Démo navigateur web en 5 étapes + bonus

Rencontres Abraham Mazel 2017
"Résister à la peur"

Présentation tirée du "guide de survie, épisode 1"

- Un ordinateur infecté par un virus peut transmettre ce virus à ses contacts,
- une boîte mail piratée transforme ses contacts en cibles pour le pirate,
- un ordinateur envahi de pubs empêche de travailler sur desprojets partagés,
- faire des recherches exclusivement sur Google cache une partie des informations peut-être nécessaires pour une réflexion complète,
- etc.

Étant en constant contact les uns avec les autres,
ce qui touche notre ordinateur peut toucher nos contacts,
parfois sans même qu'on s'en aperçoive.

En ligne sur aloeil.info, mise à jour prévue au cours de l'été

Modules complémentaires et extensions (1)

Contrôler les mouchards

Ghostery : Bloque les mouchards (logiciels espions, statistiques etc.), les cookies des sites publicitaires et les pubs. Très facile à utiliser, avec un tuto à l'installation.
https://www.ghostery.com/try-us/download-navigateur-extension/
Avec le succès Ghostery devient plus "clientophile", ce qui signifie qu'il négocie avec certaines entreprises et laisse passer quelques mouchards, pubs et cookies.

Privacy Badger : Bloque les mouchards, les cookies et pubs. Moins facile à utiliser : il faut choisir ce qu'on bloque ou autorise, mais on peut annuler chaque action. Très fiable, développé par l'Electronic Frontier Foundation
https://www.eff.org/fr/privacybadger
Avec le succès Ghostery devient plus "clientophile", ce qui signifie qu'il négocie avec certaines entreprises et laisse passer quelques mouchards, pubs et cookies.

Umatrix : Bloque les mouchards, les cookies et pubs. Très précis, compliqué à utiliser, mais très fiable quand on sait s'en servir, selon des connaisseurs.
https://addons.mozilla.org/fr/firefox/addon/umatrix/ pour Firefox
https://chrome.google.com/webstore/detail/umatrix/ogfcmafjalglgifnmanfmnieipoejdcf?hl=fr
Pour Chrome (cliquer sur le lien, il ne s'affiche pas entier

Modules complémentaires et extensions (2)

Sécuriser les connexions

Https-everywhere / **Https-partout** : permet de naviguer sur internet via le protocole "sécurisé" (le S de https) pour que la connexion ne soit pas visible par un intrus sur le réseau.
https://www.eff.org/https-everywhere

Bloquer les publicités

uBlock Origin : Bloque les pubs et peut être désactivé à tout moment. Plus efficace que AdBlock Plus.
https://addons.mozilla.org/fr/firefox/addon/ublock-origin/

Voir les vidéos en évitant flash

HTML5 Video Everywhere! : Flash est plein de failles de sécurité, html5 permet de lire les vidéos directement avec le navigateur. Cette extension force la lecture des vidéos en html5. C'est aussi rapide qu'en flash et les vidéos sont plus facilement téléchargeables.
https://addons.mozilla.org/en-US/firefox/addon/html5-video-everywhere/

Et un bonus qui ne bloque rien mais utile

Lightbeam : permet de voir les sites (appelés "tierces parties") qui suivent notre navigation.
https://www.mozilla.org/fr/lightbeam/

Réglages navigateur (1)

Les réglages se font dans le **menu "hamburger"** (3 traits superposés) en général en haut à droite de la page web, puis soit le **menu "préférences"** (une roue dentée) dans Firefox puis **les différents menus**, ou les menus séparés directement dans Chrome / Chromium et Opéra.

Menu Vie privée

Cocher "Ne pas me pister" : indique aux sites visités de ne pas nous suivre dans notre navigation. S'adresse à des robots, donc ils le respectent plutôt bien, mais peu sont dans la liste des destinataires.
Cocher "vider l'historique en quittant" : permet de ne pas laisser de traces sur notre ordinateur, se protège contre une intrusion qui pourrait retourner sur des sites d'achat et retrouver notre compte et nos moyens de paiement.
Cocher "accepter les cookies" et "jusqu'à la fermeture du navigateur" : certains cookies sont indispensables pour la navigation, les achats, etc, il faut donc les accepter. Mais après la fermeture du navigateur ils n'ont pas à rester sur l'oridnateur, il faut les effacer.

Menu Sécurité

Cocher toutes les cases dans "général" : nous prévient quand un site est signalé comme dangereux ou quand un site essaye d'installer une extension ou un module.
Décocher les 2 cases "Retenir identifiants pour les sites" et "Utiliser un mot de passe général"
Effacer les mots de passe présents dans "mots de passe sauvegardés".

Réglages navigateur (2)

Menu "avancé", onglet "Mises à jour"

Cocher "Rechercher des mises à jour automatiquement" : permet de garder son navigateur toujours à jour, et d'éviter le plus possible les piratages. **Les mises à jour sont souvent des corrections de failles de sécurité.**

Menu Recherches

Le moteur de recherche sait tout de nous. Il est plus prudent de choisir des moteurs de recherche plus respectueux de notre vie privée que Google-search.

Pour supprimer des moteurs de recherche de la liste :
Décocher leur nom et/ou le sélectionner et cliquer sur "supprimer" en bas du tableau.

Pour ajouter des moteurs de recherche :
Afficher la page du moteur voulu, chercher le lien "ajouter à Firefox/Chrome...", cliquer dessus. La page du menu "recherches" s'ouvre, cochez le nom du nouveau moteur. Ensuite allez dans la barre de recherche (la petite barre de droite en haut des pages web), cliquez dedans et vérifiez que le nouveau moteur est bien présent dans les choix.

Ce qu'on ne sait pas toujours

Widgets sociaux

Les petites icones "facebook", "twitter", etc. : Même si on n'a pas de compte, afficher une page web qui contient un de ces widgets nous fait suivre par le propriétaire de ce widget. Les bloquer permet de ne pas être suivi par eux.

Quand on clique sur un bouton de réseau social "Partager" une info d'un site, on donne aussi l'accès de vos infos du réseau social au site (**l'aller donne aussi le retour**).

Partage, cloud et "j'accepte"

Stocker ses données, son travail, ses photos de vacances sur facebook ou sur un cloud, c'est **les stocker "sur l'ordinateur d'un autre"**, et c'est aussi, chez certains, **leur donner** ses photos, son travail, etc, **selon leurs Conditions Générales d'Utilisation** (CGU).
Voir le film documentaire : Les nouveaux loups du web, plusieurs prix (même gratuit) sur jupiter-films
http://www.jupiter-films.com/film-les-nouveaux-loups-du-web-47.php#dvd
ou en pear-to-pear.

Bonus sur Windows

Rencontres Abraham Mazel 2017
"Résister à la peur"

Eviter les pubs à l'installation de logiciels

Spécial Windows (1)

Télécharger un logiciel pour l'installer c'est prendre le risque de télécharger un logiciel "vérolé".
Pour l'éviter, il faut toujours **télécharger les logiciels sur le site du développeur.**
Il existe quelques autres sites de confiance, dont :
http://www.commentcamarche.net/download/
(Utiliser un bloqueur de pubs, il en diffuse beaucoup sur ses pages)

Eviter :
Clubic, Softonic, 01net.com (et d'autres), qui sont de bons sites techniques mais ont besoin des pubs pour vivre, donc en distribuent gratuitement et en affichent sur leur site et dans leurs articles. Par exemple, ne pas forcément leur faire confiance dans leurs tests comparatifs, ils sont peut-être orientés par leurs contrats publicitaires.

Installer un logiciel sur Windows risque d'installer aussi des pubs incluses avec le logiciel dans le paquet téléchargé.
Il faut refuser (bouton "non merci" ou "plus tard") tous les logiciels autres que celui que vous avez décidé de télécharger et d'installer : tous les autres sont des pubs qui vont "envahir" votre ordinateur. Il peut y avoir plusieurs invitations à refuser avant que le logiciel ne s'installe, ne pas perdre patience !

Retirer les pubs des logiciels

Spécial Windows (2)

Pour retirer les adwares (pubs), 2 logiciels libres et gratuits sont très bons et complémentaires :

Adwcleaner édité par Xplode, téléchargeable sur Toolslib :
https://toolslib.net/downloads/viewdownload/1-adwcleaner/
et sur commentcamarche :
http://www.commentcamarche.net/download/telecharger-34096208-adwcleaner
Il s'utilise sans installation, en double-cliquant directement sur l'icone du logiciel téléchargé.
Quand, après le scan, on demande à Adwcleaner de nettoyer l'ordinateur, il nous engueule et nous dit qu'il faut sortir couvert ; son logo est un morpion :p

Malewarebytes sur commentcamarche :
http://www.commentcamarche.net/download/telecharger-34055379-malwarebytes-anti-malware

Ces 2 logiciels ne traitent pas les mêmes adwares, selon l'adware qui nous embête, on peut être amené à passer les 2.