

Sécurité de votre navigateur Web Firefox et dérivés



Que voit le site que vous visitez?

Votre navigateur, Internet Explorer, Firefox, Abrowser, IceCat, Iceweasel, Epiphany, Midori, Chromium, Konqueror, Chrome, Safari, Opera envoie une quantité importante d'informations sur votre résolution d'écran, votre système informatique, l'heure de votre horloge, votre abonnement chez tel FAI, votre logiciel lorsqu'il accède à une page. Les sites que vous visitez utilisent des logiciels trackers, des mouchards, d'espionnage et déposent des cookies dans votre disque dur.

Vérifiez vous-même ce que véhicule votre navigateur

<http://www.anonymat.org/vostraces/index.php>

<https://www.cnil.fr/fr/votre-ordinateur>

Cliquez, vous êtes traqués : <https://www.youtube.com/watch?v=RfGF3OI2D5o>

<https://www.cnil.fr/fr/comment-ca-marche>

En mars 2014, en Allemagne, où l'utilisation de Google Chrome est déconseillée par l'autorité allemande de sûreté des techniques d'information, Firefox conserve sa place de leader avec 36,7% des visites mais perd toujours du terrain. Derrière Internet Explorer et Safari, Google Chrome arrive en 4ème position avec « seulement » 15,9% des visites.

<http://www.atinternet.com/documents/safari-marque-le-pas-en-europe/>

Le navigateur de Microsoft Internet Explorer est très souvent **vulnérable**

<http://www.cert.ssi.gouv.fr/site/CERTFR-2014-ALE-005/CERTFR-2014-ALE-005.html>

<http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-001/index.html>

La version de Windows 10 vous espionne

<https://www.youtube.com/watch?v=kBJn82TU63c>

Le nouveau système d'exploitation de Microsoft tout juste disponible continue à faire parler de lui côté protection des données personnelles. On a affaire un ordinateur tricheur, indiscret, violant la vie privée de chaque utilisateur. **Il suffit de lire les conditions d'utilisation de Microsoft :**

<https://www.microsoft.com/fr-fr/privacystatement/default.aspx>

Votre antivirus gratuit, si populaire, vous protège-t-il ?

La colonne 1 indique les fonctions d'un antivirus gratuit, il ne vous protège que peu

Le logiciel antivirus le plus populaire au monde :
Bientôt plus de 184 131 718 d'utilisateurs

Le leader français de la publication sur l'informatique CommentCaMarche.net a récompensé avast! avec son prix «Logiciel de référence» (pour le meilleur logiciel gratuit).

	avast! Free Antivirus	avast! Pro Antivirus	avast! Internet Security
Antivirus avec anti-espion <small>JAMÉLIORÉ</small> La protection minimale que tous les PC devraient avoir.	✓	✓	✓
Réalisez vos achats et opérations bancaires en toute sécurité <small>NOUVEAU</small> La technologie SafeZone™ assure la confidentialité de vos comptes.	✗	✓	✓
Protégez votre identité et vos données Le pare-feu silencieux bloque automatiquement les attaques de pirates.	✗	✗	✓
Débarassez-vous des SPAM L'antispam évite que des courriers indésirables n'entrent dans votre boîte de courriers entrant.	✗	✗	✓
	TÉLÉCHARGER usage domestique*	TÉLÉCHARGER et en savoir plus	TÉLÉCHARGER et en savoir plus

* avast! Free Antivirus est destiné à un usage personnel et non commercial uniquement.

Pourquoi choisir AVAST | Configuration requise | Technologie | Autres options

Procurez-vous un antivirus de confiance, primé et éprouvé par plus de 184 millions d'utilisateurs

Les icônes de Facebook sur les sites que vous visitez

Il faut savoir que lorsque est inséré sur la page d'un site le logo «J'aime» ou «Partager» de Facebook ce ne sont pas de simples liens mais une petite page web de la taille d'une icône qui permet à Facebook de savoir qui a lu quel contenu du site et à quel moment.

<https://www.youtube.com/watch?v=3xRgOWeV8NA>

L'Europe défend le droit à la protection des données personnelles : la messagerie d'un irlandais contre les géants de l'informatique, Microsoft.

<http://www.lemondeinformatique.fr/actualites/lire-patriot-act-l-irlande-defend-le-droit-a-la-protection-des-donnees-personnelles-59714.html>

Certains objecteront peut-être qu'ils n'ont rien à se reprocher, ni à cacher. **Tolériez-vous que votre facteur ouvre vos courriers, les lise, les photocopie et garde une copie à vie ? Évidemment non.** Ayez les mêmes exigences avec internet.

L'utilisation d'internet amène à la violation de droits fondamentaux, notamment la vie privée de l'internaute. Nous pouvons affirmer que le respect de la vie privée est un des piliers de la démocratie, que les régimes politiques, où cela ne l'est pas, s'appellent des régimes totalitaires. On a tous le droit à une vie privée et le chiffrement est la seule technologie qui permette de protéger vraiment cette vie privée. Donc soustraire ce droit à 60 millions de Français sous prétexte que quelques barbus islamistes pourraient utiliser cette fonctionnalité de chiffrement, c'est comme interdire les voitures parce que ça peut permettre à des terroristes de se déplacer rapidement, ou fermer les écoles parce qu'il y a des pédophiles en France.

Ce qu'en pense la CNIL (Commission nationale de l'informatique et des libertés) :

«Lorsqu'on ne s'étonne plus du traçage, de la vidéosurveillance ou de la conservation des données, c'est justement le signal qu'on est entré dans un monde orwellien.»

[Alex Türk](#), ex-président de la CNIL

<https://www.cnil.fr/fr/cookies-et-autres-traceurs-premier-bilan-des-controles>

Concrètement, sécuriser son navigateur

Installez des modules complémentaires dans votre navigateur :
à installer dans Firefox → Outils → extensions

Calomel = qualité de HTTPS des sites visités (on a parfois des surprises avec celui de certaines banques)

<https://addons.mozilla.org/fr/firefox/addon/calomel-ssl-validation/?>

[src=search](#)

Flash Video Downloader = enregistre des vidéos dans le dossier Téléchargements

<https://addons.mozilla.org/en-US/firefox/addon/6584>

HTTPS-EVERYWHERE = Favorise le HTTPS (qui est chiffré) par rapport au HTTP (qui n'est pas chiffré).

<https://www.eff.org/https-everywhere>

DownThemAll = continuer un téléchargement arrêté

<https://addons.mozilla.org/fr/firefox/addon/downthemall/?src=cb-dl-users>

Un des deux modules anti-publicité

uBlock Origin = antipub le + puissant

<https://addons.mozilla.org/fr/firefox/addon/ublock-origin/?src=ss>

Paramétrage → Ouvrir Firefox → Outils → Modules complémentaires → Préférences → afficher le tableau de bord → Listes de filtres → cocher la case *Anti-Thirdparty social*

AdBlock Edge = une version modifiée de AdBlock Plus qui ne considère pas qu'il y a des pubs acceptables.

<https://addons.mozilla.org/fr/firefox/addon/adblock-edge/>

Un anti-cookie

Self-Destructing-cookies = Détruit les cookies et les données LocalStorage (stockés localement) à la fermeture des onglets, tout en permettant de définir des listes blanches.

<https://addons.mozilla.org/fr/firefox/addon/self-destructing-cookies/?src=search>

Un des deux anti-trackers

NoScript = Permet de choisir quand un script est autorisé à être exécuté.

<https://noscript.net/>

Ghostery = anti-trackers et anti-espions (n'est plus libre mais plus facile à gérer que NoScript)

<https://addons.mozilla.org/fr/firefox/addon/ghostery/?src=cb-dl->

users

Paramétrage → Ouvrir Firefox → Outils → Modules complémentaires → Préférences → Cocher toutes les cases → Menu Blocking Options → Cliquer Block all categories

Les anti-espions

Privacy-Badger = anti-espions

<https://www.eff.org/privacybadger>

Policy-Control = Aide au contrôle de politique que vous désirez rapidement désactiver et permettre différents types de ressources telles que le Javascript, CSS, et médias. L'extension peut être employée pour augmenter la confidentialité de vie privée en bloquant le contenu non désiré

<http://firefox.add0n.com/policy-control.html>

Comment effectuer vos recherches sur internet avec google ou un autre moteur de recherche ?

Un moteur de recherche est une application web permettant de retrouver des ressources (pages web, articles de forums Usenet, images, vidéo, fichiers, etc.) associées à des mots quelconques.

- [Ask](#) (multilingue)
- [Baidu](#) (chinois)
- [Bing](#) (multilingue)
- [Blekkio](#) (anglais)
- [DuckDuckGo](#) (multilingue)
- [Dazoo FR](#) (français)
- [Exalead](#) (français)
- [Gigablast](#) (anglais)
- [Google](#) (multilingue)
- [LeMoteur](#) (français)
- [Lycos](#) (multilingue)

- [Mozbot](#) (multilingue)

- [Panguso](#) (chinois)

- [Qwant](#) (multilingue)
- [Sohu](#) (chinois)

- [Soso](#) (chinois)
- [Naver](#) (Coréen)
- [V9](#) (chinois, multilingue)
- [Voila](#) (français)
- [Yahoo!](#) (multilingue)
- [Yandex](#) (russe, anglais)
- [Tinghir](#) (multilingue,)

Classement des moteurs de recherche en pourcentage des chercheurs uniques ayant effectuée une recherche sur un ou plusieurs moteurs de recherche en décembre 2012

Ran g	Moteur de recherche	Part des recherches
1	Google	76,6 %
2	Baidu	19,2 %
3	Yahoo	19,2 %
4	Microsoft	17,6 %
5	Yandex	4,9 %

Classement des [robots d'indexation](#) en part des [collectes](#) de [page](#) totales

Ran g	Robot d'indexation	Part des collectes de page totales
1	Googlebot	60,5 %
2	MSN/Bing Bot	24,5 %
3	Baidu Spider	4,4 %
4	Majestic12 Bot	3,0 %
5	Yandex Bot	2,3 %
6	Autres	3,0

Le plus utilisé est Google mais il est très indiscret

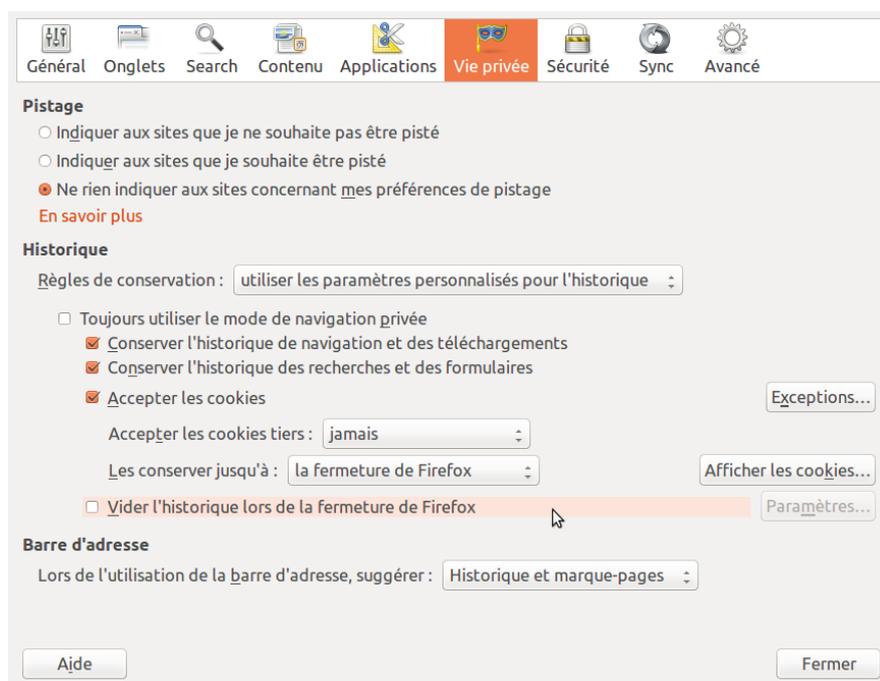
1 . Vous pouvez passer par un [proxy](#) qui utilise une nouvelle adresse IP lors de chaque recherche, reçoit le cookie à votre place et le supprime ensuite.

2 . Vous pouvez configurer votre navigateur **Firefox**

- **Options > Vie privée > Cochez Toujours utiliser le mode de navigation privée. Les sites ne le respectent peu car vous ne pourrez plus ouvrir de nombreuses pages.**

- *Utiliser des paramètres personnalisés*

Vous pouvez cocher la ligne accepter les cookies et mettre à cookies tiers : **Jamais** . **Les sites ne le respectent peu car vous ne pourrez plus ouvrir certaines pages.**



4. Je préfère installer l'extension **Self-Destructing-cookies** qui détruit les cookies et les données LocalStorage (stockés localement) à la fermeture des onglets, tout en permettant de définir des listes blanches.

<https://addons.mozilla.org/fr/firefox/addon/self-destructing-cookies/?src=search>

5 . La meilleure solution en plus de configuration précédente de votre navigateur web est de passer par un *autre moteur de recherche plus respectueux de votre vie privée* qui respecte votre confidentialité

En voici quelques uns

- <https://www.qwant.com/> (Français)
- [DuckDuckGo](#) (Américain)
- [disconnect](#) (Américain) Pour des recherches sur Google, Bing, Yahoo ou encore Blekko et DuckDuckGo, le tout en restant anonyme et insensible à 100% aux différents outils de traçage mais demande des cookies.
- [Ixquick](#) (Néerlandais) Ixquick fonctionne globalement de la même façon que DuckDuckGo. Il va chercher ses résultats sur dix autres moteurs et sites Internet, dont AOL, Bing, Google et Wikipédia.
- [Framabee](#) (Français) Le moteur de recherches de l'association Framasoft.
- [searx](#) (Français) Moteur de recherche de "La quadrature du net.
- [Unbubble](#) (Europe)
- [ahmia](#) Un moteur de recherche pour les sites onion.

<https://www.ixquick.com/fra/privacy-policy.html>

Ainsi pour chercher une documentation sur google par ixquick passez par ces liens ils ne laissent aucun cookie et n'enregistre rien de vos surfs.

Mémo­ri­sez ces liens dans vos Favoris ou Marque-pages ou utilisez-le comme page d'accueil de votre navigateur

Ixquick

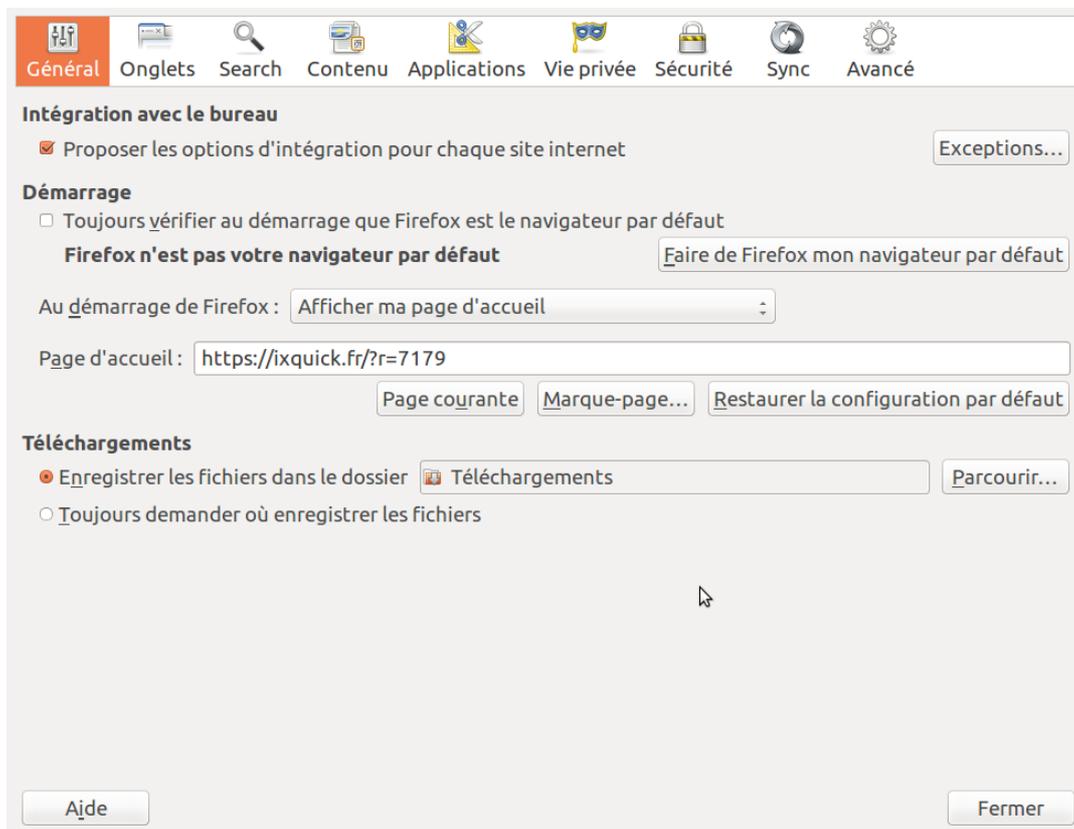
<https://ixquick.fr/?r=7179>

ou

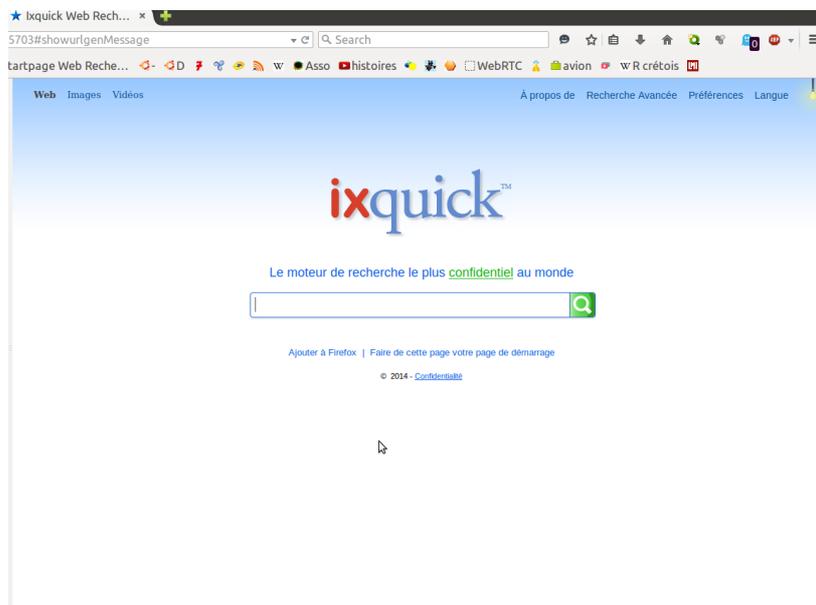
Startpages

<https://startpage.com/?r=6946>

Ouvrir Firefox → Outils → Options → Page d'accueil (sous Windows)
Ouvrir Firefox → Édition → Préférences → Page d'accueil (GNU/Linux)



Tapez votre mot clé de recherche

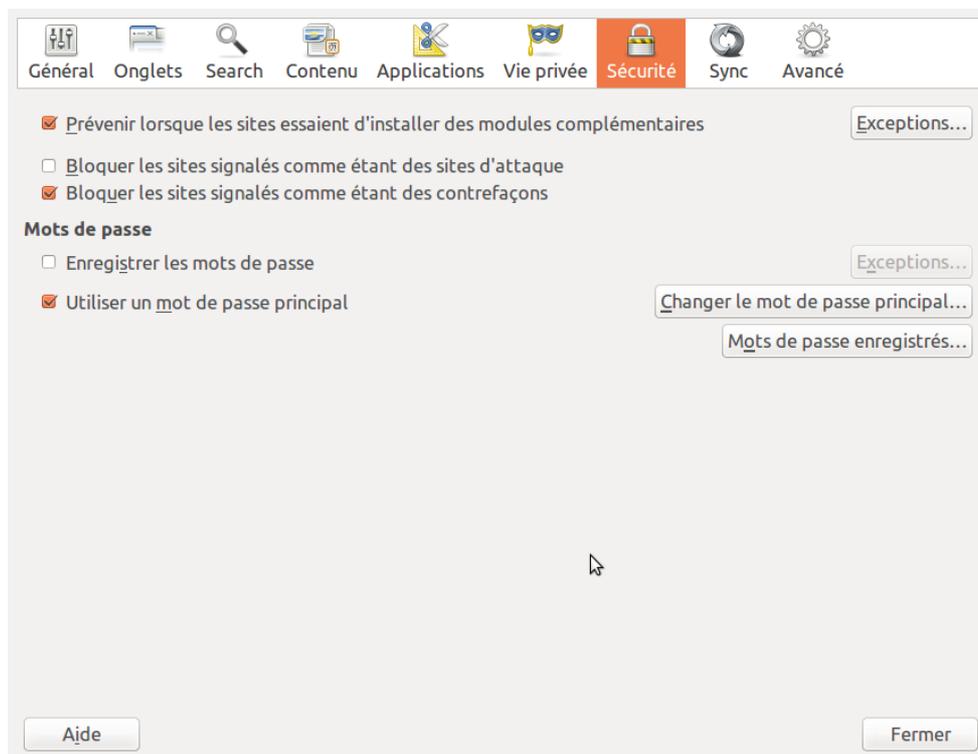


Valider par entrée
Cliquer sur le lien intéressant

Ne pas enregistrer vos mots de passe dans le navigateur

Ouvrir Firefox → Outils → Options → Sécurité (sous Windows)

Ouvrir Firefox → Édition → Préférences → Sécurité (GNU/Linux)



Créer un mot de passe principal qui sera un leurre pour les sites

Corriger l'indiscrétion dans le navigateur Firefox et dérivés

Les entrées de réglage de Firefox sont indiquées [ici](#)

Essayons de corriger tout cela. Il y a donc plusieurs choses à faire :

Écrivez dans la barre d'adresse de votre navigateur Firefox:
[about:config](#)

Évidemment Cliquer **je ferai attention, promis**

Masquer la dernière page visitée : modifiez la chaîne ***network.http.sendRefereHeader***, Cette chaîne permet au navigateur de mémoriser les pages visitées auparavant ; double clic sur cette ligne, en lui assignant la valeur **0**. ainsi ous n'avez visité aucun site

Profil publicitaire de l'internaute

Renvoi de la recherche à Google à des fins de définir votre profil publicitaire. Cette fonctionnalité est **activé par défaut**, vous pouvez la désactiver en mettant la variable en double cliquant sur la ligne : **browser.safebrowsing.malware.enabled à false**

On peut aussi enlever toutes les adresses google.com dans les autres variables **browser.safebrowsing.malware** Double clic sur la ligne, effacer, valider **OK**

Géolocalisation de votre Fournisseur d'Accès à Internet

Saisissez **geo.enabled** dans le champ « Filtre »

Faire un double-clic sur la préférence **geo.enabled** à **false**

Double clic **geo.wifi.uri**; effacer le contenu des coordonnées GPS, valider OK

La fonctionnalité de géolocalisation est maintenant désactivée

Souriez vous n'êtes plus filmé vous pourrez quand même faire votre recherche.

Télécharger Firefox :

<https://www.mozilla.org/fr/firefox/new/>

<http://www.toolinux.com/Mozilla-la-vie-privee-est-elle>

Bibliographie :

Guide de l'autodéfense numérique : <https://guide.boum.org/>

https://www.laquadrature.net/fr/Vie_privée

<https://sortirdefacebook.wordpress.com/>

<https://www.controle-tes-donnees.net/>

Ledatux <asso.ledatux@laposte.net>