# ccèsTI CITOYEN 2.0

Fonds de développement économique LaPrade St-Maurice

## Cybersécurité en voyage

# La cybersécurité en voyage

## Wi-Fi

Vous pouvez connecter vos appareils à Internet à partir de points d'accès sans fil, parfois gratuitement, dans des cafés, des hôtels ou des aéroports pendant vos déplacements. Ces réseaux Wi-Fi publics ne sont pas sécurisés et sont accessibles à tous. **N'étant pas sécurisés, ils sont donc faciles à pirater.**

Les gens qui cherchent à effectuer un vol d'identité et de renseignements personnels peuvent créer des points d'accès gratuits à Internet d'une manière qui inspire confiance. Ils peuvent même imiter un réseau légitime en modifiant légèrement son nom. Lorsque vous vous branchez à leur système, votre appareil électronique devient vulnérable à une attaque. Assurez-vous de vérifier le nom de toute connexion Internet avant d'ouvrir une session.

**Les renseignements transférés au moyen d'un réseau inconnu peuvent être interceptés**. Ne vous connectez pas à des comptes renfermant de l'information sensible **comme un compte bancaire** et ne transmettez aucun renseignement que vous refuseriez de divulguer à quiconque.

## Ordinateurs publics

Les **enregistreurs de frappe**, un type de logiciel malveillant, sont couramment utilisés pour voler des renseignements personnels. Les enregistreurs de frappe sont des applications logicielles clandestines ou des dispositifs physiques reliés aux ordinateurs qui permettent de s'emparer de toute l'information qui a été saisie dans un appareil. Pour vous protéger des enregistreurs de frappe :

- Gardez toujours une dose de scepticisme par rapport à la sécurité d'un réseau ou d'un appareil inconnu. Lorsque vous utilisez gratuitement des ordinateurs ou des réseaux, présumez que toute information que vous y aurez saisie pourrait être vue par un tiers.

- Si vous vous servez d'un ordinateur partagé ou public, n'utilisez pas la fonction **Se souvenir de moi** lorsque vous ouvrez une session pour accéder à vos comptes. Quand vous avez terminé, **n'oubliez pas de vous déconnecter de vos comptes**.

## Le Bluetooth

Le Bluetooth permet d'établir la connexion entre deux appareils pour effectuer des appels en mains libres comme, par exemple, lorsque vous êtes au volant d'une voiture. L'utilisateur doit permettre à un autre appareil de se connecter au sien avant qu'un échange de données puisse se faire. Après l'établissement de la connexion, les deux appareils peuvent se transmettre des données librement et l'utilisateur n'a ensuite que peu de contrôle, voire même aucun, sur ces échanges. **Il est préférable de ne pas associer vos appareils à ceux des voitures de location; si vous le faites, n'oubliez pas de supprimer les données stockées et de supprimer votre appareil de la liste des appareils associés à ceux de la voiture de location**. Lorsque vous associez votre appareil à celui d'une voiture, vos renseignements personnels y sont stockés.

**Certains appareils permettent la connexion automatique, ce qui signifie que d'autres réseaux Bluetooth peuvent se connecter à votre appareil sans autorisation. Désactivez le Bluetooth** pendant vos déplacements pour empêcher toute tentative de communication non désirée. Supprimez les appareils perdus ou volés de votre liste d'appareils associés.

## Avant de partir

- Mettez à jour tous vos logiciels antivirus, VPN, etc.
- Installez les correctifs les plus récents des systèmes d'exploitation et des applications de vos appareils
- Assurez-vous de posséder tout le matériel et tous les logiciels nécessaires pour ne pas avoir à les acheter à l'étranger
- Activez le verrouillage de votre appareil par NIP, reconnaissance faciale, etc.
- Si possible, utilisez l'authentification à facteurs multiples sur vos appareils ainsi que pour vos applications et vos comptes afin d'ajouter une couche de sécurité supplémentaire
- Certains appareils peuvent être verrouillés à distance, localisés grâce à des programmes en nuage et offrent un logiciel antivol. Vérifiez si votre appareil possède ces options et assurez-vous d'être familier avec eux
- Avant de quitter la maison, sauvegardez les fichiers importants pour vous comme des photos ou documents dans un autre appareil ou sur un nuage comme iCloud, Google disque ou One Drive de Microsoft en cas de perte ou de vols de vos appareils

## En voyage

- Soyez conscient de votre entourage. Méfiez-vous des personnes qui vous épient et essaient de voir votre écran ou votre clavier
- Désactivez votre connexion Wi-Fi et Bluetooth quand vous n'avez pas besoin d'utiliser ces fonctions
- Rechargez votre téléphone au moyen de votre propre ordinateur ou d'un port d'attache directement branché au mur. Ne rechargez pas vos appareils au moyen d'autres ordinateurs ou d'autres appareils que vous ne pouvez contrôler, comme les ports d'attache dans les hôtels. Un appareil inconnu peut héberger des logiciels malveillants qui pourraient être transférés au vôtre en cas de connexion
- Ne connectez jamais un appareil inconnu à votre tablette électronique ou à votre ordinateur portatif. Tout ce qui se branche sur un port USB peut être un dispositif de stockage et risque de cacher un logiciel malveillant, **clé USB, lecteur MP3, téléphone intelligent, lecteur de disque dur externe**, etc.
- Ne branchez pas de supports d'enregistrement inconnus comme des CD, des DVD ou des disquettes, à votre ordinateur. Ils pourraient contenir des logiciels malveillants qui lisent automatiquement le contenu du support d'enregistrement ou de stockage. Votre ordinateur risque d'être infecté, même si vous ne cliquez pas sur le fichier malicieux

## Protection de vos appareils

Il est tout aussi important d'assurer la protection matérielle de vos appareils que de protéger vos données numériques. Les appareils électroniques sont très recherchés par les voleurs en raison de leur dimension relativement petite et du profit élevé que génère leur vente.

Un voleur peut transférer les données d'un appareil non surveillé dans un appareil de stockage secondaire et télécharger un logiciel malicieux auquel il accédera plus tard.

- Gardez toujours vos appareils sur vous. Ne laissez pas votre téléphone se charger dans une autre pièce ouverte pendant que vous allez prendre votre repas ailleurs et ne prêtez pas votre téléphone à un inconnu qui veut faire un appel
- Gardez sous clé tout bien de valeur ou tout appareil électronique que vous n'utilisez pas et qui renferme des données de nature délicate
- Ne laissez jamais un bien de valeur ou un appareil électronique qui renferme des données de nature délicate dans votre chambre d'hôtel. Si vous n'avez pas le choix, enlevez la pile si vous le pouvez, et la carte SIM, et apportez-les avec vous
- Tout comme vous ne porteriez pas de bijoux de valeur dans un endroit dangereux, ne faites pas étalage de vos coûteux appareils
- Ne cachez pas vos appareils dans une quelconque **bonne cachette** dénichée dans la chambre d'hôtel. Si c'est la première fois que vous voyez cette chambre, d'autres l'ont vue bien plus souvent avant vous
- Rangez vos appareils électroniques dans votre bagage de cabine pour ne pas les perdre ou les endommager durant le vol
- Éteignez vos appareils quand vous passez aux douanes et aux postes d'inspection

## Code QR

Le code QR peut mener à un site Web frauduleux où les fraudeurs auront accès aux renseignements personnels fournis. Également, les fraudeurs peuvent utiliser le code QR pour lancer une application de paiement frauduleuse ou pour diffuser un logiciel malveillant.

Dans un scénario type, les fraudeurs prétendent être une organisation légitime qui annonce une vente ou une offre. Lorsque vous balayez le code QR, vous serez amenés à saisir des renseignements personnels et financiers confidentiels, comme le numéro de votre carte de crédit. Ces renseignements seront volés.

### Conseils pour éviter cette arnaque

Voici des conseils pour déceler et éviter les arnaques liées au code QR :

- **Prenez votre temps.**
  Un code QR est un outil qui favorise une action rapide, donc parfait pour les publicitaires. Quant à nous tous, il est important d'évaluer d'abord la nécessité de balayer un code QR et la pertinence de révéler les renseignements demandés
- Une fois le code QR balayé, il faut vérifier l'adresse du site Web qui s'affiche en haut du navigateur.
  **Attention** si le domaine ou l'application ne correspond pas au nom de l'organisation qui a fourni le code QR, fermez la page du navigateur si le code QR ouvre un site suspect
- **Ne balayez pas un code QR s'il a l'air d'avoir été imprimé sur une étiquette collée ensuite sur un autre code QR**. Par exemple, sur un panneau dans la rue ou pour accéder à un menu dans un restaurant. En cas de doute, informez-vous auprès d'un employé ou trouvez le

site recherché par les moyens traditionnels. Les fraudeurs peuvent faire imprimer des codes QR malveillants et les coller sur de vraies annonces.

- Méfiez-vous et vérifiez attentivement l'adresse URL du site Web si l'on vous demande un mot de passe ou des justificatifs d'identité après avoir scanné un code QR. Lorsque vous savez que vous devrez entrer des informations personnelles, inscrivez plutôt l'adresse du site en question dans un navigateur Internet ou en effectuant une recherche par vous-même dans un moteur de recherche. **Évitez de faire un achat via un code QR.**

### Que faire si vous êtes victime de cette arnaque

Votre institution financière ne ménage aucun effort afin de protéger les renseignements personnels que vous lui confiez et de vous donner les outils pour faire de même. Si vous pensez avoir été victime d'une arnaque liée au code QR où vous avez donné vos renseignements financiers à un fraudeur, communiquez immédiatement avec votre institution financière.

## Les lois et les règlements d'autres pays

Vous devez respecter les lois sur la propriété intellectuelle, les renseignements numériques et les données cryptées des pays que vous visitez. **Ce qui est considéré comme légal au Canada ne l'est pas nécessairement ailleurs**. Par exemple :

- Vous accédez à votre boîte de courrier électronique dans un autre pays. Savez-vous si le gouvernement étranger vous surveille?
- Le roman osé que vous avez sauvegardé sur votre appareil est-il considéré comme du matériel pornographique dans le pays que vous visitez?
- La musique ou les films que vous avez téléchargés sur votre appareil pourraient-ils vous poser des problèmes par rapport aux lois locales en matière de propriété intellectuelle ou de ressources numériques?
- Certains pays peuvent-ils vous contraindre à leur fournir les données contenues sur votre appareil? Qu'arrive-t-il si les données sont la propriété intellectuelle d'une entreprise?

Les lois peuvent viser le matériel informatique et le support de stockage. Si vous ne connaissez pas les lois sur la propriété intellectuelle, les renseignements numériques et les données cryptées de votre pays de destination, communiquez avec l'ambassade ou la mission du pays au Canada avant votre départ à l'étranger.

Les agents des services frontaliers sont légalement autorisés à faire des fouilles et à confisquer les appareils de toute personne qui entre dans leur pays ou qui en sort. N'apportez pas dans un autre pays des données que vous ne voudriez pas perdre.

## Si vous avez besoin d'aide

Communiquez avec le bureau du gouvernement du Canada à l'étranger le plus près ou appelez notre **Centre de veille et d'intervention d'urgence** au +1 613 996 8885 (à frais virés si possible) dans les situations suivantes :

- Vous avez besoin d'aide à l'étranger à la suite d'une tentative de fraude
- Vous avez besoin d'aide pour rentrer au Canada
- Vous craignez de subir un traitement non équitable en vertu des lois du pays
- Vous doutez de la véracité d'une demande d'aide de l'une de vos connaissances qui se dit en difficulté à l'étranger.

Le gouvernement du Canada n'interfère pas dans les affaires juridiques d'ordre privé et n'exerce aucune influence sur les procédures judiciaires d'un autre pays. Toutefois, les agents consulaires peuvent vous fournir une liste d'avocats dans le pays concerné.