La gestion de votre empreinte numérique

Une empreinte numérique est l'ensemble des données présentes sur Internet, liées à vos activités en ligne. Il s'agit notamment de vos messages sur les réseaux sociaux, chats et SMS, de votre historique de navigation, vos courriels, achats en ligne et données de localisation. Votre empreinte numérique peut :

- **Accroître le risque d'être victime d'une arnaque.** Les arnaqueurs et les fraudeurs peuvent utiliser votre empreinte numérique pour vous cibler, usurper votre identité ou voler vos données.
- **Exposer vos activités à une surveillance, que ce soit par des autorités gouvernementales ou par des individus abusifs ou manipulateurs.** Il s'agit notamment de connaître votre localisation si vous l'avez activée ou si vous vous connectez à vos réseaux sociaux.
- **Accroître le risque de victimisation** Les criminels utilisent l'empreinte numérique pour cibler des personnes et les entraîner dans des formes de travail forcé ou contraint. Des extrémistes et autres acteurs malveillants peuvent également utiliser l'empreinte numérique pour cibler des personnes au moyen de discours haineux ou des crimes motivés par la haine.
- **Nuire à votre dossier d'immigration.** Dans le cadre de nombreuses demandes d'immigration, il est désormais obligatoire de fournir les comptes de réseaux sociaux, les identifiants et autres données numériques, et les appareils électroniques peut être inspectés lors de l'entrée aux États-Unis ou d'une mise en garde à vue par le Département de la sécurité intérieure (Department of

Homeland Security). L'activité en ligne d'une personne peut être utilisée pour influencer les décisions concernant sa détention, son expulsion, le changement de son statut, sa naturalisation, l'asile ou d'autres formes d'aides à l'immigration.

La gestion de votre empreinte numérique est fondamentale pour préserver votre sûreté, votre sécurité et votre réputation !

12 Conseils pour la gestion de votre empreinte numérique

1. **Protégez vos appareils et vos comptes.** Assurez-vous que tous vos appareils sont protégés par un mot de passe fort et dans l'idéal, par l'authentification à deux facteurs. Il s'agit de deux méthodes d'authentification, comme un mot de passe en plus de la saisie d'un code que vous recevez sur votre téléphone portable.

2. **Ne partagez pas des données à caractère privé.** Ne publiez pas votre nom complet, votre adresse, votre numéro de téléphone ou d'autres données privées sur Internet, y compris sur les réseaux sociaux.

   Ne géolocalisez pas vos publications sur les réseaux sociaux.

   Ne publiez pas de photos permettant d'identifier votre localisation, votre domicile, votre lieu de travail ou d'études, comme des numéros de maison, des panneaux de rue, des plaques d'immatriculation, des logos d'uniforme, etc.

3. **Activez la confidentialité de vos comptes.** Si vous avez des comptes sur des réseaux sociaux, assurez-vous qu'ils sont configurés en mode privé. En général, il suffit d'aller dans votre compte, puis dans les Paramètres ou la rubrique Confidentialité, et de vous assurer que l'option « privé » est activée.

4. **Supprimez vos comptes inactifs.** Si un compte n'est plus utilisé, pensez à le supprimer. Pensez également à désactiver le stockage en ligne ou les comptes sur des anciens appareils encore en votre possession mais peu utilisés.

5. **Désactivez le suivi de localisation.** Pour cela, rendez-vous dans les paramètres de votre appareil, généralement à la rubrique « Confidentialité », « Sécurité » ou « Localisation ». Désactivez ensuite les services de localisation pour empêcher les applications et les services d'accéder à votre position.

6. **Limitez vos publications.** Publiez un minimum de données en ligne.

   Faites attention au contenu de vos publications, qui peut être déformé ou vous rendre plus vulnérable à des attaques ciblées. Par exemple, une photo où vous consommez de l'alcool, tenez une arme, etc.

7. **Refusez les demandes d'amis de personnes inconnues.** N'acceptez que les demandes d'amis de personnes que vous connaissez. N'importe qui peut se cacher derrière un profil, y compris des escrocs, des trafiquants et des personnes cherchant à vous surveiller.
   Supprimez de votre liste d'amis celles et ceux que vous ne connaissez pas personnellement.

8. **Supprimez les contenus et applications sensibles de vos téléphones et autres appareils.** Si vous voyagez à l'international, les agents du Département de la sécurité intérieure peuvent inspecter les appareils électroniques aux points d'entrée lors de votre retour aux États-Unis. Supprimez tous les messages, photos, applications et autres contenus qui pourraient être mal interprétés.

9. **Communiquez en toute sécurité.** Privilégiez les applications offrant un cryptage de bout en bout, comme WhatsApp, Signal et Telegram.

   Remarque : même si elles sont plus sécurisées, les plateformes de messagerie chiffrée peuvent contribuer à votre empreinte numérique via les métadonnées enregistrées (contacts, horaires des échanges), ainsi que le contenu partagé (vidéos, images, informations de profil). Restez vigilant.e dans vos communications.

10. **Faites attention lorsque vous naviguez sur le web.** Ne cliquez pas sur des liens suspects provenant d'expéditeurs inconnus et ne consultez pas des sites dont la fiabilité n'est pas établie, car ils peuvent vous exposer à des virus ou à une surveillance.

    Ne communiquez que les informations nécessaires et méfiez-vous des sites ou des applications qui en demandent plus.

    Pensez à vider régulièrement les cookies et le cache de votre navigateur. Pour cela, accédez aux Paramètres de votre navigateur, puis à la rubrique Confidentialité, et sélectionnez « Supprimer les données de navigation » ou une option équivalente.

11. **Utilisez un téléphone portable temporaire ou jetable.** Ces téléphones sont souvent prépayés et sans contrat, ce qui permet de mieux préserver votre anonymat et d'éviter

d’être tracé.e. Toutefois, si vous optez pour un téléphone temporaire, assurez-vous que les personnes qui doivent vous joindre (travailleur social, avocat, etc.) ont bien votre nouveau numéro. Certaines personnes préfèrent utiliser deux téléphones : un temporaire pour leurs activités en ligne, et un permanent pour leurs communications importantes et régulières avec leurs contacts clés.

12. **Utilisez des caches pour caméras.** Recouvrez l’objectif de votre téléphone et votre ordinateur portable quand vous ne les utilisez pas. Cela limite les risques d’intrusion dans votre vie privée.