Votre identité numérique

Le navigateur révèle votre identité numérique personnelle avec l'adresse ip de chaque machine

https://whoer.net/fr

https://www.cnil.fr/fr/votre-ordinateur et https://www.cnil.fr/fr/comment-ca-marche

Vérifiez vous-même ce que véhicule votre navigateur

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

Votre navigateur, **Internet Explorer, Edge, Firefox, Abrowser, IceCat, Iceweasel, Epiphany, Chromium, Konqueror, Chrome, Safari, Opera, Palemoon, Brave etc** 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, d'analyse, des mouchards, d'espionnage dans votre navigateur.

Cliquez, vous êtes traqués en permanence :

https://www.youtube.com/watch?v=5mmQeb8mXVk

https://www.journaldunet.com/media/publishers/1514605-sacha-morard-groupe-le-monde/

Concrètement, sécuriser son navigateur

Installez des modules complémentaires dans votre navigateur :

Firefox → Outils → modules complémentaires

Un module anti-publicité

uBlock Origin = antipub le + adapté

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 toutes les cases Publicités, confidentialité, réseaux sociaux, domaines malveillants, nuisances → Appliquer.

Enfin, un bloqueur efficace de publicité. Facile sur CPU et mémoire.

Les Cookies

Un cookie est un petit fichier envoyé par un site Internet que vous visitez. Ce fichier contient une poignée d'informations que ce site souhaite pouvoir réutiliser au cours de votre visite actuelle ou lors de vos prochaines visites.

Les cookies ont de multiples usages : ils peuvent servir à mémoriser votre identifiant client auprès d'un site marchand, le contenu courant de votre panier d'achat, la langue d'affichage de la page web, un identifiant permettant de tracer votre navigation à des

fins statistiques ou publicitaires, etc. Certains de ces usages sont strictement nécessaires aux fonctionnalités expressément demandées par l'utilisateur ou bien à l'établissement de la communication et donc exemptés de consentement. D'autres, qui ne correspondent pas à ces critères, nécessitent un consentement de l'utilisateur avant lecture ou écriture.

Un effaceur de cookie
Cookie AutoDelete =
Supprime automatiquement les cookies lorsqu'ils ne sont plus utilisés par les onglets ouverts du navigateur. Avec les cookies, les sessions persistantes, ainsi que les informations utilisées pour vous espionner, seront effacées.

Configurer → aller dans les **préférences**, cocher toutes les cases jusqu'à la dernière, régler à 3 secondes
https://addons.mozilla.org/firefox/addon/cookie-autodelete

Un anti-espion
Privacy-Badger = bloque les données collectées au travers de cookies tiers. Il protège votre vie privée en bloquant les publicités d'espionnage et les traqueurs invisibles. Empêche la prise d'empreintes digitales sur toile, (comme CanvasBlocker), les supercookies (comme Click&Clean), et les cookies uniques qui contiennent des ID de suivi.
https://privacybadger.org/fr/

HTTPS Everywhere

HTTPS Everywhere est une extension Firefox produite en collaboration entre The Tor Project et la Electronic Frontier Foundation. Il crypte vos communications avec un certain nombre de sites Web importants. Beaucoup de sites sur le web offrent un support limité pour le chiffrement sur HTTPS, mais le rendent difficile à utiliser. Par exemple, ils peuvent utiliser par défaut le protocole HTTP non chiffré ou remplir des pages chiffrées avec des liens renvoyant vers le site non chiffré. L'extension HTTPS Everywhere corrige ces problèmes en réécrivant toutes les requêtes de ces sites vers HTTPS.
https://www.eff.org/https-everywhere

Voici les domaines pris en charge:
https://www.eff.org/https-everywhere/atlas/

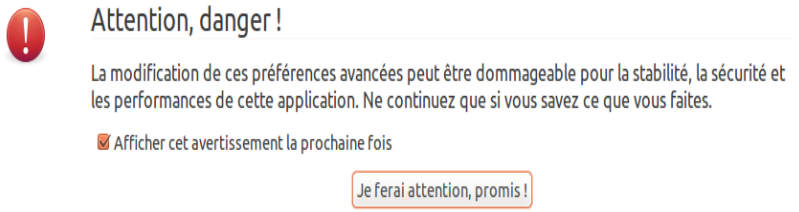
Et https://www.eff.org/https-everywhere/rulesets explique comment ajouter un jeu de règles à HTTPS Everywhere.

Corriger l'indiscrétion dans le navigateur Firefox et dérivés

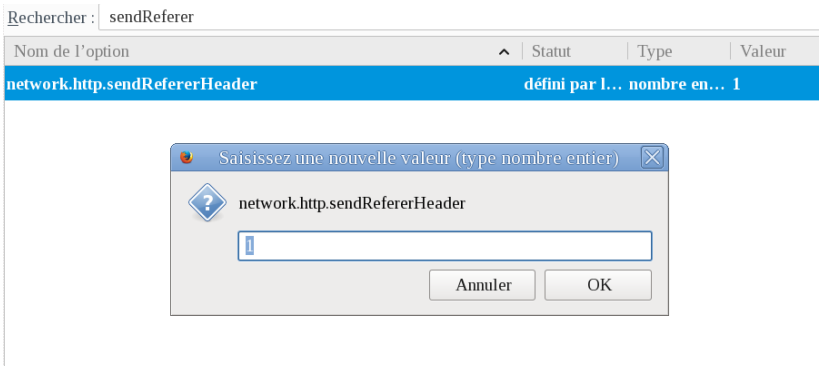
Essayons de corriger tout cela. Il y a donc plusieurs choses à faire :

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 ***1***.



La Télémétrie :
Si vous désactiver la télémétrie il y a bien des chances que vous ne pourrez ouvrire de nombreux sites.

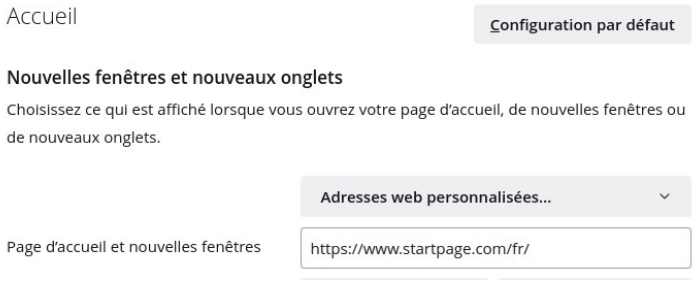
Vérification de l'efficacité des modules

Après installation et configuration des modules, il est possible de vérifier si l'on est unique ou pas sur Internet en visitant le site Web https://amiunique.org/ ou *Panopticlick*.

Quelques réglages des paramètres de votre navigateur internet
Ouvrir Firefox → Outils → Options → (sous Windows)
Ouvrir Firefox → Édition → Préférences → (GNU/Linux)

Onglet général → Langue choisir français

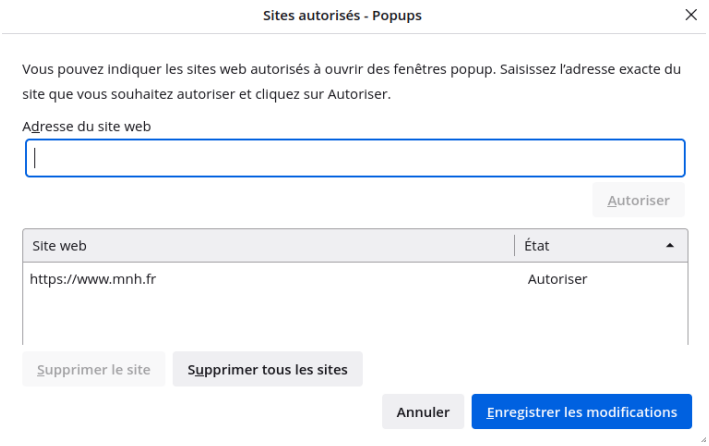
Onglet Accueil → choisir un moteur de recherches personnalisé respectueux de votre vie privée *https://www.startpage.com/fr/*



Décochez activités récentes et Brèves

Onglet Recherche par défaut → Startpage
Supprimer Google, Bing, Amazon,eBay trop indiscrets

Onglet vie privée et sécurité
Décocher proposer d'enregistrer mots de passe
Décocher compléter les champs de cartes bancaires automatiquement
Permission à lecture automatique → Paramètres → autoriser l'audio et la vidéo
Bloquer les pop up → Exceptions
Le site de la Mutuelle Hospitalière MNH ne pourra s'ouvrir que si vous écrivez son adresse dans la liste blanche



Onglet Synchronisation
Synchroniser Firefox sur vos autres appareils → ordinateurs et tablettes et smartphones

Le risque de lire son courrier électronique avec le navigateur internet
Le webmail est un client de messagerie qui s'exécute sur les serveurs du Fournisseur d'Accès Internet (Orange, SFR, Bouygues, Free...) ; il se réalise sur les serveurs américains d'adresses gratuites (Gmail,Yahoo,Windows Live, Hotmail) par l'intermédiaire d'un navigateur internet.

En cas de panne de connexion interne toute la correspondance est indisponible. **Consulter sa messagerie sur le navigateur augmente le risque de se faire pirater sa messagerie d'autant plus que la plupart des personnes oublie de se déconnecter.**

En laissant vos fenêtres et portes ouvertes de votre adresse avec une affiche vous pouvez entrer ne vous étonnez pas que des rôdeurs franchissent facilement le seuil.

Utilisez un logiciel de messagerie comme THUNDERBIRD ; les messages seront lus et écrits dans votre machine. Choisissez le protocole IMAP.

Le risque de perte de confidentialité de vos messages qui passent par des serveurs étrangers.

Le texte de Google sur gmail est explicite

« *Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection. This analysis occurs as the content is sent, received, and when it is stored.* »

« *Nous analysons (scanner) vos emails entrants et sortants et ceux qui sont déjà enregistrés pour vous offrir un meilleur service publicitaire, détection de spam et de virus.* »

Google, c'est comme la cigarette : c'est votre choix mais il impacte les autres
https://www.ladn.eu/tech-a-suivre/donnees-personnelles-pourquoi-arreter-services-gafa/

Les conditions d'utilisation de **Microsoft** sont éclairantes :

«Si vous utilisez une adresse e-mail fournie par une organisation à laquelle vous êtes affilié, comme un employeur ou un établissement d'enseignement, pour vous connecter aux services en ligne de Microsoft, le propriétaire du domaine associé (par ex. votre employeur) peut : (1) contrôler et administrer votre compte de services en ligne de

Microsoft et (2) accéder à vos données, notamment au contenu de vos communications et fichiers, et les traiter.»

«Nous utilisons également les données pour vous proposer des publicités plus pertinentes, que ce soit dans nos produits sujets à publicité (comme MSN ou Bing) ou dans des produits tiers.»

Yahoo a révélé avoir été piraté plusieurs fois. Des informations concernant la totalité des comptes se sont retrouvées dans la nature. Disons-le tout net : en matière de sécurité informatique, Yahoo a une responsabilité importante. C'est navrant de confier sa messagerie à ce type de champions informatiques peu sécurisés.
http://www.futura-sciences.com/tech/actualites/securite-yahoo-reconnait-3-milliards-comptes-ont-ete-pirates-2013-64447/

Firefox ou un de ses dérivés est le navigateur par défaut de tous les Systèmes informatiques GNU/Linux

Bibliographie :

Recommandations de l'ANSSI (Agence nationale de la sécurité des systèmes d'information)

https://www.ssi.gouv.fr/uploads/2013/05/anssi-guide-recommandations_mise_en_oeuvre_site_web_maitriser_standards_securite_cote_navigateur-v2.0.pdf

https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-un-systeme-gnulinux/

Mots de passe : https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_MDP_NoteTech.pdf

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

https://framablog.org/2016/10/05/tristan-nitot-livre-surveillance/

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

https://framatube.org/media/controle-tes-donnees-quest-ce-que-le-profilage

https://sortirdefacebook.wordpress.com/

https://controle-tes-donnees.net/

Les 10 règles pour rester net sur le web

Ledatux - Club informatique de Lédat 47300
05 53 40 83 83
Mardi et Samedi de 9 h à 12 h, Jeudi de 20 à 22 h – sauf jours fériés de septembre à juin
ledatux@netcourrier.com
http://www.net1901.org/association/LEDATUX,871303.html