

Les navigateurs

- Historique et généralités
- Les navigateurs courant
- Le fonctionnement
- Favoris, historique, mots de passe
- Cookies, token, popups
- Extensions
- Dangers-précautions

Par Etienne Moret. La plupart des textes sont fourni par l'IA de infomaniak :
<https://euria.infomaniak.com/>

Les navigateurs

- Le couteau suisse du travail avec d'autres ordinateurs
- Depuis l'invention du WorldWideWeb (1990)
- C'est le client qui pilote l'interaction

Navigateurs : fonctionnement

- Protocole http (exemple)
- Pages fixes/ pages dynamiques
- Travail sur le serveur
- Travail sur le client

Navigateurs : principales fonctions

- Barre de navigation
- Historique
- Favoris
- Téléchargements
- Supprimer les données de navigation
- Paramètres : confidentialité et sécurité
- Menus, Hyperliens

Navigateurs : dangers pour les clients

Les navigateurs sont la porte d'entrée vers internet pour les utilisateurs et constituent une cible de choix pour dérober des données personnelles ou prendre le contrôle de l'appareil.

- **Phishing (Hameçonnage) et Ingénierie Sociale** : Création de sites web frauduleux imitant des banques, réseaux sociaux ou services connus pour tromper l'utilisateur et lui voler ses identifiants, numéros de carte bancaire ou autres données sensibles.
- **Malvertising (Publicité Malveillante)** : Injection de code malveillant dans des réseaux publicitaires légitimes. L'utilisateur est infecté simplement en visitant un site et en chargeant une publicité compromise, sans même cliquer dessus (attaque "drive-by download").

Navigateurs : dangers pour les clients

- **Exploitation de Failles du Navigateur (Zero-days)** : Utilisation de vulnérabilités inconnues dans le moteur du navigateur (Chrome, Firefox, Safari, etc.) ou ses extensions pour exécuter du code à distance, installer des malwares ou prendre le contrôle de l'appareil.
- **Vol de Cookies et Session Hijacking** : Interception des cookies de session (souvent via des attaques XSS ou sur des réseaux Wi-Fi non sécurisés) pour usurper l'identité de l'utilisateur et accéder à ses comptes sans mot de passe.
- **Cryptojacking** : Utilisation discrète des ressources de l'appareil de l'utilisateur (CPU/GPU) via un script dans le navigateur pour miner de la cryptomonnaie à l'insu de la victime, ralentissant considérablement l'appareil.

Navigateurs : dangers pour les clients

- **Extensions Malveillantes** : Des extensions de navigateur, parfois téléchargées en grand nombre avant d'être transformées en outils d'espionnage, peuvent surveiller l'historique, voler des données ou injecter du contenu dans les pages visitées.
- **Attaques par Fingerprinting (Empreinte Numérique)** : Collecte passive d'informations sur la configuration du navigateur et de l'appareil pour créer une empreinte unique permettant de suivre l'utilisateur à travers le web, même sans cookies.

Navigateurs : protection

Navigateurs à jour, bloqueurs de publicité et de traqueurs (uBlock Origin, Brave), vigilance face au phishing, extensions de sécurité, utilisation de gestionnaires de mots de passe, et désactivation des fonctionnalités inutiles (JavaScript si possible, Flash obsolète).

Les cookies : description

Les cookies sont de petits fichiers texte placés sur votre appareil par un site web pour mémoriser des informations lors de votre navigation. Leurs fonctions principales sont :

- **Fonctionnement technique (Cookies essentiels)** : Ils sont indispensables au bon fonctionnement de nombreux sites. Ils permettent de se souvenir de votre panier d'achat, de votre langue préférée, ou de votre état de connexion (vous restent connecté après avoir fermé la page). Sans eux, de nombreuses fonctionnalités web modernes seraient impossibles.
- **Suivi et personnalisation (Cookies de tracking)** : Ils permettent aux sites de mémoriser votre comportement (pages visitées, temps passé) pour personnaliser l'expérience utilisateur (recommandations de produits, contenu adapté).
- **Publicité ciblée** : Ils sont utilisés par les réseaux publicitaires pour suivre votre navigation à travers différents sites et vous afficher des publicités basées sur vos centres d'intérêt présumés.

Les cookies : description

L'utilisation des cookies, en particulier ceux de suivi, soulève plusieurs problématiques majeures :

- **Atteinte à la vie privée** : Le suivi transversal permet de créer des profils détaillés des utilisateurs, révélant leurs habitudes, leurs préférences politiques, leur santé ou leur situation financière sans leur consentement explicite et éclairé.
- **Vol de données et piratage** : Si un cookie n'est pas sécurisé (par exemple, s'il n'est pas marqué "HttpOnly" ou "Secure"), il peut être intercepté par des attaquants via des attaques de type "Man-in-the-Middle" ou "Cross-Site Scripting (XSS)", permettant de dérober des sessions de connexion ou des données sensibles.
- **Manipulation et bulles de filtres** : L'accumulation de données via les cookies permet aux algorithmes de ne montrer aux utilisateurs que des informations qui confirment leurs opinions préexistantes, renforçant la polarisation sociale et facilitant la désinformation.
- **Surconsommation et addiction** : Certains mécanismes de cookies, combinés à des algorithmes, sont conçus pour maximiser le temps passé sur une plateforme, exploitant les biais psychologiques pour encourager une consommation excessive de contenu ou d'achats impulsifs.

Les cookies : protection

Se protéger contre les cookies et les popups nécessite une combinaison de paramètres navigateur, d'extensions et de comportements de navigation. Voici les méthodes les plus efficaces :

- **Utiliser la navigation privée** : Mode "Incognito" (Chrome, Edge) ou "Navigation Privée" (Firefox, Safari). Les cookies et l'historique sont effacés automatiquement à la fermeture de la fenêtre. Idéal pour une navigation ponctuelle, mais ne protège pas contre le traçage en temps réel.
- **Configurer les paramètres du navigateur** :
 - **Bloquer les cookies tiers** : Désactivez les cookies de suivi tiers dans les paramètres de confidentialité de votre navigateur. Ils sont souvent responsables du profilage cross-site.
 - **Refuser les cookies de tous les sites** : L'option la plus stricte, mais elle risque de casser le fonctionnement de nombreux sites (panier d'achat, connexion).
 - **Suppression automatique** : Configurez votre navigateur pour qu'il supprime les cookies et les données de site à chaque fermeture.

Les cookies : protection

Utiliser des extensions de blocage :

uBlock Origin : Le blocage le plus complet. Il filtre non seulement les publicités, mais aussi de nombreux scripts de traçage et les cookies tiers par défaut.

Privacy Badger (EFF) : Apprend automatiquement à bloquer les traqueurs qui vous suivent à travers le web.

Cookie AutoDelete : Supprime automatiquement les cookies inactifs après un délai défini.

Changer de navigateur : Des navigateurs comme Brave (bloquant natif), DuckDuckGo ou Firefox (avec protection renforcée) offrent une meilleure confidentialité par défaut que Chrome ou Safari.

Les token : description

Les Tokens d'Authentification (Sécurité Informatique)

Dans le domaine de la sécurité web et des applications, un token est une chaîne de caractères utilisée pour authentifier un utilisateur sans qu'il ait à renvoyer son mot de passe à chaque requête.

- **Fonctionnement :**
 - L'utilisateur se connecte une fois avec ses identifiants.
 - Le serveur génère un token unique (souvent un JWT - JSON Web Token) et l'envoie au navigateur.
 - Le navigateur stocke ce token (dans le localStorage, sessionStorage ou un cookie).
 - À chaque demande suivante, le navigateur envoie ce token avec la requête. Le serveur le valide et autorise l'accès.

Les token : danger

Rôles :

- Maintenir la session : Éviter de devoir se reconnecter à chaque page.
- Sécurité : Le token a une durée de vie limitée. S'il est volé, il n'est utile que pendant un court laps de temps.
- Décentralisation : Contrairement aux sessions traditionnelles stockées sur le serveur, les tokens permettent une architecture "stateless" (sans état), idéale pour les applications distribuées.

- **Dangers :**

- Vol de session (XSS) : Si un site web est vulnérable à des injections de scripts, un attaquant peut voler le token et usurper l'identité de l'utilisateur.
- Stockage non sécurisé : Stocker un token dans le localStorage le rend accessible par n'importe quel script du site, augmentant le risque de vol via XSS.
- Rejet de token (Token Replay) : Si le token n'a pas de durée de vie courte ou de mécanisme de révocation, un attaquant qui l'intercepte peut l'utiliser indéfiniment.

Les popups : définition et avantages

Les popups (fenêtres contextuelles) sont des éléments d'interface web qui s'affichent par-dessus le contenu principal d'une page. Leur utilisation soulève un débat constant entre efficacité marketing et expérience utilisateur.

Taux de conversion élevé : C'est leur principal atout. Une étude de Sumo indique que les popups bien conçus peuvent générer jusqu'à 10 % de nouvelles inscriptions à une newsletter. Ils captent l'attention immédiatement, là où un simple bandeau peut être ignoré.

Collecte de données ciblée : Ils permettent de récupérer des informations précieuses (emails, préférences, données de contact) au moment le plus pertinent, par exemple juste avant qu'un utilisateur ne quitte le site (popup de sortie) ou après qu'il a consulté une page spécifique.

Communication d'urgences ou d'offres : Idéal pour mettre en avant des promotions limitées dans le temps, des lancements de produits ou des alertes importantes (maintenance, changements de tarifs) sans encombrer la navigation permanente.

Segmentation de l'audience : Les popups modernes peuvent être conditionnés (ex: n'afficher qu'aux visiteurs venant d'une source spécifique ou aux nouveaux visiteurs), rendant le message plus pertinent et moins intrusif.

Les popups : inconvénients et risques

- **Expérience utilisateur dégradée** : C'est le défaut majeur. Une popup qui bloque le contenu immédiatement à l'arrivée est souvent perçue comme agressive, frustrante et peut pousser l'utilisateur à quitter le site (taux de rebond accru).
- **Impact négatif sur le référencement (SEO)** : Google pénalise les pages où la popup bloque le contenu principal sur mobile ou où elle est difficile à fermer. Cela peut nuire au positionnement du site dans les résultats de recherche.
- **Désengagement et fatigue** : Un excès de popups (pop-up fatigue) entraîne une désensibilisation. L'utilisateur finit par les fermer systématiquement sans lire, ou développe une aversion envers la marque, perçue comme "spammeuse".
- **Problèmes d'accessibilité** : Les popups mal codés peuvent être inaccessibles aux personnes utilisant des lecteurs d'écran ou la navigation au clavier, violant ainsi les normes d'accessibilité web (WCAG).

Les popups : protection

- **Activer le bloqueur de popups intégré** : La plupart des navigateurs modernes (Chrome, Firefox, Edge, Safari) ont un bloqueur de popups activé par défaut. Assurez-vous qu'il n'est pas désactivé dans les paramètres.
- **Extensions de blocage avancées** :
 - **uBlock Origin** : Extrêmement efficace pour bloquer les popups, les fenêtres contextuelles de publicité et les redirections malveillantes.
 - **Popup Blocker (spécifiques)** : Des extensions dédiées peuvent être installées si le navigateur ne suffit pas.
- **Ne pas cliquer sur les faux boutons de fermeture** : Beaucoup de popups malveillants imitent une croix "X" qui, si on clique dessus, lance en fait une publicité ou un téléchargement. Cherchez toujours le vrai bouton de fermeture, souvent plus petit ou moins visible.
- **Ignorer les demandes d'autorisation** : Si un site demande "Autoriser les notifications ?" ou "Autoriser les popups ?", cliquez toujours sur **Bloquer** ou **Refuser**, sauf si vous faites confiance au site.

Les popups : bonnes pratiques

- **Mettre à jour régulièrement** : Les navigateurs et les extensions de sécurité sont mis à jour fréquemment pour contrer les nouvelles techniques de contournement.
- **Vérifier les permissions** : Dans les paramètres du navigateur, vérifiez les sites ayant reçu l'autorisation d'afficher des popups ou d'accéder à vos notifications et révoquez-les si nécessaire.
- **Utiliser un DNS privé** : Des services comme AdGuard DNS ou NextDNS peuvent bloquer les domaines connus pour héberger des publicités et des popups au niveau du réseau, avant même qu'ils n'atteignent votre navigateur.

En combinant un navigateur sécurisé (comme Firefox ou Brave) avec une extension comme **uBlock Origin**, vous bloquerez la grande majorité des cookies de tracking et des popups intrusifs sans sacrifier la fonctionnalité des sites légitimes.

Fenêtre de navigation privée

Brave ne se souvient jamais de ce que vous faites dans une fenêtre de navigation privée. Les sites que vous consultez n'apparaissent pas dans votre historique. Les cookies, les données de formulaire et les données de site disparaissent lorsque vous fermez toutes les fenêtres de navigation privée. Veuillez noter que votre activité de navigation peut toujours être visible par toute personne ou entreprise pouvant accéder à votre réseau comme votre FAI ou votre employeur (si vous naviguez sur un réseau professionnel). Pour plus de confidentialité, ouvrez une fenêtre de navigation privée avec Tor.

Navigation privée

La navigation privée (appelée "Incognito" sur Chrome, "InPrivate" sur Edge, "Navigation privée" sur Firefox) offre des avantages réels, mais souvent surestimés. Voici ce qu'elle fait FAIT (avantages réels)

1. Pas d'historique local conservé :

- Les pages visitées ne sont pas enregistrées dans l'historique du navigateur
- Les recherches ne restent pas dans la barre d'adresse
- Utile pour cacher votre activité aux autres personnes utilisant le même ordinateur

2. Pas de cookies persistants :

- Les cookies créés pendant la session sont automatiquement supprimés à la fermeture
- Empêche le suivi publicitaire basé sur les cookies d'une session à l'autre
- Permet de se connecter à plusieurs comptes différents sur un même site (ex : deux comptes Gmail) sans déconnexion manuelle

Navigation privée

3. **Pas de données de formulaires enregistrées :**

- Les mots de passe, adresses et informations de carte bancaire ne sont pas sauvegardés
- Réduit le risque qu'une autre personne accède à ces données sur votre machine

4. **Séparation des sessions :**

- Les extensions (sauf celles explicitement autorisées) sont généralement désactivées
- Isolement de la session normale, utile pour tester des sites sans interférence

Navigation privée

Ce que la navigation privée NE FAIT PAS (limites importantes)

1. **Vous n'êtes PAS anonyme sur Internet :**

- Votre fournisseur d'accès Internet (FAI) voit toujours votre activité
- Les sites web visités peuvent toujours identifier votre adresse IP
- Votre employeur ou administrateur réseau peut toujours tracer votre navigation

2. **Pas de protection contre le fingerprinting :**

- Les sites peuvent toujours vous identifier via votre configuration (résolution d'écran, polices installées, version du navigateur, etc.)
- Cette technique de "prise d'empreinte" contourne totalement la navigation privée

Navigation privée

3. Les moteurs de recherche vous tracent toujours :

- Google, Bing et autres enregistrent vos recherches liées à votre adresse IP
- Seule une connexion via VPN ou l'utilisation de moteurs respectueux de la vie privée (DuckDuckGo, Qwant, Startpage) change cela

4. Pas de chiffrement supplémentaire :

- La navigation privée n'ajoute aucune couche de sécurité comme le ferait un VPN
- Les données transitent de la même manière, avec les mêmes vulnérabilités potentielles

5. Les téléchargements et favoris restent :

- Les fichiers téléchargés sont conservés sur votre disque dur
- Les pages ajoutées aux favoris pendant la session privée sont sauvegardées

Navigation privée

Bonnes utilisations :

- Cacher son historique aux autres utilisateurs de l'appareil
- Se connecter à un compte secondaire sans déconnecter le premier
- Éviter que les cookies publicitaires ne persistent après la session
- Tester un site web sans cache ni cookies précédents
- Rechercher des cadeaux ou informations sensibles sur un ordinateur partagé

Insuffisant pour :

- Une véritable anonymisation (préférez Tor Browser)
- Se protéger contre la surveillance du FAI ou gouvernementale (préférez un VPN)
- Naviguer sur des réseaux publics non sécurisés (préférez un VPN)
- Échapper au fingerprinting avancé

Navigation privée

La navigation privée est un outil de **confidentialité locale** (vis-à-vis des autres utilisateurs de votre appareil), pas un outil d'**anonymat en ligne**. Comme le soulignent plusieurs analyses en 2025-2026, c'est une "illusion dangereuse" si vous croyez qu'elle vous rend invisible sur Internet. Pour une protection complète, combinez-la avec un VPN, un moteur de recherche respectueux de la vie privée, et éventuellement le navigateur Tor pour les usages sensibles.

Navigation privée

Sources :

- <https://www.lesnumeriques.com/antivirus/decryptage-la-navigation-privee-suffit-elle-a-proteger-vos-informations-a221302.html>
- <https://www.phonandroid.com/navigation-privee-chrome-safari-firefox-vraie-protection-illusion.html>
- <https://www.manageengine.com/fr/blog/general/navigation-privee-mythe-ou-realite-en-matiere-de-confidentialite.html>
- <https://lecrabeinfo.net/tutoriels/pourquoi-la-navigation-privee-nest-pas-si-privee-5-idees-faussees-et-dangereuses/>

Les navigateurs : vue d'ensemble

- Pour la **compatibilité et l'écosystème** : Chrome ou Edge.
- Pour la **vie privée et l'indépendance** : Firefox ou Brave.
- Pour les **utilisateurs Apple** : Safari (indispensable pour l'autonomie).
- Pour la **personnalisation** : Vivaldi.
- Pour les **fonctionnalités intégrées** : Opera.
- Pour les **gamers** : Opera GX.



Les navigateurs : Google Chrome

Le navigateur le plus utilisé au monde, référence du marché.

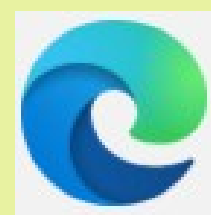
- **Caractéristiques** : Basé sur le moteur Chromium, écosystème d'extensions immense, synchronisation complète avec le compte Google, mises à jour fréquentes.
- **Avantages** : Compatibilité totale avec tous les sites web, bibliothèque d'extensions la plus vaste, performance élevée, interface intuitive, synchronisation fluide entre appareils.
- **Inconvénients** : Gourmand en mémoire RAM (impact sur la batterie et les performances), collecte massive de données personnelles pour le profilage publicitaire, dépendance à Google.



Les navigateurs : Mozilla Firefox

Le seul grand navigateur indépendant, non basé sur Chromium.

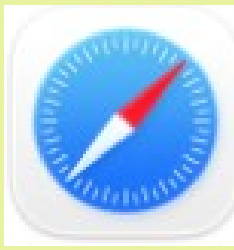
- **Caractéristiques** : Moteur de rendu Gecko, développé par une fondation à but non lucratif, personnalisation poussée, protection renforcée de la vie privée par défaut.
- **Avantages** : Respect strict de la vie privée (blocage des traqueurs natif), indépendance vis-à-vis des géants technologiques, personnalisation avancée de l'interface, consommation mémoire optimisée avec de nombreux onglets.
- **Inconvénients** : Légèrement moins rapide que Chrome sur certains benchmarks, compatibilité parfois imparfaite avec des sites optimisés exclusivement pour Chromium, bibliothèque d'extensions plus limitée.



Les navigateurs : Microsoft Edge

Le successeur d'Internet Explorer, désormais basé sur Chromium.

- **Caractéristiques** : Moteur Chromium, intégration profonde avec Windows et l'écosystème Microsoft, assistant IA Copilot intégré nativement, mode "Efficacité" pour économiser la batterie.
- **Avantages** : Performance excellente (souvent supérieure à Chrome sur Windows), fonctionnalités innovantes (onglets verticaux, lecture à voix haute avancée), intégration IA native, compatibilité totale avec les extensions Chrome.
- **Inconvénients** : Collecte de données importante (télémétrie Microsoft), interface parfois chargée avec des fonctionnalités intrusives (shopping, jeux), difficulté à le désinstaller complètement de Windows.



Les navigateurs : Apple Safari

Le navigateur par défaut sur tous les appareils Apple.

- **Caractéristiques** : Moteur WebKit, optimisation exclusive pour macOS et iOS, intégration avec l'écosystème Apple (iCloud Keychain, Handoff), focus sur l'efficacité énergétique.
- **Avantages** : Consommation énergétique minimale (meilleure autonomie sur MacBook/iPhone), rapidité exceptionnelle sur appareils Apple, protection intelligente contre le pistage (Intelligent Tracking Prevention), intégration fluide avec les services Apple.
- **Inconvénients** : Exclusivité Apple (indisponible sur Windows/Android), bibliothèque d'extensions très limitée, mises à jour liées aux versions du système d'exploitation, compatibilité web parfois en retard.



Les navigateurs : Brave

Le navigateur axé sur la confidentialité et la rapidité.

- **Caractéristiques** : Basé sur Chromium, bloqueur de publicités et de traqueurs natif, système de récompenses cryptographiques (BAT), navigation privée avec Tor intégrée.
- **Avantages** : Rapidité exceptionnelle (grâce au blocage natif des pubs), protection de la vie privée par défaut sans configuration, compatibilité avec les extensions Chrome, fonctionnalités Web3 intégrées.
- **Inconvénients** : Modèle économique basé sur la cryptomonnaie pouvant rebuter certains utilisateurs, blocage agressif pouvant casser certains sites, notoriété encore limitée, controverses passées sur certaines pratiques.



Les navigateurs : Opera / Opera GX

Le navigateur riche en fonctionnalités intégrées.

- **Caractéristiques** : Basé sur Chromium, VPN gratuit intégré, bloqueur de pubs natif, barre latérale avec messageries (WhatsApp, Telegram), version "GX" dédiée aux gamers.
- **Avantages** : Fonctionnalités intégrées sans besoin d'extensions (VPN, bloqueur), interface moderne et personnalisable, version GX avec limiteurs de ressources (CPU/RAM) pour les gamers, synchronisation multi-appareils.
- **Inconvénients** : Propriété d'un consortium chinois depuis 2016 (questions sur la confidentialité), collecte de données utilisateur, interface pouvant sembler chargée, moins de transparence que Firefox ou Brave.



Les navigateurs : Vivaldi

Le navigateur ultra-personnalisable pour utilisateurs avancés.

- **Caractéristiques** : Basé sur Chromium, personnalisation extrême de l'interface, gestion avancée des onglets (empilement, division d'écran), outils de productivité intégrés (notes, calendrier).
- **Avantages** : Personnalisation inégalée (chaque élément de l'interface), fonctionnalités de productivité natives, respect de la vie privée, gestion exceptionnelle des nombreux onglets.
- **Inconvénients** : Courbe d'apprentissage raide pour les nouveaux utilisateurs, interface par défaut moins épurée, performances légèrement inférieures à Chrome sur les machines modestes, niche pour utilisateurs power users.

Moteurs de recherche : Google

C'est le leader incontesté du marché, détenant la quasi-totalité des parts de marché mondiales.

- **Caractéristiques** : Algorithme extrêmement performant, indexation massive du web, intégration profonde avec l'écosystème (Maps, YouTube, Gmail) et fonctionnalités IA avancées (SGE).
- **Avantages** : Pertinence des résultats inégalée, vitesse d'exécution, capacité à comprendre l'intention de recherche complexe et services associés gratuits.
- **Inconvénients** : Collecte massive de données personnelles (profilage publicitaire), position dominante anticoncurrentielle, et opacité des critères de classement.

Moteurs de recherche : Bing (Microsoft)

Le principal concurrent historique de Google, désormais propulsé par l'IA de Microsoft.

- **Caractéristiques** : Intégration native dans Windows et Edge, partenariat avec OpenAI pour l'assistant Copilot, récompenses fidélité (Microsoft Rewards).
- **Avantages** : Excellente recherche d'images et de vidéos, interface conversationnelle via Copilot intégrée directement dans les résultats, programme de fidélité attractif.
- **Inconvénients** : Parts de marché faibles (moins de résultats indexés que Google), collecte de données similaire à Google bien que moins massive, interface parfois chargée.

Moteurs de recherche : DuckDuckGo

La référence en matière de protection de la vie privée.

- **Caractéristiques** : Ne trace pas les utilisateurs, ne stocke pas d'adresses IP, agrège les résultats de plusieurs sources (dont Bing) sans créer de profil.
- **Avantages** : Confidentialité totale, pas de "bulle de filtres" (les résultats sont identiques pour tous), interface épurée, extensions de navigateur pratiques.
- **Inconvénients** : Résultats parfois moins pertinents pour les requêtes très locales ou complexes, dépendance technologique vis-à-vis de Bing pour une partie de l'indexation, moins de fonctionnalités avancées (traduction, maps).

Moteurs de recherche : Qwant

Le moteur de recherche français et européen, axé sur la souveraineté numérique.

- **Caractéristiques** : Respect strict du RGPD, indexation propre (bien qu'utilisant aussi des partenaires pour combler), interface neutre sans publicité ciblée.
- **Avantages** : Protection des données garantie par la loi française, soutien à l'économie locale, fonctionnalités dédiées à l'actualité et aux réseaux sociaux (Qwant Boards).
- **Inconvénients** : Qualité des résultats parfois inférieure à Google pour les requêtes techniques ou internationales, notoriété encore limitée hors de France.

Moteurs de recherche : Ecosia

Le moteur de recherche écologique basé en Allemagne.

- **Caractéristiques** : Utilise ses revenus publicitaires pour planter des arbres, transparence financière (publication des rapports), indexation basée sur Bing.
- **Avantages** : Impact environnemental positif concret, respect de la vie privée (pas de vente de données), extension navigateur facile à utiliser.
- **Inconvénients** : Vitesse de recherche légèrement inférieure, résultats moins précis que Google, dépendance à Bing pour la technologie sous-jacente.

Moteurs de recherche : Brave Search

Un challenger récent qui construit son propre index indépendant.

- **Caractéristiques** : Index indépendant (ne dépend ni de Google ni de Bing), intégré au navigateur Brave, option "Goggles" pour personnaliser les algorithmes de classement.
- **Avantages** : Indépendance technologique, confidentialité forte, résultats souvent plus diversifiés et moins biaisés par les géants du web.
- **Inconvénients** : Index encore en construction (certains résultats manquants), notoriété faible, interface moins riche en fonctionnalités annexes.

Moteurs de recherche : IA (Perplexity, etc.)

Une nouvelle catégorie émergente en 2026.

- **Caractéristiques** : Génère des réponses synthétiques plutôt qu'une liste de liens, cite les sources, utilise le traitement du langage naturel.
- **Avantages** : Gain de temps considérable pour les recherches complexes, réponses directes et contextualisées, capacité de dialogue.
- **Inconvénients** : Risques d'hallucinations (fausses informations), opacité des sources parfois, coût (souvent payant pour les versions avancées), moindre sérendipité (découverte fortuite).

Moteurs de recherche : en résumé

En résumé :

- Pour la **pertinence pure** : Google reste imbattable.
- Pour la **vie privée** : DuckDuckGo ou Qwant.
- Pour l'**écologie** : Ecosia.
- Pour l'**intégration IA** : Bing (Copilot) ou Perplexity.
- Pour l'**indépendance** : Brave Search.

Sources : Clubic, Tool-Advisor, BeVisible, Jeremie-andre.fr
(données 2025-2026).

Les extensions (exemples)

Sécurité et confidentialité :

- **uBlock Origin** : Bloqueur de publicités léger et efficace, open source
- **Privacy Badger** : Bloque les traqueurs invisibles automatiquement
- **HTTPS Everywhere** : Force l'utilisation de connexions sécurisées
- **Bitwarden** : Gestionnaire de mots de passe gratuit et open source
- **ClearURLs** : Supprime les éléments de suivi des URLs

Les extensions (exemples)

Productivité :

- **OneTab** : Réduit la consommation mémoire en regroupant les onglets
- **Todoist** ou **TickTick** : Gestion de tâches directement dans le navigateur
- **Grammarly** : Correction grammaticale (principalement anglais)
- **Dark Reader** : Mode sombre pour tous les sites web
- **Session Buddy** : Gestion et sauvegarde des sessions d'onglets

Les extensions (exemples)

Recherche et information :

- **Reverse Image Search** : Recherche d'images inversée rapide
- **Wayback Machine** : Accède aux versions archivées des sites
- **Reader View** : Mode lecture pour articles sans distractions

Spécifiques à Firefox :

- **Container Tabs** : Isolation des sessions par site (exclusif Firefox)
- **Multi-Account Containers** : Gestion de plusieurs comptes par site

Les extensions (exemples)

Conseils d'utilisation :

- Limitez le nombre d'extensions actives pour préserver les performances
- Privilégiez les extensions open source et régulièrement mises à jour
- Vérifiez les permissions demandées avant installation
- Désactivez les extensions inutilisées

Sources : Les Numériques, Aiegeek, ExpressVPN, Clubic (2026)

Formations en ligne

<https://www.clic-formation.net/navigateur-web.html>

<https://cours-informatique-gratuit.fr/cours/les-navigateurs-internet/>

<https://nolimit.support/atelier/penser-web-surfer-sur-internet>

<https://openclassrooms.com/fr/courses/5870011-naviguez-sur-internet>

<https://www.axetcompetences.ch/formations/naviguer-sur-internet>