

Comprendre le paysage numérique

Qu'est-ce que le paysage numérique?

Le paysage numérique est le monde en ligne créé par :

- les appareils que nous utilisons (téléphones, tablettes, ordinateurs)
- les sites Web, applications et services que nous utilisons
- les informations que nous envoyons et recevons
- les personnes et systèmes qui fonctionnent en arrière-plan

Si vous utilisez le courriel, les services bancaires en ligne, les achats en ligne, les applications de messagerie ou des portails gouvernementaux ou de santé, vous faites déjà partie du paysage numérique.

Comment l'information circule-t-elle en ligne?

Lorsque vous allez en ligne :

- l'information quitte votre appareil
- elle est stockée ailleurs
- elle peut être partagée ou réutilisée

Une fois en ligne, l'information peut circuler, sa trajectoire est hors de votre contrôle. Il est donc particulièrement important d'être prudent avant de partager.

Certaines décisions en ligne sont difficiles à prendre

En effet, les décisions en ligne peuvent sembler difficiles à prendre car plusieurs facteurs psychologiques et techniques altèrent notre jugement habituel. De tels facteurs comprennent les suivants.

- L'anonymat ou l'identité cachée : il est souvent difficile de vérifier qui se cache derrière un profil ou un message, ce qui crée, bien sûr, un climat d'incertitude.
- L'imprévisibilité : les messages peuvent arriver de façon inattendue, forçant une réaction immédiate, sans préparation mentale préalable.
- Le sentiment d'urgence : de nombreuses situations en ligne (publicités, arnaques, sollicitations) utilisent des tactiques de pression pour vous pousser à agir rapidement, empêchant une réflexion rationnelle.
- La crainte de faire des erreurs fatales : une fois publiée ou envoyée, une information peut être difficile à effacer, ce qui amplifie la peur de faire un mauvais choix.

Il est donc normal d'hésiter à agir ou de ressentir de l'incertitude. Prenez une pause! Oui, la pause est l'un des outils de sécurité les plus efficaces pour reprendre le contrôle sur vos décisions en ligne.

Votre empreinte numérique

Votre empreinte numérique est la trace d'information créée par vos activités en ligne, incluant :

- les recherches et la navigation
- les publications, mentions « J'aime » et commentaires
- les courriels et messages
- l'activité dans les applications

Ces informations peuvent servir, mais elles peuvent aussi être mal utilisées si elles sont trop largement partagées.

Les risques du partage excessif

Tout ce qui est partagé en ligne peut être copié, enregistré ou repartagé.

Voici quelques habitudes à prendre et conserver pour rester en sécurité :

- évitez de partager des renseignements personnels sensibles (adresse complète, date de naissance)
- désactivez le partage de localisation lorsque c'est possible
- réfléchissez avant de publier car, même supprimées, les publications peuvent être conservées

Ce qui intéresse les fraudeurs

Les fraudeurs s'intéressent à :

- vos coordonnées
- vos habitudes et vos routines
- votre confiance
- votre sentiment d'urgence

Les fraudes reposent sur la psychologie, pas sur l'intelligence. Tout le monde peut être ciblé.

Sensibilisation au piratage psychologique

Le piratage psychologique utilise l'émotion et la manipulation plutôt que la technologie pour influencer vos actions.

Si un message joue sur l'émotion plutôt que sur la logique, faites une pause.

Qu'est-ce que l'hameçonnage?

L'hameçonnage est une fraude dans laquelle des personnes malveillantes se font passer pour une source fiable afin de voler des renseignements personnels ou financiers.

L'hameçonnage peut se présenter par :

- courriel
- message texte (texto ou SMS)
- appel téléphonique
- messages dans des applications ou sur les médias sociaux

Indices d'hameçonnage

Faites preuve de prudence si un message comporte :

- de la pression pour agir immédiatement
- une exigence de confidentialité
- une demande de paiement par cartes-cadeaux ou cryptomonnaie
- des pièces jointes ou des liens inattendus
- une demande de renseignements personnels ou financiers

Si vous avez le moindre doute, ne cliquez pas.

Votre protection en ligne

Avant de répondre à un message, posez-vous les questions suivantes :

- est-ce que je connais l'expéditeur?
- est-ce que j'attendais ce message?
- le message traite-t-il d'urgence, le contenu est-il émotionnel?
- la pièce jointe ou le lien semble-t-il inhabituel?

Si votre certitude n'est pas à 100 %? Arrêtez immédiatement et faites des vérifications.

Principes de base pour sécuriser des mots de passe

Évitez :

- d'utiliser votre nom, votre date de naissance ou le nom du service
- les séquences simples ou les expressions courantes

Utilisez plutôt :

- des mots de passe longs ou des phrases de passe
- des phrases ou des mots de passe faciles à mémoriser mais personnels
- une phrase ou un mot de passe différent pour chaque compte

Le pouvoir de la pause

Faites une pause avant de :

- cliquer sur des liens
- répondre à des messages
- partager des renseignements personnels

Faire une pause perturbe les fraudes et vous donne aussi le temps de réfléchir clairement.

Si quelque chose tourne mal

Les erreurs arrivent. L'important, c'est la réaction.

Si vous avez cliqué sur quelque chose de suspect :

- cessez de répondre
- n'envoyez pas d'autres informations
- changez vos mots de passe si nécessaire
- demandez de l'aide

De l'aide fiable est disponible

L'aide fiable peut venir des sources suivantes :

- le service de lutte contre la fraude de votre institution financière
- des services gouvernementaux (contactés directement)
- une personne de confiance, comme un ami ou un membre de la famille
- Canadiens Branchés

Ressources supplémentaires

Voici les liens qui ont été partagés dans le clavardage pendant la présentation

- Centre antifraude du Canada: Signaler les cas de fraude et de cybercriminalité
<https://antifraudcentre-centreantifraude.ca/report-signalez-fra.htm>
- Signaler les messages textes indésirables au numéro 7726
<https://www.pensezcybersecurite.gc.ca/fr/bloques/signaler-messages-textes-indesirables-numero-7726>
- Inscrivez-vous ici pour participer à d'autres ateliers
<https://cnpea.ca/fr/a-propos-du-rcpmta/webinaires-rcpmta/1480-mois-de-la-pr%C3%A9vention-de-la-fraude-s%C3%A9rie-de-webinaires-sur-la-cyber-s%C3%A9curit%C3%A9>
- Digital Footprint Check: Vérifiez gratuitement votre empreinte numérique (en anglais)
<https://www.digitalfootprintcheck.com/>
- Ce site web permet de vérifier si un appareil reçoit toujours des mises à jour (en anglais)
<https://endoflife.date/tags/device>

Vous avez des questions ou si vous souhaitez obtenir du soutien concernant l'un des sujets abordés ici? Communiquez avec Canadiens Branchés au :

www.canadiensbranches.org.

Nos personnes bénévoles sont prêtes à vous aider et à s'assurer que vous vous sentiez en confiance et bien accompagné dans votre parcours numérique.