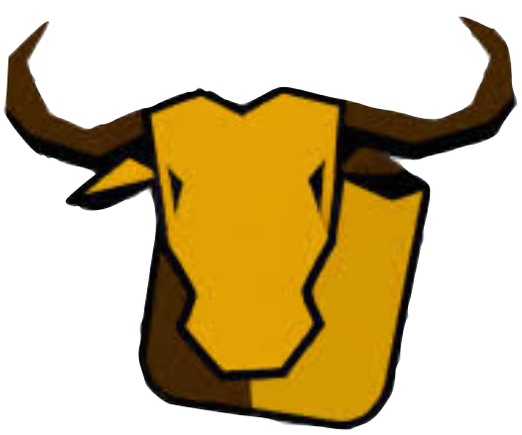
PHARE SUR WIKILIBRISTE

Wikilibriste est une communauté francophone de plusieurs milliers de passionnés qui militent pour un numérique plus **libre, éthique et respectueux de la vie privée**. Porté par un collectif de bénévoles, le projet s'organise autour d'une plateforme – un blog / wiki – où chacun peut consulter ou enrichir des centaines de fiches pratiques, tutoriels et analyses consacrés aux alternatives ouvertes aux services centralisés traditionnels. Avant de se lancer, les contributeurs recommandent de parcourir la section **Hygiène numérique** : elle dresse le panorama des risques et fixe les bases d'une transition en douceur vers des usages plus sûrs et mieux maîtrisés.

Conscient qu'un anonymat absolu est illusoire, Wikilibriste mise sur l'hygiène numérique : gestes simples, adoption progressive des outils et usage raisonné du numérique pour mieux préserver sa vie privée.

https://wikilibriste.fr/fr/hygiene-numerique



Dix gestes essentiels pour retrouver sa souveraineté numérique
par Ayo, propriétaire de Wikilibriste.fr et expert en sécurité informatique.

1. **Forger des mots de passe solides et uniques**
   - 12 caractères minimum (majuscules, minuscules, chiffres, symboles).
   - Un mot de passe ***unique*** par service.
   - Un gestionnaire de mots de passe libre :
     - Bitwarden (https://bitwarden.com/fr-fr/)
     - Protonpass (https://proton.me/fr/pass)
   - Activer sans tarder et partout où cela est possible l'authentification à 2 facteurs, appelé 2FA ou MFA, avec ces excellentes alternatives à Google authenticator :
     - Aegis Authenticator (https://getaegis.app/)
     - StratumAuth - ex. Authenticator Pro - (https://stratumauth.com/)

2. Mettre à jour systématiquement ses appareils et logiciels

Un créneau hebdomadaire suffit pour colmater les failles avant qu'elles ne deviennent des portes d'entrée pour tous types d'attaques.

- Mise à jour de vos systèmes (Linux, Windows ou Mac si vous êtes encore sur ces systèmes).
- Mise à jour de vos téléphones mobiles.
- Mise à jour de toutes applications que vous utilisez sur PC et sur mobile.

3. Sauvegarder et exporter ses données

Disque dur externe, clé USB chiffrée, cloud libre sécurisé : autant de filets de secours face aux défaillances matérielles ou aux rançongiciels (ransomwares pour les anglophiles), ces logiciels malveillants qui verrouillent vos données par chiffrement et n'en restituent l'accès qu'après paiement d'une rançon.

- Pour la partie sauvegardes locales : https://wikilibriste.fr/fr/debutant/sauvegarde
- Pour la sauvegarde en cloud :
  - Filen.io (https://filen.io)
  - Internxt (https://internxt.com/fr)
  - Infomaniak kDrive (https://www.infomaniak.com/fr/ksuite/kdrive)

4. Maîtriser les réglages de confidentialité

Chaque application dispose de son centre de contrôle ou paramètres de confidentialité et sécurité : passez-les en revue et désactivez toutes les options qui permettent la collecte de données.

5. Privilégier le logiciel libre

Issus de l'intelligence collective, les logiciels libres se multiplient : leur code source ouvert et auditable assure un niveau de sécurité élevé et en fait des alternatives crédibles, souvent équivalentes, qu'il est recommandé de privilégier.

Lorsqu'aucune option libre n'est disponible et qu'un outil propriétaire reste indispensable, informez-vous soigneusement sur ses conditions d'utilisation et la gestion de vos données personnelles avant de l'adopter. Wikilibriste recense ces solutions open source afin de vous guider vers celles qui répondent le mieux à vos besoins et votre modèle.

6. Choisir un navigateur et un moteur de recherche respectueux

Comme précisé dans notre dossier de résilience numérique, certains navigateurs sont à éviter au profit de solutions plus respectueuses de la vie privée :

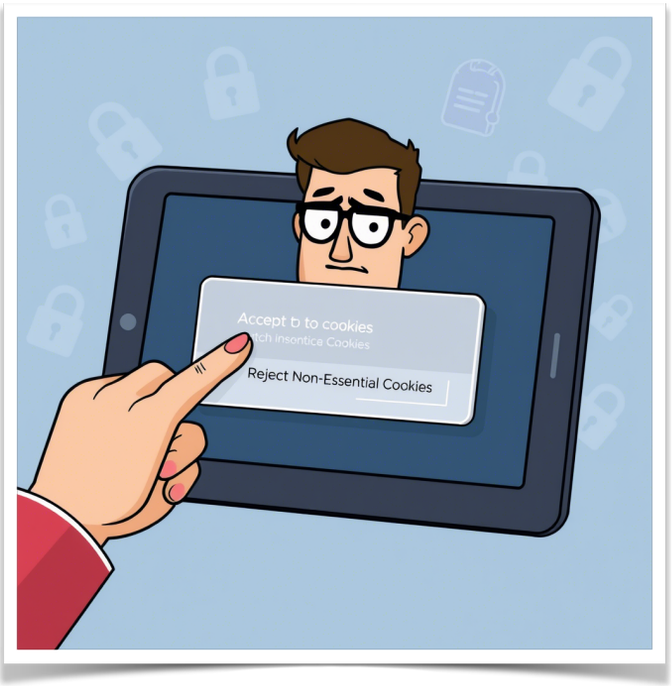
1. Optez par exemple pour **Firefox** associé à l'extension **uBlock Origin**
2. Ou choisissez un navigateur axé confidentialité tel que **LibreWolf** (https://librewolf.net) ou **Mullvad Browser** (https://mullvad.net/fr/browser).

https://wikilibriste.fr/fr/debutant/navigateurs.

Appliquez le même discernement à votre moteur de recherche :

- **Brave Search**, par exemple, est vivement recommandé pour sa politique de blocage du tracking et de respect des données.
- **SearXNG** ou **Whoogle** restent des options encore plus confidentielles.

https://wikilibriste.fr/fr/debutant/moteurs-recherche.



7. Refuser les cookies non essentiels

- Un **cookie** est un petit fichier qu'un site web dépose sur votre appareil, rattaché à son domaine : il peut retenir votre identifiant, votre langue, le contenu de votre panier… ou, plus intrusif, tracer vos habitudes à des fins statistiques ou publicitaires. Résultat : navigation profilée, vie privée en retrait, surface d'attaque élargie.
- La parade ? À chaque bannière, cliquez résolument sur **"Tout refuser"** ; en un geste, vous coupez court aux usages malveillants et fermez la porte aux profils publicitaires indésirables et à leur utilisation malveillante.

8. Utiliser un VPN de confiance lorsque nécessaire

Mullvad VPN ou iVPN chiffrent le trafic et masquent l'IP, sans pour autant promettre l'anonymat absolu.

Un VPN installe un tunnel chiffré entre votre appareil et un serveur distant : vos données circulent à l'abri des regards, votre adresse IP publique est remplacée par celle du serveur et les contenus géo-bloqués peuvent apparaître.

Toutefois, l'abonnement passe presque toujours par un prestataire commercial — paiement, éventuels journaux de connexion — si bien qu'un anonymat total reste impossible avec ces outils. Pour une approche transparente et respectueuse de la vie privée, Wikilibriste recommande des services libres et auditables tels que :

- **Mullvad VPN** (https://mullvad.net/fr)
- **iVPN** (https://www.ivpn.net/en)

https://wikilibriste.fr/fr/debutant/vpn-tor.

9. Opter pour une messagerie chiffrée open source

Pour protéger vos échanges, choisissez une messagerie **chiffrée de bout en bout (E2EE)**. Néanmoins, le chiffrement seul n'est pas une garantie absolue : si l'éditeur contrôle les clés, il peut — volontairement ou sous contrainte légale — accéder aux messages et les transmettre.

La parade ? Opter pour une solution à la fois chiffrée et open source, dont le code et la gestion des clés sont audités publiquement.

Certaines applications répondent à ces exigences, dans une moindre mesure comme :

- **Signal** (https://signal.org/fr/download) ou SimpleX (https://simplex.chat/fr)
- **Session** (https://getsession.org)
- **Element** (https://element.io), d

10. Rester vigilant

Quelques réflexes quotidiens simples protègent également efficacement vos données :

- **Navigation privée : complément, pas bouclier.** Le mode "privé" n'efface qu'historique et cookies ; il n'empêche ni les sites ni le fournisseur du navigateur de vous suivre. Installez une extension de blocage telle qu'**uBlock Origin** pour réduire le pistage.

- **Ports USB publics : danger de "juice jacking".** Ne rechargez pas téléphone ou ordinateur sur les prises des gares, aéroports ou centres commerciaux ; un logiciel malicieux peut s'y glisser au premier branchement.

- **Wi-Fi public : VPN indispensable.** Avant toute connexion sensible sur un réseau "ouvert" (hôtels, Starbucks, gare, hôpital, etc.), activez un VPN fiable pour chiffrer le trafic et décourager les interceptions locales.

- **Liens pernicieux : attention aux clics** ! Méfiez-vous quotidiennement des liens (URL) reçus et des QR codes orphelins, que ce soit par email ou sur votre mobile (SMS, whatsapp, etc.). Ne cliquez **JAMAIS** sur ces URL avant d'avoir vérifier que l'émetteur est une source fiable.

En bref : limitez les points de contact entre vos appareils et les infrastructures publiques, ou prévoyez les contre-mesures nécessaires pour déjouer toute tentative de piratage.

Pour investiguer davantage sur les mesures à mettre en place pour vous sécuriser, n'hésitez pas à utiliser le site internet Wikilibriste : https://wikilibriste.fr, ou venir poser vos questions sur le groupe Telegram de Wikilibriste : https://t.me/securite_informatique_libre.

SiTE : https://wikilibriste.fr

Telegram : https://t.me/securite_informatique_libre

NOUS SOMMES ...

Une communauté qui propose une liste d'articles et de tutoriels pour accompagner toute personne souhaitant améliorer son environnement numérique et tendre vers sa libération numérique.

Article écrit par Céline