Off grid

Table des matières

- 1. Navigateurs
- 2. Cloud
- 3. Email
- 4. Moteur de Recherche
- 5. VPN
- 6. Calendriers
- 7. Clients Email
- 8. Gestionnaire de Mots de Passe
- 9. Communication en temps réel
- 10. Système d'exploitation
- 11. Bonus
- Media
  - Films
  - Youtube
  - Mots-clés
- Tutoriel pour partir de 0
- Bonnes pratiques

Pourquoi la vie privée compte

Dans un monde où nos activités en ligne sont scrutées de près, la question de la vie privée n'a jamais été aussi pertinente. Mais pourquoi devrions nous nous en préoccuper ? Certains pourraient argumenter que la vie privée est un luxe dépassé dans l'ère numérique. Cependant, cette notion est loin d'être obsolète. En réalité, elle est au cœur de la question du pouvoir et du contrôle.

La vie privée, c'est bien plus que la simple dissimulation de secrets. Elle consiste à avoir le contrôle sur nos données, à décider qui peut y accéder et dans quelles circonstances. Cette définition souligne l'importance de protéger nos informations personnelles dans un monde où la collecte de données est omniprésente.

Bien souvent, la vie privée est confondue avec la sécurité ou l'anonymat. Pourtant, ces concepts se chevauchent mais ne se confondent pas. La sécurité concerne la confiance dans les applications que nous utilisons, tandis que l'anonymat vise à agir sans être identifié. La vie privée, quant à elle, garantit la confidentialité de nos données.

Un argument récurrent contre la protection de la vie privée est celui du "rien à cacher". Cette idée sous-entend que seuls ceux qui ont quelque chose à cacher ont besoin de vie privée. Pourtant, il s'agit d'un malentendu dangereux. La vie privée est un droit fondamental qui concerne chacun d'entre nous, indépendamment de nos activités.

Alors, comment pouvons nous protéger notre vie privée dans un monde numérique où nos données sont constamment sollicitées ? La réponse réside dans une intégration par défaut de la protection de la vie privée dans les logiciels et les services que nous utilisons. Il est temps de reconnaître que la vie privée n'est pas un luxe, mais une nécessité fondamentale pour une société libre et équitable.

Un Guide Essentiel pour Protéger votre Vie Privée en Ligne

Dans un monde numérique où nos données sont constamment exposées, il est essentiel de comprendre les menaces qui pèsent sur notre vie privée et comment y faire face. Pour simplifier, nous pouvons classer ces menaces en catégories générales, chacune nécessitant des précautions spécifiques.

1. **Anonymat** : Dissociez votre activité en ligne de votre identité réelle pour vous protéger des tentatives d'identification.
2. **Attaques Ciblées** : Protégez vous contre les attaques de pirates informatiques ou d'autres agents malveillants cherchant spécifiquement à accéder à vos données ou appareils.
3. **Attaques Passives** : Gardez vous des logiciels malveillants, des fuites de données et autres attaques visant un large groupe de personnes.
4. **Fournisseurs de Services** : Protégez vos données contre les fournisseurs de services en utilisant des outils comme le chiffrement de bout en bout.
5. **Surveillance de Masse** : Préservez votre vie privée contre la surveillance généralisée par des gouvernements, des organisations et des services en ligne.
6. **Capitalisme de Surveillance** : Protégez vous des réseaux publicitaires et d'autres collecteurs de données en limitant votre exposition en ligne.
7. **Exposition Publique** : Limitez la diffusion en ligne d'informations vous concernant, accessibles par les moteurs de recherche ou le grand public.
8. **Censure** : Contournez les efforts de censure en ligne exercés par des gouvernements ou des fournisseurs de services.

Chaque catégorie de menace requiert une approche spécifique pour se protéger. Par exemple, l'utilisation du chiffrement de bout en bout peut aider à sécuriser vos communications contre les fournisseurs de services, tandis que l'utilisation de réseaux anonymes comme Tor peut contrer la surveillance de masse.

La protection de votre vie privée en ligne nécessite donc une compréhension claire des menaces auxquelles vous êtes confronté et des outils disponibles pour vous protéger. En prenant des mesures proactives pour sécuriser vos données et votre identité en ligne, vous pouvez minimiser les risques et préserver votre vie privée dans un monde numérique en constante évolution.

Abstract >

« Pourquoi m'en faire, si je n'ai rien à me reprocher » ? Vient la question légitime : « Pourquoi m'en faire, si je n'ai rien à me reprocher, rien à cacher » ?

D'abord, ce qui sera « hors-la-loi » demain n'est pas ce qui est hors-la-loi aujourd'hui. Dans différents pays, des sms dissuasifs sont envoyés à des manifestants potentiels, des individus en désaccord avec le gouvernement, par exemple. La protection de la vie privée, c'est la protection de la liberté de penser et d'agir sans avoir de comptes à rendre. Quid si nos données sont utilisées pour museler toute contestation possible ? Il s'agit d'un système totalitaire.

Ensuite, même des actes « anodins » peuvent être retournés contre nous. Vous allez manger au fast-food en famille. Vous faites un accident vasculaire cérébral. Que dira votre assureur lorsqu'il comparera ces deux données en sa possession ? Va-t-il pouvoir vous dédommager malgré cet écart à un mode de vie sain ?

A cela, il faut ajouter la « fable de la grenouille ». La grenouille a tendance à prendre ses aises dans une casserole où l'eau bout progressivement. Avec la chaleur, elle en vient à se détendre. Jusqu'à ce qu'il soit trop tard et qu'elle meure ébouillantée. La question de la surveillance de masse, c'est cela : jusqu'à quel point irons-nous dans la collecte et le traitement massifs des données sur les citoyens avant de nous dire que « nous sommes cuits » ?

Enfin, comme le dit Snowden, à l'origine de la découverte de la surveillance de masse réalisée par la NSA, « ne pas se préoccuper de la surveillance de masse parce que vous n'avez rien à cacher, c'est comme ne pas se préoccuper de la liberté d'expression parce que vous n'avez rien à dire ». C'est égoïste. Il en va entre autres de la solidarité avec des minorités opprimées, par exemple… La protection des données personnelles est un garde-fou contre les abus de pouvoirs.

Déjà, si vous n'avez véritablement "rien à cacher", vous opposeriez-vous à ce que l'on mette une caméra dans votre salle de bain ? Dans votre chambre à coucher ? Que l'on expose vos mots doux, fussent-ils envoyés via SMS, courriel ou Facebook, sur la place publique ? Vous comprenez ici qu'il existe une sphère d'intimité dont chacun doit pouvoir rester maître, et choisir ce qu'il révèle ou non au monde.

Attention : la question n'est pas de savoir si vous même désirez rendre public tout ce qui vous concerne y compris votre sphère intime, la question est de savoir si un citoyen qui souhaite conserver une part d'intimité peut le faire !

> Voici ce qu'en dit Snowden: “Certains disent qu’ils n’ont ‘rien à cacher’, mais dire cela, c’est inverser les responsabilités”, a expliqué Edward Snowden. “Dire : ‘Je n’ai rien à cacher’, cela revient à dire : ‘Je me fiche de ce droit’. C’est dire : ‘Je ne dispose tellement pas de ce droit que j’en suis arrivé au point où je dois m’en justifier’. Alors que normalement, c’est le gouvernement qui doit se justifier de ne pas respecter vos droits”, a-t-il développé, pour appuyer son appel à une réforme de la politique américaine en matière de respect de la vie privée.

Tous les logiciels proposés ici sont Open-Source

> ⓘ Info
>
> Il est important de noter que bien souvent pour garder une sécurité optimale, il va falloir sacrifier un peu de confort. En effet, généralement, les services qui vous propose de vous faciliter la vie sont un gouffre pour la protection de vos données privées.

1. Navigateurs

- Brave
- Firefox

2. Cloud

- Proton Drive
- Syncthing

3. Email

- Proton Mail
- Mailbox.org

4. Moteur de Recherche

- DuckDuckGo
- Brave Search
- Ecosia

5. VPN

- Proton VPN

6. Calendriers

- Calendrier Proton

7. Clients Email

- Thunderbird

8. Gestionnaire de Mots de Passe

- KeePass
- Proton Pass

9. Communication en temps réel

- Signal

10. Système d'exploitation

- PC :
  - Tails
- Mobile
  - Graphene OS
- Applications Android
  - Secure Camera
  - Obtainium
  - Clavier
    - AnySoftKeyBoard

11. Bonus

- **FreeTube** Application de bureau gratuite et open-source pour YouTube. Lorsque vous utilisez FreeTube, votre liste d'abonnement et vos listes de lecture sont enregistrées localement sur votre appareil. Par défaut, FreeTube bloque toutes les publicités YouTube. En outre, FreeTube intègre en option SponsorBlock pour vous aider à sauter les segments de vidéos sponsorisées.
- Ninite Site qui permet de télécharger quelques logiciels de base comme Keepass ou Firefox en un clique, sans pub et à jour Vous pouvez même garder le .exe généré pour n'avoir qu'à mettre à jour automatique les logiciels sans revenir sur Ninite ou ailleurs
- Have I Been Pwned Permet de rechercher à travers plusieurs violations de données pour voir si votre adresse e-mail ou numéro de téléphone a été compromis.

- 10minutemail Permet de générer une adresse mail temporaire pour éviter de se faire spammer (il existe plusieurs sites différents 10minutemail qui peut être utile d'aller voir si les noms de domaine de celui-ci sont détectés et bloqués)
- Fake Name Generator Permet de générer une fausse identité numérique pour remplir des formulaires ou autre anonymement
- systemli Plusieurs services confidentiels (cloud, email, meet, réseau social, notes collaborative, message chiffré, nettoyeur de metadata, publication de textes avec expiration, appels, hebergements sites) Pas très stable à l'heure actuelle, plusieurs bugs, etc
- Onoff Application mobile pour second numéro de téléphone virtuelle (payant)

> D'autres à venir

Media

Films

- The Great Hack
- Derrière nos écrans de fumée
- Edward Snowden

Youtube

- Underscore_
- Micode

Mots-clés

> Si vous souhaitez vous renseigner un peu plus sur le sujet, vous trouverez quelques pistes ici (cette liste sera mise à jour au fur et à mesure, vous pouvez aussi m'envoyer un message[1] si vous avez trouvé de nouvelles informations)

- Wikileaks
- Julian Assange
- Edward Snowden
- Affaire Cambridge Analytica

Tutoriel pour partir de 0

1. **Jeter Alexa** et autre assistant personnel intelligent par la fenêtre (ne faites pas de cadeau empoisonné aux proches)
2. **Désactiver Siri et OK Google** dans les paramètres

3. **Désactiver Cortana** et l'empêcher de se lancer au démarrage
4. Mettre un **sticker devant sa caméra** du PC et téléphone (surtout la frontale)
5. **Désactiver FaceID** (à la rigueur utiliser l'empreinte digitale)
6. **Désactiver micro** du PC (pour l'activer que quand nécessaire)
7. Installer **Brave + Firefox** et choisir le **moteur de recherche** que vous souhaitez en suivant les recommandations de configuration
8. Prendre les services **Unlimited ou Family** de chez Proton sur 24 mois pour payer moins cher car dans tous les cas vous en aurez besoin pour la vie.
    - *Utiliser le code promo pour bénéficier de 20% de réduction*[2]
    - *Services : Mails, VPN, Calendrier, Drive et Gestionnaire de Mots de Passe*
9. Installer **Signal** et **informer son entourage** d'y aller aussi
10. Télécharger l'application clavier **AnySoftKeyboard** ou autre clavier Opensource pour les Android (À chercher pour IoS et m'envoyer un message[1-1] le cas échéant)
11. Dans le téléphone, **vérifier toutes les autorisations** de toutes les applications (même les applications systèmes qui sont parfois cachées en cliquant sur les trois points > afficher applications systèmes)
    - *À vos risques et vos choix de choisir de désactiver des autorisations que vous ne connaissez pas quand le message de prévention s'affiche. Mais pour la plupart des applications non cachées cela n'a aucune incidence*
12. Dans le PC, faire de même, naviguer dans tous les paramètres, lire et **autoriser/désactiver les autorisations inutiles** quitte à perdre un peu de confort d'utilisation

Bonnes pratiques

- Utiliser des pseudos sur Internet
- Acheter un filtre de protection et de confidentialité pour le téléphone afin de masquer l'écran pour les regards indiscrets
- Préférer le thème sombre car consomme moins d'électricité (pixel noir = pas de couleur donc pas d'allumage) et abime moins les yeux
- Activer le filtre lumières bleues sur vos appareils (les yeux vont s'habituer au contraste jaune) ou acheter des lunettes spéciales lumières bleues
- Désactiver la génération des aperçus de lien
- Mettre à jour régulièrement pour avoir les derniers correctifs de sécurité
- Laisser descendre les gens du train avant de rentrer permet d'éviter les retards de train, de se plaindre que la SNCF/RATP est nulle et participe à l'intelligence collective plutôt qu'à un peuple individualiste
- Aider et aimer son prochain même s'il n'est pas de notre avis, culture, religion.

---

1. Mail : offgrid@.com - Telegram : Jeff↩↩↩

2. M'envoyer un message[1-2] pour être whitelist afin de recevoir et utiliser le code promo↩