Fiche 9

Comment se porte votre empreinte numérique?

Avez-vous posé l'un ou l'autre de ces gestes, ces derniers mois?

- **consulter le fil d'actualités d'un média social;**
- **utiliser la carte de fidélité de votre épicerie préférée;**
- **utiliser le GPS de votre téléphone pour vous rendre à une rencontre professionnelle;**
- **répondre à l'appel téléphonique d'une personne inconnue.**

Si oui, ceux-ci sont tous susceptibles d'avoir renforcé votre empreinte numérique!

Pour aller plus loin

Dès que vous utilisez une technologie numérique, vous êtes susceptible de laisser une petite trace de votre passage, parfois même sans le savoir… un peu comme on laisserait des empreintes digitales sur les objets qu'on utilise. Toutes ces informations mises ensemble constituent votre empreinte numérique, et peuvent être utilisées par d'autres pour anticiper vos comportements ou ceux de votre organisation, via les outils d'intelligence artificielle[16].

Est-ce grave de laisser une empreinte numérique derrière soi?

Il est tout à fait normal d'avoir une empreinte numérique, cependant celle-ci peut :

- créer une faille de cybersécurité pour votre organisation, en particulier lorsqu'elle s'additionne avec celle de collègues ou de partenaires;
- augmenter votre risque d'être victime d'usurpation d'identité, sur les médias sociaux, auprès des administrations publiques, des institutions bancaires, etc.;
- vous exposer à des campagnes ciblées d'influence, affecter à moyen terme votre crédibilité, et indirectement l'autonomie du Québec au regard d'autres nations et de divers intérêts Fiche 11.

Partager ses performances de course à pied sur Strava

Une enquête publiée dans le journal *Le Monde* en 2024 a démontré comment l'utilisation de l'application sportive Strava a permis d'anticiper les futurs déplacements et lieux de séjour de plusieurs présidents, comme Emmanuel Macron, Joe Biden et Vladimir Poutine[48, 50].

Fiche 9

Comment se porte votre empreinte numérique?

Comment limiter votre empreinte numérique[49]?

- **Prenez le temps qu'il faut,** face à la multitude d'actions que vous posez dans l'univers numérique (création de comptes, remplissage de formulaires, etc.).
- **Adoptez des réflexes de sobriété numérique.** Lorsque vous utilisez des logiciels en ligne, demandez-vous s'ils offrent une réelle plus-value, en particulier pour les logiciels utilisant de l'IA générative Fiche 15.
- **Remplissez les champs obligatoires des formulaires,** et interrogez-vous sur la pertinence de fournir les informations optionnelles.
- **Désactivez les témoins,** autant que possible, lorsque vous entrez dans un espace numérique. Ces témoins gardent en mémoire votre activité sur le site Web (historique de navigation, de connexion ou d'achat). Normalement, ces informations sont utilisées pour vous offrir une expérience personnalisée, mais elles peuvent aussi être partagées et utilisées à votre insu pour d'autres fins.
- **Prenez connaissance des politiques de confidentialité et des conditions d'utilisation** des outils numériques, notamment le type d'information recueillie et leurs conditions de gestion. En cas de doute, consultez les responsables de la protection des renseignements personnels, les responsables des habilitations de sécurité ou les responsables de la sécurité des systèmes informatiques de votre organisation.
- **Faites un tour de vérification des paramètres de vos applications** pour limiter les accès publics et les paramètres qui impliquent l'accès à votre emplacement, votre calendrier, vos contacts, etc.

Pour aller plus loin