Animation 3 - Annexe 1
Quelques astuces pour limiter nos traces sur Internet

Ces conseils sont principalement valables pour le navigateur **Firefox**. Néanmoins, la plupart de ses modules ont aussi été créés pour être utilisables sur les autres navigateurs.

1) Navigateur et paramétrage

Utiliser «**Firefox**» comme navigateur (alternative à Google Chrome ou Internet Explorer par exemple).

Il suffit de le télécharger, de l'installer et de le définir comme navigateur par défaut en suivant les instructions à l'écran.

Paramétrer la navigation privée par défaut ou, au moins, effacer régulièrement – au minimum à la fermeture – les «cookies», voire l'historique (voir point 4).

Pour ce faire, aller dans « options », puis cliquer sur l'onglet « Vie privée et sécurité », aller dans la rubrique « Historique » et dans les règles de conservation, sélectionner « Utiliser les paramètres personnalisés pour l'historique ». Cocher pour terminer la case « Toujours utiliser le mode de navigation privée ».

2) Moteur de recherche

Startpage : Méta-moteur de recherche utilisant plusieurs moteurs de recherche. Un des objectifs est le respect de la vie privée de ses utilisateurs. Ils ne nous tracent pas et ne revendent pas notre historique de recherche.

Pour installer Startpage, surfer sur www.startpage.com. Parcourir la page et cliquer sur l'onglet « Faites de Startpage.com votre moteur de recherche par défaut ». Il suffit ensuite de suivre les instructions à l'écran.

Qwant, DuckDuckGo, Ecosia peuvent également convenir.

3) Ajouter les extensions élémentaires pour limiter les traces

Il est très simple d'installer ces extensions. Il suffit d'accéder au menu de Firefox (en cliquant sur les trois barres horizontales en haut à droite), de cliquer sur « modules complémentaires », puis de cliquer sur « Extensions ». Il reste alors à écrire le nom de l'extension dans la barre de recherche et de « l'ajouter à Firefox ».

HTTPS everywhere : module qui force, dès que possible, la navigation à passer sur la version cryptée du site (HTTPS://) s'il y en a une disponible.

UBlockOrigin : module qui remplace depuis quelque temps AdBlock. Ublock est donc un bloqueur de publicité très performant et personnalisable.

Privacy Badger : module d'extension libre dont l'objectif est de bloquer les régies publicitaires et les autres sites tiers qui cherchent à connaître les pages visitées par l'internaute. Il bloque également les cookies traqueurs qui ne respectent pas le réglage du navigateur web 'ne pas me pister'.

Disconnect : module qui permet de visualiser et de bloquer les trackers qui suivent vos recherches et votre historique de navigation.

4) Installer Ccleaner ou Glary Utilities

 **Ccleaner** : Logiciel à installer dont la version gratuite permet de supprimer les fichiers de suivi et les données de navigation renforçant la protection de notre vie privée. Pour supprimer ces fichiers (cookies…), il est nécessaire de le faire manuellement à travers l'interface de Ccleaner en cliquant sur « Nettoyer ».

 **Glary utilities :** Disponible gratuitement (pour une utilisation personnelle), Glary Utilities est un véritable couteau suisse pour votre ordinateur ! Cet utilitaire permet en effet de nettoyer, de réparer, d'optimiser votre ordinateur, d'assurer la confidentialité et la sécurité de vos données, etc.

Nettoyer votre ordinateur régulièrement grâce à ces programmes (au moins une fois par mois).

5) Changer de système d'exploitation

 **Linus Ubuntu** est une alternative à Windows ou Mac OS mais qui implique un changement complet de l'utilisation de son ordinateur. C'est néanmoins un rempart efficace aux GAFAM, gratuit et facile d'utilisation.

6) Mots de passe

Ne pas encoder ses mots de passe partout. Ne pas les enregistrer sur les sites que vous visitez. Les varier, les changer régulièrement. Il faut qu'ils soient longs, avec des caractères variés (minuscules, majuscules, chiffres, signes,…). Pour les retenir éventuellement les noter dans un carnet à part. Trouver une clef de lecture. Exemple : prendre les premières lettres de chaque mot d'une phrase.

 Une autre solution efficace est d'utiliser un coffre-fort à mots de passe. **Kee Pass X** est un gestionnaire de mot de passe à télécharger qui permet de sauvegarder vos mots de passe dans une base de données chiffrée.

Pour savoir si un mot de passe a été hacké : https://haveibeenpwned.com/

7) Mon adresse mail

 Il existe des adresses gratuites et sécurisées pour se débarrasser de yahoo, hotmail, gmail... Par exemple : Protonmail, dont les serveurs sont basés en Suisse, garantit à ses utilisateurs un chiffrement de bout en bout de leurs mails. Eux-mêmes sont incapables de déchiffrer et de lire les mails. De plus, il est simple, gratuit, ne nécessite pas d'installation et ne récupère pas de logs sur vous (comme l'adresse IP par exemple).

Toutefois si votre interlocuteur utilise une adresse de messagerie qui capte les données personnelles (hotmail, gmail, yahoo…), le mail ne sera évidemment pas chiffré.

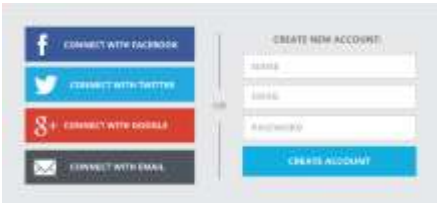
Les versions gratuites sont parfois limitées mais tout dépend de l'usage que l'on a de nos boîtes mail ; la capacité de stockage peut par exemple être limitée.

 **Mailfence** poursuit les mêmes objectifs et ses serveurs sont installés en Belgique.

Il est par ailleurs judicieux de disposer d'au moins deux adresses mail : une que vous utilisez à des fins de loisirs (concours, inscription à des forums de discussion, à des sites de rencontre…) et une autre à des fins plus personnelles (factures, achats en ligne…).

Supprimer régulièrement vos mails (ainsi que le dossier éléments supprimés) afin de limiter vos traces.

8) Se connecter via son identifiant Facebook ou Google



Évitez de vous connecter à des applications ou sites internet avec vos identifiants Facebook ou Google. Il est préférable que vous encodiez à chaque connexion vos identifiants et mot de passe créés exclusivement pour le site ou l'application. En s'inscrivant avec Facebook ou Google, c'est signer un accord de partage de ses données personnelles et donner l'accès à son nom, prénom, date de naissance, ses amis et parfois même ses photos. Une application peut également écrire en votre nom sur votre mur Facebook (résultat d'un jeu pour en faire sa promotion).

9) Trouver des services et logiciels alternatifs et libres

Consulter la page https://framalibre.org/ et https://degooglisons-internet.org/fr/list/ pour découvrir toute une série de services alternatifs et libres (framapad, framadate…)

Quelques exemples :
Framadate, alternative libre à Doodle, ne stocke pas les données personnelles, permet de planifier une rencontre à plusieurs et même de créer des sondages.

Framapad est un service de rédaction collective en ligne, alternative à Google doc ou Office 365.

Framatalk permet un échange vocal, vidéo et écrit, sans installation requise. Les conversations sont totalement privées sans analyse des données.

10) Conseils pour smartphone

- **Désactiver les applis en arrière-plan sur votre smartphone**

Celles-ci continuent à collecter des données alors que vous n'êtes pas en train de les utiliser.

- **Supprimez les applications que vous n'utilisez plus**

Ce n'est pas parce que vous supprimez les raccourcis de vos applis qui se trouvent sur votre écran d'accueil que votre compte l'est également. A partir de l'appli, demandez la suppression de votre compte et le cas échéant, à la firme de supprimer vos données personnelles.

- **Données de localisation**

Désactivez ces données à partir des paramètres de votre téléphone. Désactivez le bouton de géolocalisation, le wifi, le Bluetooth, les données mobiles quand vous n'en n'avez pas besoin.

Installer **Firefox** est également possible sur smartphone. Ajoutez **UblockOrigin** pour vous débarrasser des publicités.

Installer en outre **Startpage** comme moteur de recherche par défaut.
Pour ce faire, naviguez sur le site du moteur de recherche que vous souhaitez utiliser, ici Startpage. Maintenez votre doigt sur la barre de recherche jusqu'à ce qu'un icône « ajouter comme moteur de recherche » apparaisse. Cliquer sur l'icône et rendez-vous ensuite dans les paramètres pour définir Startpage par défaut.

F-droid est une alternative au Play Store et offre un catalogue de logiciels libres. A la différence du Play Store qui exige un compte Google, F-Droid autorise l'installation d'applications sans nécessiter de compte.

 **Silence** est une application de messagerie libre qui outre l'envoi et la réception de SMS, MMS offre d'autres avantages :

- Lorsque votre correspondant utilise également Silence, l'échange des messages sera chiffré de l'envoi à la réception. Il est alors nécessaire de se communiquer mutuellement une clé. L'application fonctionne normalement (message non chiffré) si le correspondant n'utilise pas l'application.
- Les messages reçus et envoyés peuvent également être protégés localement par un mot de passe, ce qui permet de les chiffrer en cas de perte ou de vol.

 **Signal** est une application de chat et alternative à WhatsApp, rachetée par Facebook. Au contraire de WhatsApp qui conserve les données personnelles et les utilisent à des fins de marketing, Signal ne stockent aucune information et n'a pas accès aux communications. Signal permet de dialoguer en toute confidentialité grâce au chiffrement des conversations échangées. Les messages sont donc cryptés et seuls l'émetteur et le récepteur peuvent lire les lire.
Pour utiliser l'application, votre numéro de téléphone doit être vérifié mais ne sera pas conserver.

 **Riot** est également une alternative à WhatsApp mais le cryptage doit être activé manuellement. Avec Riot, l'utilisateur ne doit pas communiquer son numéro de téléphone mais reçoit un identifiant unique.

 **Discord** est une très bonne alternative à Skype (acquis par Microsoft en 2011), le logiciel permet un chat vocal, textuel et vidéo mais a été initialement pensé pour les « gamers". Fonctionne sur PC et smartphone.

Au niveau du cryptage, la politique de confidentialité de Discord indique clairement qu'ils ne vendent pas nos données personnelles.

LineageOS permet de remplacer le système Android fournit par Google et installé par défaut sur la plupart des smartphones. Semblable à Linus Ubuntu (alternative au système d'exploitation Windows sur ordinateur), LineageOS est à manipuler avec prudence car l'installation reste très délicate et compliquée. Il est possible de bloquer son téléphone en cas de mauvaise manipulation et de perdre sa garantie.

LineageOS incarne cependant un rempart efficace contre Google et offrira plus de contrôle sur son téléphone.

11) Pour aller plus loin…

Les cafés cryptés de Barricade, 21 rue Pierreuse, 4000 Liège. Un samedi par mois, de 13h30 à 17h30, http://www.barricade.be/agenda/cafe-crypte

Pour passer aux logiciels libres : Lilit (Liege linux team), Service de proximité de Grivegnée, 5 avenue Albert Ier, 4030 Liège. 1er jeudi du mois de 19h30 à 22h30. http://www.lilit.be/

Un guide d'autodéfense numérique : https://guide.boum.org

L'étude élaborée par l'équipe du professeur Douglas C. Schmidt, spécialiste des systèmes logiciels, **« Ce que collecte Google** »