## Donnés personnelles / confidentialité

1. Régler paramètres de vie privée (réseaux sociaux, navigateur, cookies intersites: <http://www.youronlinechoices.com> --> respect du RGPD *« si c’est gratuit c’est vous le produit »*
2. Navigateurs : ~~google chrome~~ --> LibreWolf, Firefox hardened (avec un user.js), basés sur chromium : Brave, ungoogled chromium (<https://ungoogled-software.github.io/ungoogled-chromium-binaries/>)...
3. Extensions pour bloquer pub & trackers (filtres) : Ublock Origin (possibilité de bloquer les avis de consentement aux cookies), Clear URL’s, CanvasBlocker Decentraleyes, Privacy Badger
4. (meta)Moteur de recherche : <https://searx.be/search> <https://startpage.com> <https://duckduckgo.com/> <https://qwant.com>
5. Utiliser des logiciels non propriétaires, open source (fondation mozilla, <https://framasoft.org>)
6. VPN
7. <https://www.privacytools.io/>
8. DNS Cloudflare (1.1.1.1 ou 1.0.0.1 et 2606:4700:4700::1111 ou 2606:4700:4700::1001)
9. Fingerprint : <https://amiunique.org>
10. <https://web.archive.org>
11. Vie privée très important pour les journalistes :

- Réseau Tor

- <https://totem-project.org/fr/index.html>

Ccl: *La vie privée totale sur internet n’existe pas*

## Sécurité

1. Mot de passe fort : <https://www.ssi.gouv.fr/administration/precautions-elementaires/calculer-la-force-dun-mot-de-passe/>
2. Gestionnaire de mdp : <https://keepassxc.org>
3. Virtual Private Network
4. Vérifier si une adresse @ a été piraté : <https://haveibeenpwned.com>
5. Faire des sauvegardes (sur un disque dur externe ou cloud) en prévision du phishing.
6. Vérifier où on rentre ses informations sensibles. Se méfier lorsque c’est louche, fautes d’orthographes, intonations, faire attention aux messages (lien) de ses proches : vérifier les noms de domaine
7. Lieu public : éviter de se connecter au wifi. Se connecter à un VPN : <https://protonvpn.com/fr>
8. Pour tester des virus = machines virtuelles, mais VPS (Virtual Private Server) mieux
9. Faire attention aux virus sur internet, vérifier la fiabilité d’un site internet : <https://fr.scamdoc.com/>
10. connections en HTTPS -> chiffrement des communications. Même si pas un gage de la fiabilité du site web
11. proxy sécurisé gratuit : <https://hide.me>, <https://startpage.com>
12. mettre à jour les logiciels
13. toujours verrouiller sa session, très important dans le monde professionnel