Choisir et configurer son navigateur internet

Pour naviguer sur internet, pour faire un lien entre votre ordinateur local et les pages d'un site Web, vous utilisez un navigateur. Il existe de nombreux navigateurs et tous n'ont pas les mêmes qualités ... ni les mêmes défauts !
Rappel: qu'est-ce-qu'un réseau local ? qu'est que le www ? comment relie-t-on son réseau local au www ? qu'est qu'un fournisseur d'accès ? qu'est qu'une connexion chiffrée, comment la reconnaît-on ?

Pour imager le navigateur dans le monde réel, on pourrait dire qu'il est la porte de l'habitation, il permet la communication entre l'espace intérieur (l'habitation, une pièce dans l'habitation/ la box, un espace de stockage dans l'ordinateur) et l'espace extérieur (la ville, la rue/ le www).
Ainsi pour circuler sur les pages publiées sur le www, on utilise généralement un navigateur. Pour assurer la sécurité de son espace intérieur (un ordinateur), il faut choisir une porte adaptée et dotée de serrure pour filtrer qui peut entrer et qui ne peut pas.

Éléments de choix :
Quels sont le principaux navigateurs disponibles ?
Il en existe de nombreux. Trois d'entre eux représentent plus de 90% des usages.
L'un appartient au monde Microsoft (Internet Explorer puis Edge), les deux autres au monde Netscape (noyau chrome développé par Netscape puis libéré par Netscape et repris par Mozilla; plusieurs navigateurs dérivés dont Chrome de Google).

Edge (ex IE)	Firefox	Google Chrome
		
- vendu par Microsoft	- proposé par Mozilla.org	- proposé par Google.inc
licence	licence	licence
- nombreuses failles de sécurité pas ou tardivement corrigées	- peu de failles de sécurité ou failles très vite corrigées	- peu de failles de sécurité mais sécurité compromise par l'éditeur.
- présence de portes dérobées vers ...	- pas de porte dérobée révélée	- présence de portes dérobées vers ...
- pas ou peu d'outils/options de personnalisation	- nombreuses options de personnalisation	- options de personnalisation proposées par Google
NS	- nombreux modules complémentaires	- nombreux modules complémentaires validés par Google

Lequel choisir ?

1. On élimine les navigateurs qui comportent des failles nombreuses et/ou rarement ou

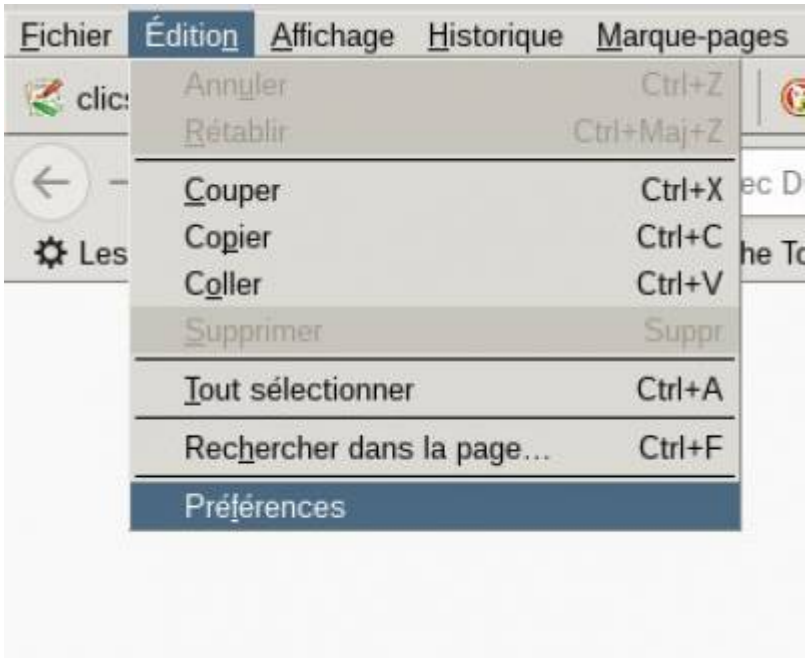
tardivement corrigées (on élimine Edge)
2. On élimine les navigateurs proposés par des éditeurs qui font commerce des données des utilisateurs (on élimine Chrome)
3. On choisit un navigateur qui propose de nombreuses options de personnalisation et un grand éventail de modules (on choisit Mozilla Firefox)
4. On choisit un navigateur dont le code informatique source est totalement libre et ouvert (pour les logiciels propriétaires, personne, hors le concepteur, ne peut savoir ce que le logiciel fait vraiment de vos données) (on choisit Mozilla Firefox)

Le navigateur qui répond le mieux aux enjeux de sécurité des données personnelles est Mozilla Firefox.

Paramétrer Mozilla Firefox :

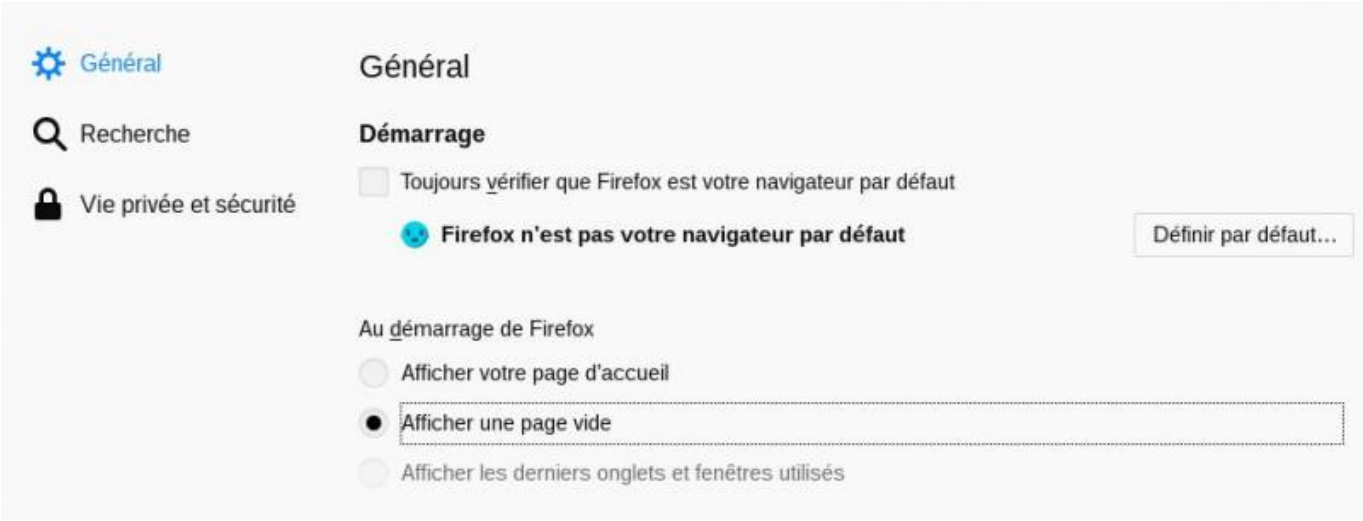
Configuration de base

vous pouvez télécharger la dernière version de Mozilla Firefox à l'adresse : https://www.mozilla.org/fr/firefox/new/ Une fois téléchargé, installé et lancé, vous pourrez paramétrez avec soin les options de ***Vie privée*** et de ***Sécurité*** (au menu **Outils / Options**/ ou **Édition / Préférences**/)



Général

Le paramétrage des Préférences est classé en plusieurs chapitres. Commençons par le chapitre **Général** pour nous arrêter sur le paramètre **Au démarrage de Firefox** Ce paramètre vous permet d'ajuster ce qui est affiché par Firefox au moment de son démarrage. L'affichage d'une page vide est conseillé.



(on est en droit de penser que c'est vous, personnellement, qui décidez d'aller sur un site, pas votre navigateur !)

Recherche

Firefox vous propose de choisir le moteur de recherche qu'il utilisera, par défaut, lorsque vous lancerez une recherche.
Nous vous conseillons de choisir un moteur de recherche qui ne stocke pas vos recherches, qui ne les utilisent pas pour dresser de vous un profil avec des algorithmes, qui ne les utilisent pas pour filtrer les résultats ou pour vous envoyer les publicités, à l'écran, dans votre boîte mail ou ….
Nous vous proposons de préférer Qwant lite ou DuckDuckGo ou Disconnect qui tous les trois, s'engagent à ne stocker aucune de vos recherches.
Searx et Framabee sont également des choix pertinents.

Vie privée et sécurité

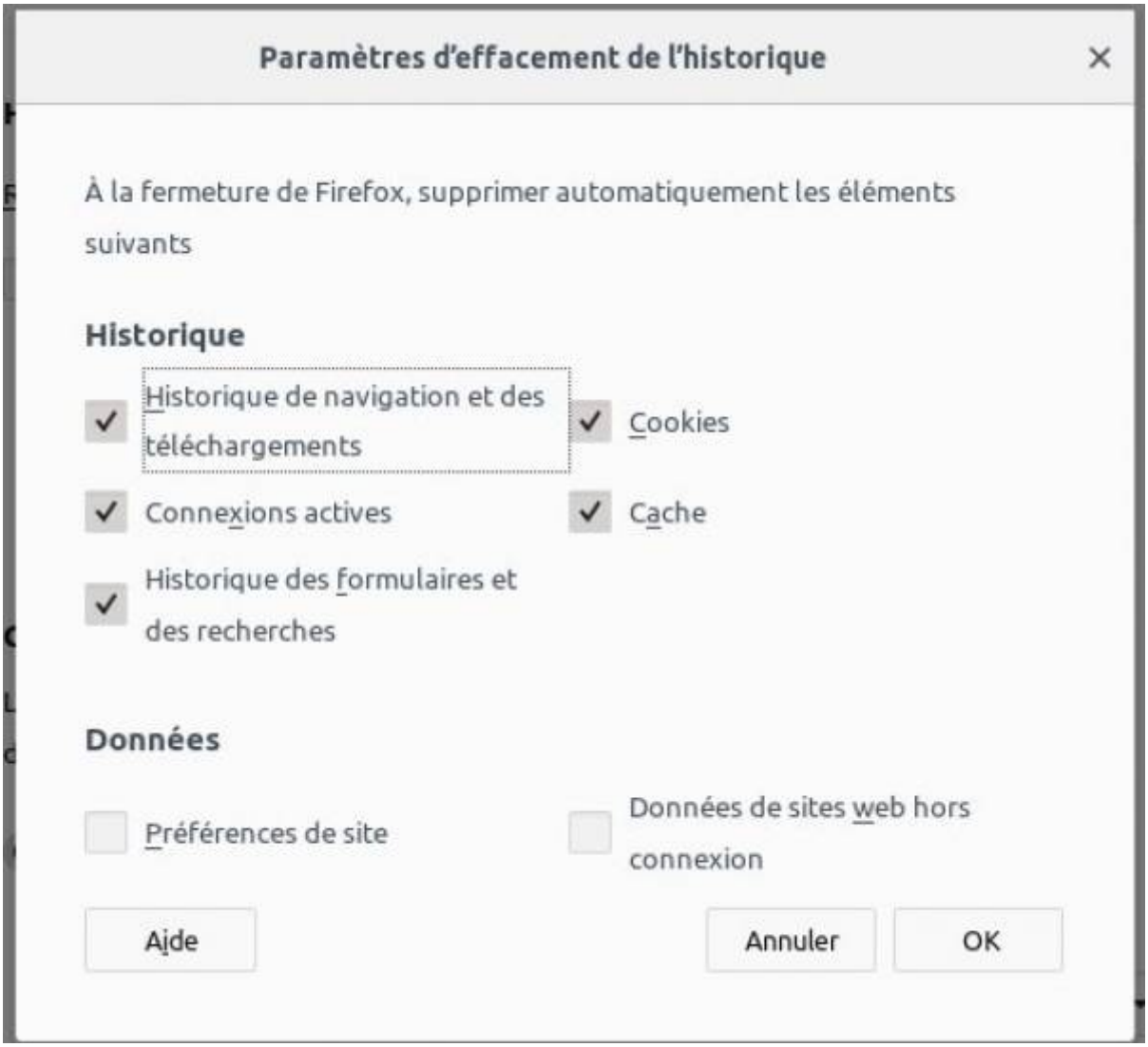
Ce chapitre réclame toute votre attention.

Formulaires et mots de passe

- Proposer d'enregistrer les identifiants et les mots de passe pour les sites Web
  celle option permet de demander au navigateur de retenir à votre place vos mots de passe pour les sites que vous fréquentez. Cela peut être une solution intéressante si elle vous permet de varier les mots de passe (pour rappel, il est dangereux d'utiliser le même mot de passe pour des sites différents. Il est impératif d'avoir un mot de passe spécifique pour chacun des sites où vous vous créez un compte).
  Si vous activez cette option, n'oubliez pas d'**Utiliser un mot de passe principal** pour votre coffre-fort de mots de clés.
- Utiliser un mot de passe principal: ce mot de passe doit être un mot de passe fort: il dit comporter des lettres minuscules,des lettres majuscules, des chiffres et, idéalement des caractères spéciaux.
  Exemples: 19_Jul45Lil_Med ou -19+Jul45Rbx+Imp \\Attention, ne jamais utiliser des mots qui pourraient être présent dans un dictionnaire, annuaire, etc

Historique

- Règles de conservation: voulez-vous ou non, que Firefox conserve l'historique des pages que vous avez visité, des formulaires que vous avez complétés sur le Web.
  Attention: si vous pouvez accéder à votre historique, des logiciels que vous avez installés sur votre ordinateur pourront y accéder également. Les personnes qui peuvent accéder physiquement ou à distance à votre ordinateur le pourront également. Idéalement, il faudra supprimer votre historique quand vous fermez votre navigateur.
- Utiliser les paramètres personnalisés



Cookies et données de sites

Les cookies sont des petits fichier texte placés sur le disque dur de votre ordinateur par le navigateur à la demande des sites que vous visitez. Des informations sur votre navigation peuvent ainsi être stockées et lues par des tiers. A l'origine, es cookies ont été inventés pour permettre aux sites d'authentifier les internautes et d'enregistrer leurs préférences de navigation; entre-temps, leur utilisation a été largement détournée à des fins commerciales. Si la connexion Internet entre le navigateur et le site n'est pas chiffrées, les informations que contiennent les cookies circulent en clair et peu être l'objet d'interception. Si accepter les cookies pendant la durée de la navigation sur un site peut être utile, il vaut mieux demander à Firefox de refuser les cookies tiers et supprimer tous les cookies à la fermeture du navigateur.

Barre d'adresse

Ces options permettent de configurer la barre d'adresse.

Protection contre le pistage

Sécurité

Protection contre les contenus trompeurs

Cetificats

Modules complémentaires pour améliorer la protection de la vie privée

FIREFOX > Outils > Modules Complémentaires > Extensions > Recherche
Que sont les modules complémentaires ?
Des modules complémentaires apportent au nevigateur des fonctionalités supplémentaires ou rendent le navigateur plus efficace dans le respect de votre vie privée. Il est utile et nécessaire de vérifier qui a conçu le module et si le code du module est libre. Pour améliorer la sécurité de vos visites sur internet, l'installation des modules complémentaires ci-dessous est fortement conseillée:

1. Publicités:
   Ublock Origin: extension pour Firefox qui filtre le contenu des pages web afin d'en supprimer les bannières de publicité: navigation plus lisible, rapide, propre.
2. Connexion sécurisée: https://www.eff.org/https-everywhere
   Https Everywhere: sélectionne la navigation sécurisée https sur tous les sites où cela est possible.
3. Filtrage des mouchards du Web: https://www.eff.org/privacybadger
   Privacy Badger: extension pour Firefox qui filtre le contenu des pages web afin d'en supprimer les mouchards du Web (statistiques, etc).
4. Anonymiser les recherches Google: https://disconnect.me/search
   Disconnect Search: redirige vos recherches pour les rendre anonymes pour le moteur de recherche.
5. Protection supplémentaire pour votre Firefox!
   Noscript: https://noscript.net/ (pour les utilisateurs avancés)
   Protection supplémentaire pour votre Firefox : NoScript ne permet l'exécution de scripts JavaScript que sur les domaines de confiance de votre choix (p.ex. le site de votre banque).
   Ce système de blocage préventif de scripts basé sur une liste blanche empêche l'exploitation de failles de sécurité (connues et même inconnues) sans perte de fonctionnalités...

Certains de ces modules peuvent aussi être installés dans les autres navigateurs cités.

Configuration avancée

- Protéger son identité sur le web [édité le 30 septembre 2018]
- The Complete Firefox Privacy and Security Guide

Tor: Cacher les participants des communications : le routage en oignon

“Le routage en oignon, utilisé par exemple par Tor, peut fournir un certain anonymat sur Internet en

masquant d'où provient une communication. En utilisant un tel système, l'adresse IP qui apparaît sur Internet, et qui sera par exemple enregistrée dans les journaux de connexion des serveurs utilisés, n'est pas la nôtre mais celle d'un autre ordinateur.”
Il existe une version spécialisée de Mozilla Firefox pour mettre en œuvre le routage en oignon: le **Tor Browser** (navigateur Tor)
Vous pouvez télécharger Tor et l'installer.
* Cacher les parties prenantes d'une conversation avec Tor Browser où vous retrouverez en ligne une présentation de Tor, détaillée et accessible à tous.

Aller plus loin

- Tout sur les cookies Http Cookies explained
- Guide d'autodéfense numérique

.body { font-family: sans-serif; background-color: #1b1b1b; }

— *André Vanderlynden 2018/11/05 23:00*