TELUS Averti

Comment protéger ta vie privée en ligne

Créé en partenariat avec: Habilo Médias

Te promener sur Internet et marcher sur du béton frais ont une chose en commun : l'empreinte de ton passage pourrait y rester à vie. Chaque fois que tu consultes un site web ou une application connectée, tu y laisses une empreinte numérique. Parfois, tu sais avec certitude quelle est cette empreinte, par exemple, quand une photo ou un message est partagé en ligne, mais, souvent, tu ne sais pas vraiment quelles informations tu laisses derrière toi.

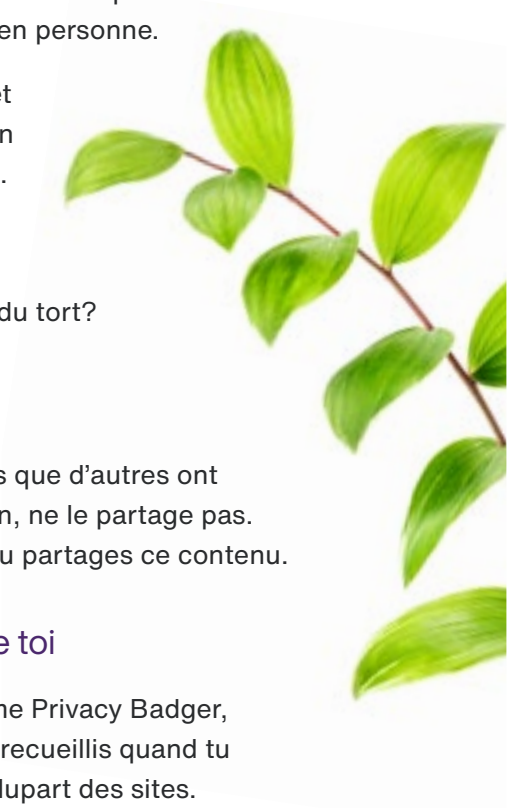
Heureusement, il y a des façons de contrôler la quantité de renseignements qui est collectée à ton sujet, et ce à quoi ils serviront.

Bien choisir ce que l'on partage en ligne

- Quel que soit le site, n'entre jamais de renseignements privés, comme ta date de naissance complète, un numéro de carte de crédit ou tes noms d'utilisateur et mots de passe, sauf s'il s'agit d'un site sécurisé envers lequel tu as confiance. Tu sauras qu'un site est sécurisé quand l'adresse commence par https (au lieu de http) et qu'elle est précédée du petit cadenas.
- Il faut aussi savoir que les réseaux Wi-Fi publics n'offrent pas la même sécurité qu'un réseau à la maison. N'oublie pas que les noms des réseaux peuvent être modifiés, ce qui permet aux pirates de créer de faux réseaux en leur donnant un nom qui semble officiel, comme « Bibliothèque municipale » ou « Café Wi-Fi ». Ces pirates peuvent ensuite espionner les gens qui se connectent au réseau, ou installer un logiciel malveillant dans leurs appareils. Vérifie deux fois plutôt qu'une pour t'assurer d'être connecté au bon réseau.
- Ne magasine pas en ligne et n'accède pas à ton compte bancaire à partir d'un ordinateur public ou partagé. Cela s'applique aussi à certains endroits qui te semblent sûrs, comme la bibliothèque de ton école. Même là, quelqu'un pourrait voir ce que tu tapes et envoies à l'aide de ton ordinateur. Les ordinateurs partagés ne devraient servir qu'à la navigation. Il ne faut pas les utiliser pour accéder à des comptes personnels.
- C'est aussi une bonne idée de masquer la caméra sur les ordinateurs portables et les autres appareils mobiles, par exemple, avec un papier Post-it ou un protecteur de webcaméra. Des cybercriminels pourraient potentiellement accéder aux caméras de tes appareils (ou aux microphones) et t'enregistrer sans que tu le veuilles ou que tu le saches.

Médias sociaux

- Quand tu publies des photos, ou quoi que ce soit d'autre, sur un réseau social, demande-toi d'abord qui pourra voir ta publication. La quasi-totalité des médias sociaux propose des paramètres de gestion de la vie privée. Cela te donne un certain contrôle sur qui verra ou non tes publications. Cependant, n'oublie pas que tes amis pourront quand même partager tes photos et tes messages avec d'autres personnes.
- Quand quelqu'un veut être ajouté à ta liste d'amis, réfléchis bien avant d'accepter. Refuse les demandes de gens que tu n'as encore jamais rencontrés en personne.
- Même en configurant soigneusement tes paramètres de vie privée, et peu importe la confiance que tes amis t'inspirent, il existe toujours un risque que tes publications soient vues par les mauvaises personnes. Avant de partager quelque chose, pose-toi ces quatre questions :
  - Est-ce que je veux qu'on me voie comme ça?
  - Est-ce que quelqu'un peut utiliser cette publication pour me faire du tort?
  - Vais-je me sentir mal si quelqu'un partage ma publication?
  - Quelle est la pire chose qui puisse arriver si je publie ceci?
- Penses-y deux fois avant de partager des publications ou des photos que d'autres ont partagées. Si le contenu peut être blessant ou gênant pour quelqu'un, ne le partage pas. Dans l'incertitude, vérifie auprès de la personne si elle accepte que tu partages ce contenu.



Contrôler ce que les applications et les sites web savent de toi

- Ajoute un module d'extension ou un plugiciel à ton navigateur, comme Privacy Badger, Ghostery et Disconnect, pour contrôler les renseignements qui sont recueillis quand tu visites un site web. Ces outils bloquent les fonctions de suivi sur la plupart des sites.
- Installe un moteur de recherche, comme DuckDuckGo, qui n'enregistre pas tes renseignements personnels ou tes données de recherches sur le web, et donc qui ne les partage pas non plus. Utilise le mode Incognito ou le mode Privé avec ton navigateur.
- Sur un téléphone ou une tablette, vérifie les autorisations pour comprendre quels renseignements sont recueillis par chaque application. Tu peux alors désactiver chaque élément que tu ne souhaites pas partager. Sur un iPhone ou un iPad, clique sur Réglages, puis sur Confidentialité. Ensuite, regarde chaque catégorie, comme Micro ou Appareil photo, pour voir quelles applications ont accès à ces fonctions sur ton appareil. Sous Android, ouvre Paramètres et clique sur Applications, puis sur Gestion des autorisations.

Pour être en sécurité en ligne, tu dois t'informer des menaces qui existent et prendre le temps nécessaire pour sécuriser tes comptes et protéger tes renseignements personnels.

telus.com/**averti**