Ouvrir un lien dans un conteneur spécifique :

- Faites un **clic droit** sur n'importe quel lien.
- Choisissez "**Ouvrir le lien dans un nouveau conteneur**" (Open Link in New Container) → sélectionnez le conteneur .

#### Ouvrir un favori dans un conteneur :

1. Allez dans les paramètres de l'extension.
2. Activez "**Activer le menu des favoris**" (Enable bookmarks menu) .
3. Désormais, un clic droit sur un favori propose "**Ouvrir le favori dans un onglet conteneur**" .

#### Synchroniser vos conteneurs entre plusieurs ordinateurs :

- Connectez-vous à un **compte Mozilla** dans Firefox.
- Dans les paramètres de l'extension, activez la synchronisation.
- Vos conteneurs (noms, couleurs, icônes, assignations de sites) seront synchronisés sur tous vos appareils connectés .

### 3.6 Tableau récapitulatif : actions et bénéfices

Action	Bénéfice
Installer Multi-Account Containers	Isolez vos identités en ligne : travail, perso, banque, shopping
Créer un conteneur "Réseaux"	Facebook et Twitter ne peuvent plus vous tracer sur

## Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V1.1

Action	Bénéfice
sociaux"	d'autres sites
Assigner un site à un conteneur	Automatisation : plus besoin de penser à changer manuellement
Utiliser des couleurs par conteneur	Repérage visuel immédiat : vous savez dans quel contexte vous êtes
Synchroniser avec un compte Mozilla	Même organisation sur tous vos ordinateurs

### 3.7 Limites importantes

Limite	Explication
<b>Ne bloque pas le fingerprinting</b>	Les conteneurs isolent les cookies, mais pas l'empreinte numérique (voir section 5).
<b>Nécessite une installation manuelle</b>	Ce n'est pas une fonction intégrée par défaut, c'est une extension à ajouter .
<b>La synchronisation nécessite un compte Mozilla</b>	Cela peut réduire légèrement l'anonymat.
<b>Ne remplace pas uBlock Origin</b>	Les conteneurs gèrent les cookies, mais pas la suppression des publicités ou des traqueurs tiers.

💡 **Comparaison avec Facebook Container** : Facebook Container isole automatiquement Facebook. Multi-Account Containers est plus généraliste mais nécessite une configuration manuelle. Vous pouvez utiliser les **deux** simultanément, mais installez d'abord Multi-Account Containers, puis désassociez [facebook.com](https://facebook.com) , [messenger.com](https://messenger.com) et [instagram.com](https://instagram.com) avant d'installer Facebook Container .

## Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V1.1

### 4. Comment faire ? (Le pas à pas général)

#### Méthode A : Firefox (ordinateur – recommandé)

##### Étape 1 : Téléchargez et installez Firefox

1. Rendez-vous sur [firefox.com](https://www.firefox.com)
2. Cliquez sur "Télécharger" (gratuit)
3. Lancez l'installation (Windows : .exe, Mac : .dmg, Linux : paquet .deb ou .rpm)

##### Étape 2 : Ajoutez les extensions de blocage et d'isolation

1. Ouvrez Firefox → cliquez sur les trois traits (menu hamburger) en haut à droite
2. **Extensions et thèmes** → Rechercher des extensions
3. Installez **uBlock Origin** (bloque publicités, traqueurs, scripts malveillants)
4. Installez **Privacy Badger** (bloque les traqueurs invisibles, créé par EFF)
5. Installez **Firefox Multi-Account Containers** (isole vos identités en ligne)
6. (Optionnel) CanvasBlocker (perturbe l'empreinte numérique – fingerprinting)

##### Étape 3 : Activez la protection renforcée

1. Menu → **Paramètres** → **Vie privée et sécurité**
2. Dans "Protection renforcée contre le pistage", cochez "**Stricte**"
3. Décochez les cases d'analyse (envoi de données techniques à Mozilla) si vous le souhaitez.

##### Étape 4 : Configurez vos conteneurs

- Ouvrez quelques conteneurs personnalisés (Travail, Personnel, Banque, Réseaux sociaux)
- Assignez les sites que vous utilisez le plus souvent

#### Méthode B : Brave (mobile et ordinateur – excellent pour smartphone)

##### Étape 1 : Téléchargez Brave

## Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V1.1

- Ordinateur : [brave.com/download](https://brave.com/download)
- Android / iPhone : Play Store ou App Store

### Étape 2 : Activez les protections maximales

- 1.Lancez Brave → cliquez sur l'icône lion (Shields) dans la barre d'adresse
- 2.Réglez :

- Traqueurs et publicités bloqués → **Strict**
- Mise à niveau vers HTTPS → **Toujours**
- Cookies → **Bloque les cookies tiers**
- Fingerprinting → **Strict**

### Étape 3 : Désactivez les récompenses (Rewards) (optionnel)

Brave a un système facultatif de cryptomonnaies (Rewards). Allez dans **Paramètres** → **Crypto** → désactivez tout si vous ne souhaitez pas y participer.

### Étape 4 : Synchronisation privée (si plusieurs appareils)

Brave permet une synchronisation chiffrée sans compte central. Cliquez sur l'icône QR code dans **Paramètres** → **Synchronisation** → créez une chaîne privée.

## Méthode C : Chromium (vanilla) – pour les puristes open source

Chromium est la version sans Google du code source de Chrome. Mais attention : il ne bloque rien par défaut.

**Notre avis** : Chromium ne n'est pas recommandé pour la vie privée. Il est techniquement open source mais ne contient aucun bouclier. Firefox ou Brave sont bien meilleurs par défaut.

## Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V1.1

### Méthode D : LibreWolf (Firefox déjà durci)

LibreWolf est une version de Firefox pré-configurée pour la vie privée maximale (résistance au fingerprinting, téléphonie désactivée, uBlock Origin intégré).

**Utilisation** : Rien à configurer, c'est déjà fait. Par défaut, il oublie tout à la fermeture (sauf si vous paramétrez autrement).

---

### 5. 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
- 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 ?

- Activez les protections anti-fingerprinting dans **Brave** (Shields → Strict fingerprinting)
- Sur **Firefox** : installez **CanvasBlocker** et passez en mode fenêtre privée / résolution standard
- La solution quasi totale : **Tor Browser** (tous les utilisateurs Tor ont une empreinte volontairement identique)

## Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V1.1

⚠ **Limite** : Rien n'est parfait. Les navigateurs privés réduisent le risque, mais les sites très motivés (Google, Meta) contournent souvent les protections.

### Comment vérifier votre propre empreinte ?

Allez sur [amiunique.org](https://amiunique.org) (site de l'Université de Lorraine). Cliquez sur "Voir mon empreinte".

- Résultat : "Votre navigateur est unique parmi X millions".
- Plus ce chiffre est bas, mieux vous êtes protégé (idéal : vous n'êtes pas unique).

### 6. Tableau récapitulatif des niveaux de protection

Navigateur	Bloqueur pubs/trace urs	Anti-fingerprinting	Open source	Usage quotidien	Recommandé débutant
Firefox + uBlock + Privacy Badger + Containers	✓ Bon	✓ Moyen	✓ Oui	✓ Oui	✓ Oui
Brave (Shields max)	✓ Excellent	✓ Bon	✓ Oui	✓ Oui	✓ Oui (surtout mobile)
LibreWolf	✓ Excellent	✓ Très bon	✓ Oui	✓ Oui (léger)	⚠ Plutôt avancé
Chromium nu	✗ Aucun	✗ Aucun	✓ Oui	⚠ Partiel	✗ Non
Tor Browser	✗ Extrême	✓ Extrême	✓ Oui	✗ Non (lent, bloqué)	✗ Non

## Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V1.1

### 7. 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.
"Brave est-il un navigateur de cryptomineurs?"	Non – Brave a eu une polémique en 2020 (insertion automatique d'affiliations). Ils ont corrigé depuis. Le navigateur est aujourd'hui excellent pour la vie privée, et vous pouvez désactiver les Rewards.
"Qu'est-ce que Privacy Badger apporte en plus de uBlock?"	uBlock bloque les listes connues ; Privacy Badger <b>apprend</b> dynamiquement les traqueurs que vous rencontrez. Ensemble, ils sont complémentaires.
"Les conteneurs Firefox, c'est compliqué à configurer?"	Non – l'extension est simple à prendre en main. Vous pouvez commencer avec les conteneurs par défaut (Personnel, Travail, Banque, Shopping) et créer les vôtres au fur et à mesure .
"Puis-je utiliser les conteneurs sur mobile?"	Non – Multi-Account Containers n'existe que sur la version ordinateur de Firefox.
"Est-ce que les sites vont me bloquer parce que j'utilise Brave?"	Très rare. Certains sites très "DRM" (streaming, banques) peuvent demander Chrome, mais c'est l'exception. Brave émule Chrome – il est reconnu comme Chrome par 99 % des sites.
"Tor Browser, est-ce légal?"	Oui – Totalement légal en France et dans la plupart des démocraties. Utiliser Tor n'est pas un délit.

### 8. Challenge 7 jours

**Challenge** : Pendant 7 jours, utilisez uniquement **Firefox + uBlock Origin + Privacy Badger + Multi-Account Containers** (ordinateur) et **Brave** (téléphone). Ne rouvrez ni Chrome, ni Edge, ni Safari.

## Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V1.1

### À faire :

- 1.**Jour 1-2** : Installez Firefox et les trois extensions (uBlock, Privacy Badger, Multi-Account Containers)
- 2.**Jour 3** : Créez vos conteneurs (Travail, Personnel, Banque, Réseaux sociaux)
- 3.**Jour 4** : Assignez vos sites principaux aux bons conteneurs (ex: toujours ouvrir Gmail Travail dans le conteneur Travail)
- 4.**Jour 5** : Utilisez les conteneurs toute la journée – observez les couleurs des onglets
- 5.**Jour 6** : Désinstallez Chrome de votre ordinateur
- 6.**Jour 7** : Allez sur [amiunique.org](https://amiunique.org) pour vérifier votre empreinte numérique

### Vous allez constater :

- Beaucoup moins de publicités (y compris sur YouTube)
- Chargement des sites plus rapide (moins de scripts traqueurs)
- Moins de bannières "Acceptez les cookies" (uBlock en bloque certaines)
- Fin de la confusion entre comptes professionnels et personnels
- Les traqueurs ne vous suivent plus d'un site à l'autre

## 9. Alternatives et approfondissements

### Si vous avez besoin de...

### Essayez plutôt...

Navigateur ultra-léger (vieux PC)	Falkon (KDE) ou Midori (basés QtWebEngine)
Navigateur open source avec blocage maximal sans config	LibreWolf ou Tor Browser
Navigateur sur iOS (iPhone)	Brave ou Firefox Focus (n'oublie rien)
Éviter le fingerprinting plus efficacement	Activez <code>privacy.resistFingerprinting = true</code> dans <code>about:config</code> (Firefox)
Naviguer sans laisser de traces sur un ordinateur partagé	Tor Browser (fermeture = tout disparaît)

## Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V1.1

### 10. En résumé (ce que vous gagnez)

Action	Gagné
Remplacer Chrome par <b>Firefox + uBlock Origin</b>	Navigation sans publicités ciblées, sans collecte Google, open source
Ajouter <b>Privacy Badger</b>	Protection supplémentaire contre les traqueurs novices
Ajouter <b>Multi-Account Containers</b>	Isolation des identités : travail, perso, banque, réseaux sociaux séparés
Utiliser <b>Brave</b> sur mobile	Blocage intégré, navigation rapide, respectueux de la vie privée (et mieux que Chrome sur Android)
Activer la protection stricte dans Firefox / Brave	Moins de fingerprinting (sans garantie absolue)
Consulter <a href="https://amiunique.org">amiunique.org</a>	Comprendre que votre navigateur vous identifie, même avec des blocages
Utiliser <b>Tor Browser</b> pour certains besoins précis	Anonymat presque total (lent, mais efficace)

### 11. Conclusion générale

Si vous êtes...	Choisissez...
Ordinateur quotidien	<b>Firefox + uBlock Origin + Privacy Badger + Multi-Account Containers</b> (le combo gagnant)
Mobile quotidien (surtout Android)	<b>Brave</b> (bloqueur intégré Shields, plus simple et efficace)
Puriste open source / exigeant sur vie privée	<b>LibreWolf</b> (Firefox déjà durci)
Anonymat extrême ou	<b>Tor Browser</b> (usage ponctuel uniquement)

## Fiche Pratique N°11 : Naviguez sans être pisté – Protection avancée V1.1

Si vous êtes...

Choisissez...

---

contournement de censure

---

### Ce qu'il faut retenir :

- Aucun navigateur n'est une **panacée**. Le fingerprinting reste une menace. Tor Browser est le seul à uniformiser les empreintes, mais il est trop lent pour un usage quotidien.
  - Multi-Account Containers** est un outil puissant qui vient compléter uBlock Origin et Privacy Badger. Il isole les cookies et les identifiants, mais ne bloque pas les publicités ni le fingerprinting.
  - À tester absolument** : [amiunique.org](https://amiunique.org) – vous serez surpris de voir à quel point votre navigateur vous identifie, même avec des protections actives.
- 

### Test final :

1. ☒ Installez Firefox
2. ☒ Ajoutez uBlock Origin, Privacy Badger et Multi-Account Containers
3. ☒ Créez au moins 3 conteneurs (Travail, Personnel, Réseaux sociaux)
4. ☒ Assignez vos sites principaux (Gmail pro dans Travail, Gmail perso dans Personnel, Facebook dans Réseaux sociaux)
5. ☒ Ouvrez les mêmes sites dans différents conteneurs – vérifiez que vous êtes connecté à des comptes différents
6. ☒ Activez la protection stricte contre le pistage
7. ☒ Allez sur [amiunique.org](https://amiunique.org) pour mesurer votre empreinte

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