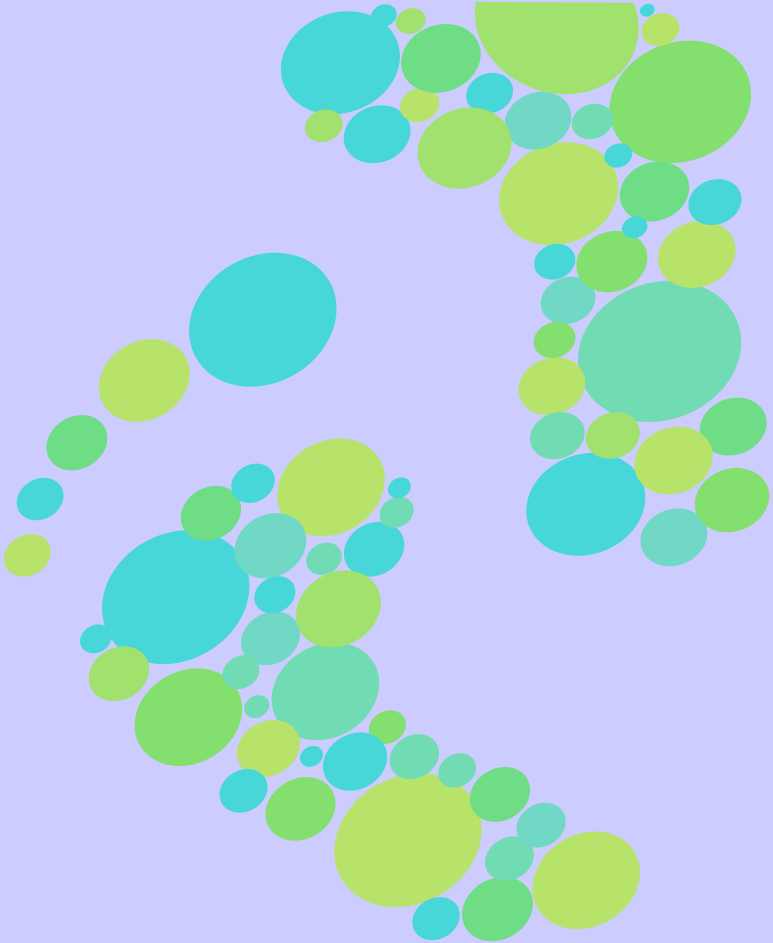
Document réalisé par les étudiants d'HEC Montréal dans le cadre du cours de Responsabilité Numérique des Organisations - été 2025.



GUIDE POUR UNE MEILLEURE HYGIÈNE NUMÉRIQUE

Prendre soin de son empreinte numérique passive en 10 mesures

Tout comme se laver les mains, les dents ou encore avoir une activité physique sont des gestes d'hygiène corporelle profondément ancrés dans notre quotidien, il serait bon d'**instaurer des gestes simples dans nos habitudes d'utilisation des outils numériques pour prendre soin de notre empreinte numérique passive**.

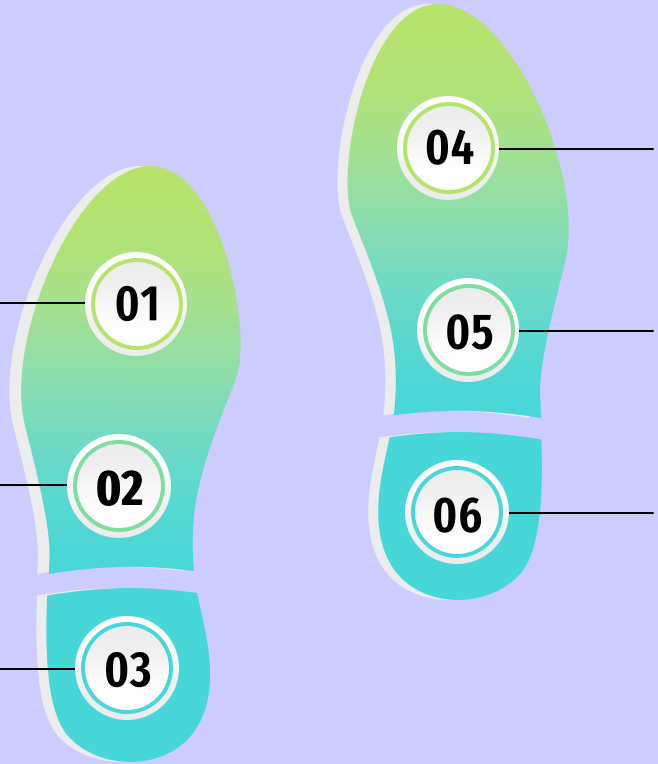
Sans faire de vous un expert en cyber-sécurité, ce guide est là pour vous aiguiller dans la **mise en place des bonnes habitudes** en matière d'**hygiène numérique**.

Il faut bien commencer quelque part et
vous venez de télécharger un bon point de départ !

Document réalisé par les étudiants d'HEC Montréal dans le cadre du cours de Responsabilité Numérique des Organisations - été 2025.

Document réalisé par les étudiants d'HEC Montréal dans le cadre du cours de Responsabilité Numérique des Organisations - été 2025.

Sommaire



Document réalisé par les étudiants d'HEC Montréal dans le cadre du cours de Responsabilité Numérique des Organisations - été 2025.

1. Qu'est-ce que l'empreinte numérique passive ?

Considérez votre empreinte numérique comme un **regroupement d'informations que l'on peut utiliser pour mieux vous connaître**.
Cette empreinte peut donc avoir un impact positif comme négatif, selon sa composition. Elle peut même être dangereuse si trop riche en information et facilement accessible.

Souvent représentée telle une empreinte de pieds laissée dans le sable, l'empreinte numérique fait référence aux informations que nous laissons derrière nous lorsque nous utilisons internet.

À travers les sites web que nous consultons, les courriels que nous envoyons et les informations que nous soumettons ou téléchargeons en ligne nous contribuons à notre empreinte de façon active et passive.

Document réalisé par les étudiants d'HEC Montréal dans le cadre du cours de Responsabilité Numérique des Organisations - été 2025.

Le Centre de la Sécurité des télécommunications du Gouvernement du Canada définit ces deux types d'empreintes comme suit :

Empreinte numérique active	Empreinte numérique passive
Données laissées à la suite d'activités intentionnelles, telles que l'affichage de contenu sur les médias sociaux, le remplissage de formulaires en ligne ou l'acceptation des témoins de navigateur.	Données laissées **involontairement** ou **sans le savoir**. Ces données sont souvent recueillies par la surveillance de votre adresse IP. Les sites Web et les applications peuvent installer des témoins sur les dispositifs sans vous en aviser, utiliser le suivi de la location ou consigner vos activités.

Ces empreintes contiennent parfois des informations sensibles dont certaines personnes ou organisations pourraient tirer profit au moyen de techniques de collecte de ces données, compromettant ainsi confidentialité et sécurité. Des empreintes numériques compromises peuvent alors entraîner un vol d'identité ou encore une atteinte à votre réputation.

Document réalisé par les étudiants d'HEC Montréal dans le cadre du cours de Responsabilité Numérique des Organisations - été 2025.

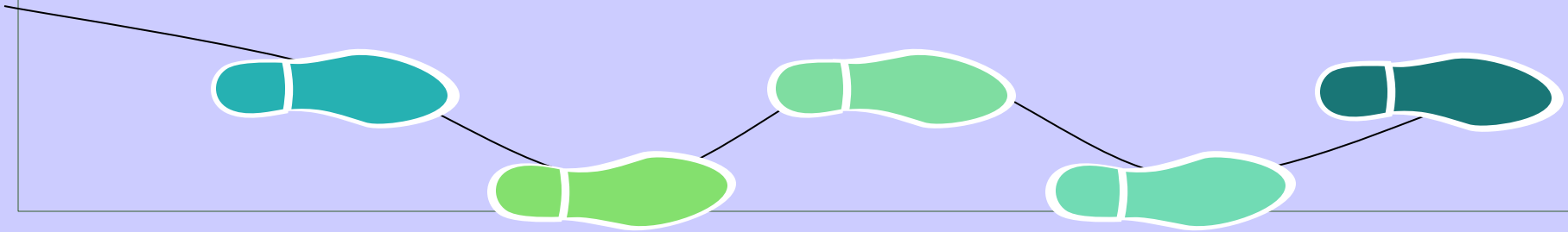
2. Routine à intégrer dans vos gestes du quotidien

Voici **5 mesures à vous approprier** telles des réflexes prudents et des comportements **à intégrer dans votre routine** afin d'atténuer les risques associés à votre empreinte numérique passive.

Elles sont recommandées par le Centre de la sécurité des télécommunications du Gouvernement du Canada.

On s'est dit qu'on pouvait leur faire confiance, **et vous ?**

On passe à l'action ?



Document réalisé par les étudiants d'HEC Montréal dans le cadre du cours de Responsabilité Numérique des Organisations - été 2025.

1 - Lire les politiques de confidentialité et les conditions d'utilisation

Avant de télécharger une application ou d'utiliser un service, il est important de lire et de bien comprendre les types d'information recueillie, les façons dont cette information peut être utilisée et les mesures de sécurité en place pour protéger vos renseignements personnels.

2 - Désactiver les témoins (cookies)

Même si vous ne partagez pas activement de l'information sur les applications et sites Web, vos données font l'objet d'un suivi par l'entremise de votre appareil, de votre adresse IP et de votre réseau.

3 - Configurer les paramètres par défaut de vos applications

Les paramètres de certaines applications sont réglés par défaut à « accès public ». Prendre le temps de configurer vos paramètres de sécurité et de protection de la vie privée au mode le plus sécurisé et restrictif possible est important.

4 - Désactiver les paramètres de surveillance

Éviter d'utiliser les applications non nécessaires qui exigent l'accès à votre emplacement (géolocalisation), à votre calendrier ou à vos contacts. Désactivez les paramètres qui analysent et surveillent vos activités dans le but de vous présenter de la publicité ciblée.

5 - Rester au fait des changements

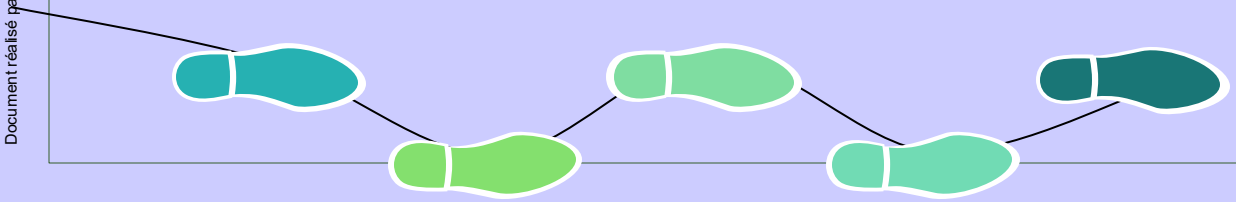
Les conditions d'utilisation et paramètres de protection de la vie privée des applications sont régulièrement mises à jour, assurez-vous d'en avoir connaissance.

Document réalisé par les étudiants d'HEC Montréal dans le cadre du cours de Responsabilité Numérique des Organisations - été 2025.

3. Bonnes habitudes, pour une approche plus globale

Là encore, nous nous appuyons sur les recommandations du Centre de la sécurité des télécommunications du Gouvernement du Canada :

- ☐ Installer un **antivirus** et un **pare-feu**
- ☐ Appliquer l'**authentification multifacteur** (AMF)
- ☐ Privilégier les **phrases de passe** robustes
- ☐ **Privilégier les réseaux sécurisés,** éviter le Wi-Fi public,
- ☐ **Identifier** les applications ou **bloquer** les adresses IP, les noms de domaine et les types de fichiers **reconnus pour être malveillants**



L'intelligence artificielle (IA), portez-y attention particulière !

Les algorithmes d'intelligence artificielle (IA) construisent leur banque de données avec les informations que vous lui fournissez. Qu'il s'agisse d'images ou des textes, tout l'intéresse !

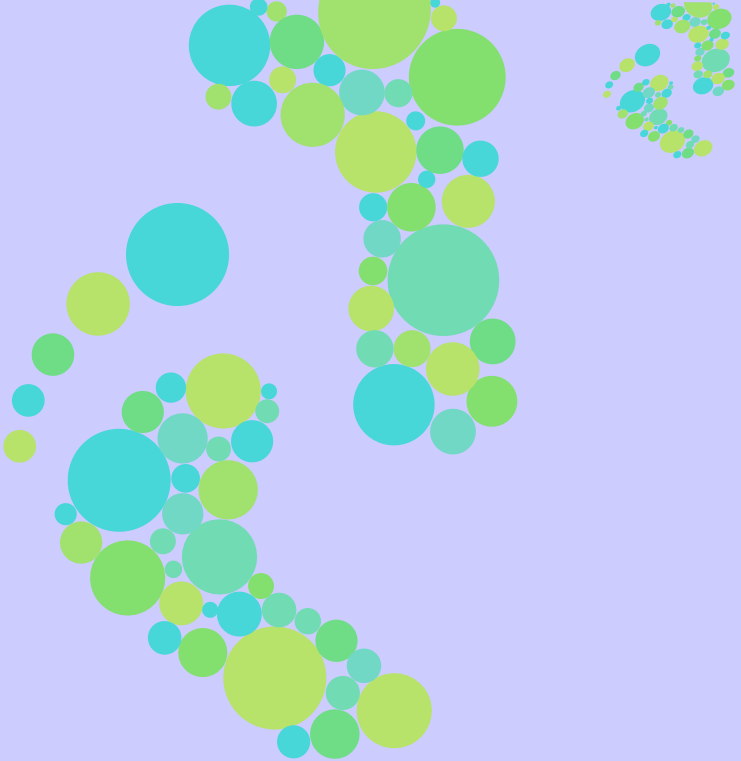
Plus encore que les moteurs de recherche, l'IA peut analyser votre empreinte numérique passive en effectuant un suivi de vos comportements en ligne. Ces systèmes sont souvent munis de composantes de collecte des données servant à des fins d'analyse et même de réutilisation pour améliorer l'apprentissage et les performances. Les données saisies pourraient être conservées dans le système, pour des fins d'entraînement, et ensuite divulguées en réponse à la demande d'autres utilisateurs qui ne devrait pas y avoir accès, normalement.

Plus vous partagez d'informations, plus vous êtes à risques pour la sécurité de vos renseignements et votre sécurité financière.

Soyez prudents et ne partagez pas d'informations personnelles, confidentielles ou sensibles au moyen de l'IA!

Document réalisé par les étudiants d'HEC Montréal dans le cadre du cours de Responsabilité Numérique des Organisations - été 2025.

4. Boite à outils



Check-list

01 Lire les politiques de confidentialité et les conditions d'utilisation

02 Désactiver les témoins (cookies)

03 Configurer les paramètres par défaut des applications

04 Désactiver les paramètres de surveillance

05 Rester au fait des changements

06 Installer antivirus et pare-feu

07 Appliquer l'authentification multifacteur

08 Privilégier les phrases de passe robustes

09 Privilégier les réseaux sécurisés

10 Bloquer les applis, adresses IP, domaines et fichiers malveillants

Document réalisé par les étudiants d'HEC Montréal dans le cadre du cours de Responsabilité Numérique des Organisations - été 2025.

Document réalisé par les étudiants d'HEC Montréal dans le cadre du cours de Responsabilité Numérique des Organisations - été 2025.

5. Pour aller plus loin

- Pour avoir une idée du type d'empreinte que vous laissez (tout en contribuant à une étude fiable 😉) : https://amiunique.org/fr
- Pour vérifier si votre adresse e-mail est victime d'une violation de données : https://haveibeenpwned.com https://www.malwarebytes.com/digital-footprint

  Et autres : Kaspersky, AVG, Norton, Bitdefender
- The National Cybersecurity Alliance, OBNL dont la mission est de créer un monde plus sûr et interconnecté : https://www.staysafeonline.org/
- Extension de navigateur "Consent-o-Matic" qui permet de répondre automatiquement aux fenêtres contextuelles, en fonction des préférences personnalisables de l'utilisateur :

Firefox: https://addons.mozilla.org/en-US/firefox/addon/consent-o-matic/

Chrome: https://chrome.google.com/webstore/detail/consent-o-matic/mdjildafknihdffpkfmmpnpoiajfjnjd

Installez l'**extension d'Hygiène Numérique que nous vous proposons** pour recevoir des **rappels simples et efficaces** afin de mieux protéger vos données au quotidien.

Document réalisé par les étudiants d'HEC Montréal dans le cadre du cours de Responsabilité Numérique des Organisations - été 2025.

6. Conclusion

Bien que l'on apprécie une navigation personnalisée, adaptée à nos besoins et favorisant une meilleure expérience utilisateur, il reste important de veiller à la collecte de données passives qui vient avec.

La collecte de données passives est un élément clé dans un paysage numérique plus personnalisé et plus efficace pour l'usage intelligent des données.

En ayant une bonne hygiène numérique vous maitriserez davantage votre empreinte numérique passive. Vous serez davantage conscients des informations que vous partagez et vous pourrez ainsi réduire considérablement les risques associés à vos activités en ligne.

Tout comme la pleine conscience peut être bénéfique à votre bonne santé physique, la pleine conscience en matière de partage passif de vos données contribuera à votre bonne santé numérique !

Protéger vos données, c'est protéger votre liberté !

Document réalisé par les étudiants d'HEC Montréal dans le cadre du cours de Responsabilité Numérique des Organisations - été 2025.

Sources

- Centre de la sécurité des télécommunication, Gouvernement du Canada (février 2024), *Empreinte numérique*, ITSAP.00.133, ISBN 978-0-660-69845-8, récupéré le 09/06/2025 de www.cyber.gc.ca/sites/default/files/itsap.00.133-empreinte-num%C3%A9rique.pdf
- Agence nationale de la sécurité des systèmes d'information du gouvernement français (septembre 2017), *Guide d'hygiène informatique, renforcer la sécurité de son système d'information en 42 mesures*, Version 2.0.
- CNIL (Commission Nationale de l'Informatique et des Libertés), Janvier 2019. *La forme des choix, Données personnelles, design et frictions désirables,* CAHIERS IP INNOVATION & PROSPECTIVE numéro 06.
- Ministère de la cybersécurité et du numérique (Gouvernement du Québec) : *Mathieu, cyberprudent* récupéré le 09/06/2025 de https://youtu.be/St34iLIV444?si=exBr1DxtfRqXR9Jj
- Ministère de la cybersécurité et du numérique du Québec, *Guide des bonnes pratiques d'utilisation de l'intelligence artificielle générative applicable aux outils d'intelligence artificielle générative externes*, octobre 2024.
- Gildas Avoine, Pascal Junod (2024), *Cybersécurité et hygiène numérique au quotidien, 129 bonnes pratiques à adopter pour se protéger*, Dunod.
- Malwarebytes (2025), *What is a digital footprint and how to protect it*, récupéré le 09/06/2025 de https://www.malwarebytes.com/fr/cybersecurity/basics/digital-footprint
- Guilloteau, Stéphane, 29 juin 2020 - Mis à jour le mercredi 15 juin 2022, *Que sont les "dark patterns" et leurs impacts sur les données personnelles ?* récupéré de https://hellofuture.orange.com/fr/que-sont-les-dark-patterns-et-leurs-impacts-sur-les-donnees-personnelles/#_edn11
- Système d'intelligence open source Knowlesys, Académie OSINT (2025), Guide essentiel pour comprendre et gérer votre empreinte numérique récupéré le 2025-06-09 de https://knowlesys.com/fr/osint-academy/analytics/essential-guide-to-understanding-and-managing-your-digital-footprint.html
- Métadonnées et vie privée, un aperçu technique et juridique (et son infographie), Octobre 2014, Commissariat à la protection de la vie privée du Canada. https://www.priv.gc.ca/media/2347/md_info_201410_f.pdf