CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Dispositifs mobiles et voyages d'affaires

Octobre 2024

ITSAP.00.087

À titre d'employée ou employé, vous avez accès à l'information importante et sensible de votre organisation. Vous êtes responsable de protéger cette information, même lorsque vous voyagez. Si vous êtes en voyage d'affaires, vous devez connaître les risques que représente l'utilisation d'un dispositif mobile dans un nouvel emplacement. Un dispositif compromis pourrait permettre un accès non autorisé au réseau de votre organisation et à ses renseignements. Avant votre voyage, tenez compte des points qui suivent.

- Les auteures et auteurs de menace pourraient repérer et cibler des dispositifs mobiles pour :
  - installer un code malveillant sur le dispositif afin d'accéder à l'information et d'infecter les autres réseaux de votre organisation;
  - utiliser les connexions réseau du dispositif, p. ex. Wi-Fi et Bluetooth;
  - activer le microphone ou la caméra du dispositif;
  - suivre vos déplacements;
  - intercepter les communications transmises 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.
  - Il faut donc supposer que les bureaux, les hôtels, les cafés Internet et les autres lieux publics ne sont pas privés.

Voyages à haut risque

Les voyages peuvent être considérés comme à haut risque lorsque les variables suivantes sont prises en compte :

- l'identité de l'employée ou employé en voyage (p. ex. directrice générale ou directeur général);
- la tenue d'événements spéciaux (p. ex. Forum économique mondial);
- les emplacements à risque élevé selon Affaires mondiales Canada.

Si vous ignorez le degré de risque lié au voyage, communiquez avec le service de sécurité des TI de votre organisation.

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

- Si votre organisation dispose d'un inventaire de dispositifs de voyage, communiquez avec le service des TI pour vous procurer un tel dispositif.
  - 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.
- Supposez que toutes les communications transmises par des fournisseurs publics risquent d'être interceptées. Avant votre voyage, chiffrez toute l'information sensible contenue dans vos dispositifs mobiles.
- Signalez à votre service de sécurité des TI tout problème de rendement du dispositif ou toute préoccupation en matière de sécurité.

SÉRIE SENSIBILISATION

No de cat. D97-1/00-087-2024F-PDF
978-0-660-72984-8

Guide à l'intention des employées et employés en voyage d'affaires

Avant le voyage

- **Protéger ses biens.** Sauvegardez vos renseignements et mettez à jour les logiciels de votre dispositif pour en accroître les capacités de défense.
- **Voyager sous le couvert de l'anonymat.** Désactivez les fonctions de localisation, de Bluetooth et d'autoconnexion de votre dispositif.
- **Voyager léger.** Limitez-vous aux dispositifs dont vous avez besoin, et supprimez les données inutiles.
- **Verrouiller ses renseignements.** Activez et mettez à jour les paramètres de phrase de passe et de mot de passe, et activez l'authentification multifacteur.

Pendant le voyage

- **Garder ses dispositifs en sa possession en tout temps**. Si vous devez laisser un dispositif sans surveillance, enlevez la batterie et la carte SIM si possible, et gardez-les avec vous. Éteignez vos dispositifs lorsque vous passez aux douanes ou à d'autres postes d'inspection.
- **Avoir connaissance de son environnement.** Méfiez-vous des personnes qui pourraient essayer de regarder votre écran ou votre clavier à votre insu. Éteignez vos dispositifs lorsque vous passez aux douanes ou à d'autres postes d'inspection.
- **Désactiver la fonction « Se souvenir de moi » sur les sites Web.** Saisissez vos justificatifs chaque fois que vous ouvrez une session, pour éviter que vos mots de passe soient enregistrés.
- **Se connecter de façon sécuritaire.** Dans la mesure du possible, accédez à Internet en utilisant les données de votre forfait cellulaire, et évitez de vous connecter à des réseaux Wi-Fi inconnus, non sécurisés ou publics pour accéder à de l'information sensible.
- **Communiquer en toute sécurité.** N'enregistrez ou ne communiquez aucune information dont la classification est supérieure à celle du dispositif. N'envoyez pas de messages NIP à NIP pour transmettre de l'information sensible, puisque cette information n'est pas protégée par les paramètres de sécurité.

Après le voyage

- **Signaler les préoccupations soupçonnées en matière de sécurité** au service des TI de votre organisation.
- **Modifier ses justificatifs.** Changez les mots et les phrases de passe ainsi que les NIP des dispositifs et des comptes que vous avez utilisés à l'étranger.
- **Utiliser des logiciels antivirus.** Ces logiciels vous permettent d'analyser les dispositifs pour détecter les activités malveillantes avant de vous connecter à vos réseaux à domicile et au travail.

Pour en savoir plus

- Utiliser son dispositif mobile en toute sécurité (ITSAP.00.001)
- Conseils sur les appareils mobiles à l'intention des voyageurs connus du public (ITSAP.00.088)
- Sécurité des appareils lors des déplacements et du télétravail à l'étranger (ITSAP.00.188)
- Sécurisation de l'entreprise et des technologies mobiles (ITSM.80.001)
- Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030)

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**.