# DISPOSITIFS MOBILES ET VOYAGES D'AFFAIRES

MAI 2021

ITSAP.00.087 V2

Si vous êtes un voyageur d'affaires, vous devez connaître les risques que représente l'utilisation de vos dispositifs mobiles lors de vos déplacements. Un dispositif compromis peut fournir un accès non autorisé au réseau de votre organisation, ce qui menace la sécurité de votre information et celle de votre organisation. Le présent document contient de l'information sur les menaces et les risques qui pèsent sur vos dispositifs mobiles lors de vos déplacements et donne les pratiques à adopter pour éviter que les risques se matérialisent.

## MENACES ET RISQUES

Un dispositif mobile est une cible de choix pour les voleurs. Un auteur de menace pourrait accéder à l'information qu'il contient et utiliser le dispositif ou l'information à des fins malveillantes. Chacun devrait prendre des mesures pour protéger ses dispositifs mobiles lors de déplacements. Toutefois, les auteurs de menace sont plus susceptibles de s'en prendre à des personnes qui occupent des postes supérieurs ou qui traitent des renseignements précieux.

Ils peuvent recourir à des dispositifs commerciaux d'espionnage électronique (p. ex. des intercepteurs d'IMSI) aux fins suivantes :

- repérer et cibler des dispositifs mobiles;
- installer du code malveillant sur un dispositif;
- utiliser les connexions réseau d'un dispositif (p. ex. Wi-Fi, Bluetooth);
- accéder au dispositif et suivre vos déplacements;
- activer le microphone ou la caméra du dispositif;
- intercepter vos communications.

Dans certains pays, les centres d'affaires et les réseaux téléphoniques des hôtels sont surveillés, et les chambres d'hôtel sont parfois fouillées. Il faut donc supposer que les bureaux, les hôtels, les cafés Internet et les autres lieux publics ne sont pas privés.

## AVANT LE VOYAGE

Avant votre voyage, prenez les mesures suivantes :

- désactivez certaines fonctions, comme la connexion Bluetooth et les écouteurs sans fil;
- effacez les données non nécessaires;
- limitez-vous aux dispositifs nécessaires pour le travail;
- changez vos mots et vos phrases de passe;
- sauvegardez vos données.

SÉRIE SENSIBILISATION



No de cat. D97-1/00-087-2021F-PDF
ISBN 978-0-660-38742-0

## PENDANT LE VOYAGE

Pendant votre voyage, prenez les mesures suivantes pour vous protéger :

- gardez votre téléphone sur vous en tout temps. Si vous devez laisser votre dispositif sans surveillance, enlevez la batterie, si possible, ainsi que la carte SIM et gardez-les avec vous;
- éteignez vos dispositifs lorsque vous passez aux douanes ou à d'autres postes d'inspection;
- videz la corbeille et les fichiers **récents** après chaque utilisation. Nettoyez votre navigateur après chaque utilisation (effacez l'historique, la mémoire cache, les témoins, les URL et les fichiers Internet temporaires);
- soyez attentif à ce qui se passe autour de vous et méfiez-vous des personnes qui pourraient essayer de regarder votre écran ou votre clavier à votre insu;
- **n'activez jamais** la fonction Se souvenir de moi sur les sites Web. Saisissez vos justificatifs à chaque fois.
- **évitez** les réseaux Wi-Fi inconnus, non protégés ou publics et les bornes de chargement;
- respectez la classification de sécurité du dispositif, c'est-à-dire **ne l'utilisez pas** pour enregistrer ou communiquer de l'information d'une classification supérieure;
- gardez un œil sur vos câbles, vos chargeurs et vos périphériques. Les auteurs de menace peuvent programmer les microcontrôleurs contenus dans les câbles modernes pour compromettre votre dispositif;
- ignorez le contenu provenant de sources inconnues, c'est-à-dire n'ouvrez **pas** les courriels et les pièces jointes et ne cliquez **pas** sur les liens;
- n'utilisez pas d'autres chargeurs que le vôtre;
- communiquez immédiatement avec votre service de sécurité des TI si votre dispositif est volé ou égaré ou si vous avez des préoccupations de sécurité.

## APRÈS LE VOYAGE

À votre retour de voyage, prenez les mesures suivantes :

- signalez les incidents suspects à votre service de sécurité des TI;
- changez les mots et les phrases de passe ainsi que les NIP des dispositifs et des comptes que vous avez utilisés à l'étranger.

## VOYAGE À HAUT RISQUE

Le voyage peut être considéré à haut risque si le voyageur est bien connu ou d'une grande notoriété (p. ex. chef de la direction), si l'événement ou la conférence a un grand retentissement (p. ex. Forum économique mondial) ou si la destination représente un risque élevé (selon Affaires mondiales Canada). Si vous ignorez quel est le degré de risque lié au voyage, communiquez avec votre service de sécurité des TI.

Les mesures spéciales suivantes s'imposent lors des voyages à haut risque.

- N'utilisez pas vos dispositifs habituels de travail ou personnels. Si vous devez apporter un dispositif personnel, désactivez les fonctions de Bluetooth, de Wi-Fi et de partage de localisation et connectez-vous à un réseau privé virtuel.
- Demandez à votre service de TI s'il peut vous fournir un dispositif de voyage, un dispositif « jetable » ou un compte temporaire réservé aux milieux à haut risque où la menace est élevée.
- Supposez que toutes les communications transmises par des fournisseurs publics risquent d'être interceptées. Avant votre voyage, chiffrez toute l'information de nature délicate contenue sur vos dispositifs mobiles.
- Supposez que les connexions Internet, les photocopieurs et les télécopieurs des hôtels sont surveillés. Ne les utilisez que pour traiter de l'information de nature non-délicate.
- Signalez à votre service de sécurité des TI tout problème de rendement du dispositif ou toute préoccupation de sécurité.

## AUTRES PUBLICATIONS

Le Centre pour la cybersécurité a rédigé d'autres publications qui aideront les voyageurs d'affaires à utiliser leurs dispositifs mobiles de façon sécuritaire pendant leurs déplacements. En voici quelques-unes.

- *Utiliser son dispositif mobile en toute sécurité (ITSAP.00.001)*
- *Sécurisation de l'entreprise et des technologies mobiles (ITSM.80.001)*
- *Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032)*
- *Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030)*
- *Conseils de sécurité sur les gestionnaires de mots de passe (ITSAP.30.025)*
- *Conseils de sécurité pour les dispositifs périphériques (ITSAP.70.015)*

Vous avez des questions ou vous avez besoin d'aide? Vous voulez en savoir plus sur les questions de cybersécurité? Consultez le site Web du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) à **cyber.gc.ca**.