DISPOSITIFS MOBILES ET VOYAGES D'AFFAIRES

OCTOBRE 2018 ITSAP.00.087

Quels sont les risques et les menaces?

Lorsque vous êtes en voyage d'affaires, vous devez bien évaluer les risques potentiels liés à l'utilisation d'un dispositif mobile. Un dispositif compromis peut fournir un accès non autorisé au réseau de votre organisme, ce qui menace à la fois la sécurité de votre information et de celle de votre organisme. Veuillez tenir compte des observations importantes suivantes :

- Les dispositifs mobiles des cadres supérieurs et des personnes qui travaillent avec de l'information importante risquent plus d'être ciblés que les dispositifs des autres employés.
- Les auteurs de menaces utilisent des technologies commerciales (p. ex. capteurs IMSI [identité internationale d'abonné mobile]) qui leur permettent de prendre les mesures suivantes :
  - trouver et cibler un dispositif mobile;
  - télécharger un programme malveillant sur un dispositif;
  - utiliser les connexions réseau d'un dispositif (p. ex. Wi-Fi, Bluetooth);
  - se servir du dispositif pour infecter d'autres réseaux de votre organisme;
  - accéder à un dispositif afin d'en déterminer l'emplacement;
  - activer le micro ou la caméra d'un dispositif;
  - intercepter les communications envoyées par voie électronique.

- Dans certains pays, les centres d'affaires et les réseaux téléphoniques des hôtels sont surveillés, et les chambres d'hôtel sont parfois fouillées. Les utilisateurs ne doivent avoir aucune attente de confidentialité dans les bureaux, les hôtels, les cafés Internet et les autres endroits publics.
- Les dispositifs mobiles sont des cibles de choix pour les voleurs. Si un voleur s'en empare, il pourrait accéder à l'information qu'ils contiennent, puis l'utiliser à des fins malveillantes.

Pratiques exemplaires – Avant le voyage

- Désactivez les fonctions semblables à Bluetooth et les capacités de casque d'écoute sans fil.
- Supprimez l'information inutile de votre dispositif.
- Apportez seulement les dispositifs dont vous aurez besoin pour votre travail.
- Modifiez vos mots de passe avant de partir.
- Sauvegardez vos données importantes.

Vous voulez en savoir plus?

Veuillez lire les publications suivantes :

- Sécurité des dispositifs mobiles – Sécuriser le GC (ITSE.80.001);
- Utiliser son dispositif mobile en toute sécurité (ITSAP.00.001);
- Sécurisation de l'entreprise et des technologies mobiles (ITSM.80.001);
- Technologies mobiles pour les voyages internationaux - Conseils pour les gestionnaires en sécurité des TI du gouvernement du Canada (ITSB-88).

SÉRIE SENSIBILISATION

Pratiques exemplaires – Pendant le voyage

- Gardez votre dispositif sur vous en tout temps. Si vous devez le laisser sans surveillance, retirez la pile et, dans la mesure du possible, la carte SIM, puis gardez-les sur vous.
- Éteignez vos dispositifs lorsque vous passez la douane ou d'autres postes d'inspection.
- Modifiez régulièrement les mots de passe de vos dispositifs mobiles et des applications et sites Web que vous utilisez souvent.
- Videz la corbeille et les dossiers « récents » après chaque usage. Nettoyez votre navigateur après chaque utilisation (c.-à-d. effacez les fichiers d'historique, la mémoire cache, les témoins, les URL et les fichiers Internet temporaires).
- Soyez conscient de votre environnement immédiat et des personnes qui pourraient voir votre écran ou votre clavier.
- N'utilisez pas la fonction « se souvenir de moi » des sites Web; tapez votre mot de passe chaque fois que vous ouvrez une session.
- N'utilisez pas de réseaux Wi-Fi publics.
- N'enregistrez et ne communiquez pas d'information dont la classification est supérieure à celle du dispositif.
- N'utilisez pas la messagerie NIP à NIP pour échanger de l'information sensible, car il n'existe aucun paramètre de sécurité pour protéger l'information transmise.
- N'ouvrez pas de courriels ou de pièces jointes, et ne cliquez pas sur des liens provenant de sources inconnues.
- Consultez votre division de la sécurité des TI dans les plus brefs délais pour obtenir de l'aide en cas de vol, de perte ou de préoccupations de sécurité.

Pratiques exemplaires – Après le voyage

- Si le dispositif a été hors de votre possession pour une quelconque raison ou si vous avez des doutes quant à la sécurité du dispositif, signalez-les à la division de la sécurité des TI de votre organisme.
- Modifiez les mots de passe de vos dispositifs et de tout service en ligne auquel vous vous êtes connecté pendant votre voyage à l'étranger.

Voyages à risques élevés

On considère qu'un voyage comporte des risques élevés en fonction des facteurs suivants : identité du voyageur (p. ex. un directeur général), événement spécial (p. ex. le forum économique mondial) ou région à haut risque (selon Affaires mondiales Canada). En cas de doute sur le niveau de risque, communiquez avec la direction de la sécurité des TI de votre ministère.

Si vous entreprenez un voyage à risques élevés, vous devez tenir compte des considérations particulières suivantes :

- N'utilisez pas vos dispositifs personnels ni ceux que vous utilisez régulièrement au travail. Si votre organisme possède des dispositifs réservés aux voyages, demandez à votre service des TI de vous en fournir un à cette fin. Si vous utilisez un dispositif personnel, désactivez les fonctionnalités Bluetooth, Wi-Fi et liées au partage de localisation, et ayez recours à un RPV pour une sécurité accrue.
- Tenez pour acquis que toutes les communications transmises par des fournisseurs publics risquent d'être interceptées et chiffrez toute l'information sensible sur vos dispositifs mobiles avant le voyage.
- Tenez pour acquis que les connexions Internet, les photocopieurs et les télécopieurs des hôtels sont surveillés et ne sont adéquats que pour la transmission d'information non sensible.
- Signalez tout problème de performance du dispositif observé pendant le voyage ou toute autre préoccupation de sécurité connexe à la division de la sécurité des TI de votre organisme.

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