Conseils sur les appareils mobiles à l'intention des voyageurs connus du public

Si vous occupez un poste très en vue, notamment à titre de politicien ou comme membre de la haute direction, vous devez protéger vos appareils mobiles lorsque vous voyagez. Les appareils mobiles contiennent des informations sensibles, ce qui en font une cible alléchante pour les auteurs de cybermenace. S'ils réussissent à compromettre votre appareil ou l'information qui s'y trouve, ces auteurs de menace pourraient s'en servir contre vous ou l'organisation que vous représentez. Nous abordons ci-dessous des menaces courantes et les mesures de sécurité à prendre avant, durant et après votre voyage afin de protéger vos appareils mobiles.

MENACES

Les auteurs de menace emploient différentes techniques pour obtenir l'accès à des appareils et à l'information sensible. Voici quelques exemples de méthodes d'attaques :

- **Espionnage par-dessus l'épaule :** Vol d'information sensible consistant à épier l'appareil en personne.
- **Hameçonnage :** Envoi de courriels ou de textos frauduleux comportant des fichiers ou des liens malveillants ou demandant des renseignements personnels.
- **Usurpation de réseau :** Le fait de se faire passer pour un autre réseau.
- **Brouillage des signaux :** Interférence, perturbation ou blocage des signaux et des services de communication.
- **Attaque par interception :** Exploitation de vulnérabilités dans le but d'intercepter des communications.
- **Rançongiciel :** Utilisation de logiciels malveillants pour chiffrer des fichiers ou verrouiller l'accès aux systèmes et aux appareils jusqu'à ce que la victime verse une somme d'argent.

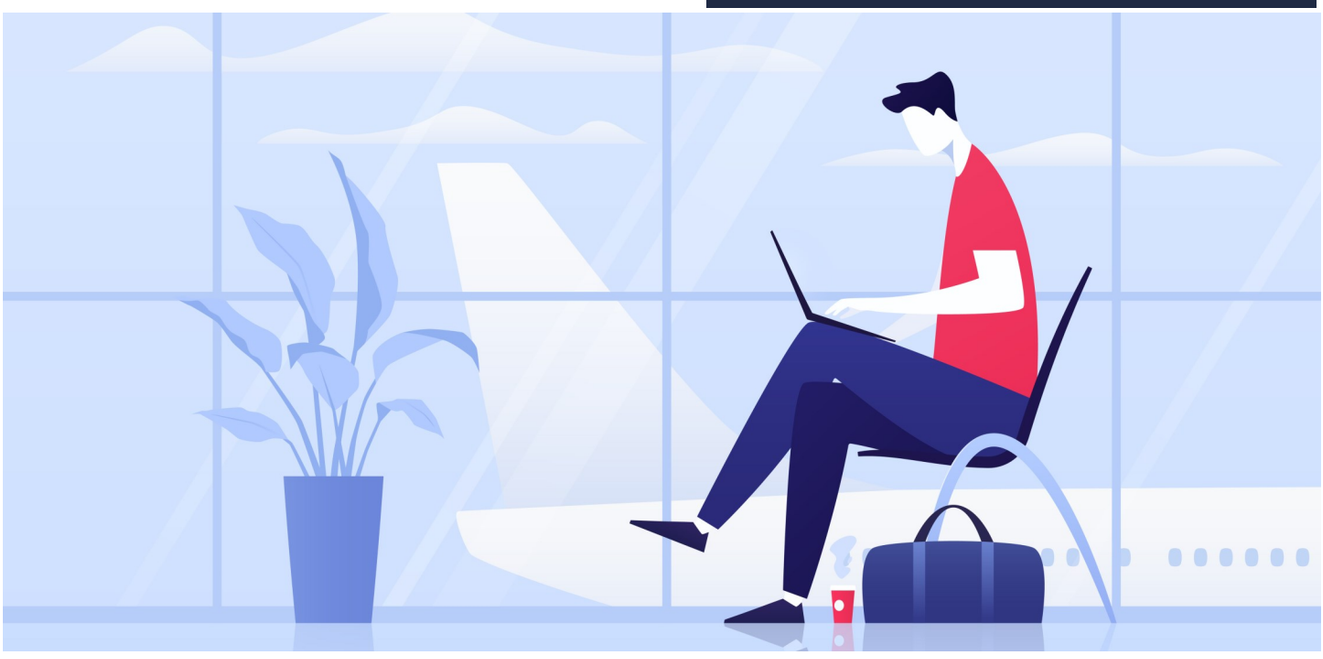
Pour en savoir plus sur ces menaces, consultez les documents suivants : *Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage (ITSAP.00.100)*, *Utiliser le Wi-Fi sans compromettre la sécurité de votre organisation (ITSAP.80.009)* et *Rançongiciels : comment les prévenir et s'en remettre (ITSAP.00.099)*.

RISQUES

Le voyage peut comporter des **risques élevés** si le voyageur est bien connu ou d'une grande notoriété, tout particulièrement lorsqu'il se rend à un événement ou à une conférence à grand retentissement (p. ex. le Forum économique mondial) ou si la destination représente un risque élevé selon Affaires mondiales Canada.

Lors de vos déplacements, des auteurs de menace de services de renseignement étrangers, de groupes criminels ou d'organisations concurrentes pourraient tenter de compromettre vos appareils. Dans le cadre de vos fonctions, vous êtes sans doute appelé à traiter de l'information très sensible. Les auteurs de menace ciblent des données techniques, politiques, stratégiques, militaires, financières et personnelles. S'ils réussissaient à compromettre votre appareil ou l'information qui s'y trouve, ils pourraient s'en servir contre vous ou l'organisation que vous représentez.

Votre organisation devrait prendre en considération les risques associés aux voyages internationaux et déterminer son niveau de tolérance à l'égard de tels risques. Vous et votre organisation devriez mettre en œuvre des mesures pour atténuer les risques cernés.



Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

 No de cat.D96-74/2021F-PDF ISBN 978-0-660-40284-0

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

NON CLASSIFIÉ

AVANT DE PARTIR

- Utilisez des appareils temporaires (« jetables ») appartenant à votre organisation, si possible.
- Activez l'authentification multifacteur pour l'accès à vos appareils et à vos comptes.
- Installez un pare-feu et des solutions antivirus et de protection contre les logiciels espions.
- Exécutez les mises à jour et installez les correctifs sur les systèmes d'exploitation et les applications.
- Enregistrez des sauvegardes afin de pouvoir restaurer au besoin les appareils à votre retour.
- Effacez les données et les applications non nécessaires des appareils.
- Installez un réseau privé virtuel (RPV) sur vos appareils afin d'assurer le transfert sécurisé des données.
- Configurez un bac à sable afin d'accéder en toute sécurité aux données organisationnelles à l'écart des autres applications de l'appareil.
- Limitez les privilèges administratifs pour sécuriser les paramètres des logiciels et restreindre le téléchargement d'applications.
- Configurez les appareils de manière à ce que l'antivirus s'exécute dès l'installation de périphériques de stockage (comme les lecteurs USB).
- Mettez en œuvre des paramètres de sécurité réseau appropriés pour les appareils (p. ex. restreindre la connectivité Wi-Fi aux réseaux sécurisés, désactiver la détection du partage de connexion).
- Configurez les appareils mobiles de manière à désactiver l'accès aux connexions externes (p. ex. Wi-Fi et Bluetooth) au moment d'accéder au réseau sécurisé de l'organisation (c'est-à-dire le réseau interne).
- Fermez vos appareils avant de passer aux douanes et à la sécurité.
  - Informez les services des TI si vos appareils ont été inspectés par le personnel de sécurité.

PENDANT VOTRE VOYAGE

- Chiffrez l'information sensible.
- Évitez d'utiliser vos comptes personnels dans la mesure du possible.
  - Si nécessaire, sécurisez vos appareils au moyen de l'authentification multifacteur, informez les services des TI et changez vos mots de passe à votre retour.
- Désactivez les services Bluetooth et Wi-Fi.
- Supposez que les communications transmises sur les réseaux de fournisseurs publics pourraient être interceptées.
- Évitez d'utiliser les réseaux de l'hôtel et les services Wi-Fi et Bluetooth publics.
- Utilisez le réseau et le RPV de votre organisation pour accéder à l'information sensible et en envoyer.
- Assurez-vous de maintenir les chargeurs, les câbles et les périphériques sous votre contrôle en tout temps.
- Évitez d'utiliser les supports de stockage (p. ex. clés USB) et les périphériques qui vous sont remis par des sources externes.
- Gardez vos appareils sur vous et soyez attentif à ce qui se passe autour de vous en tout temps.

À VOTRE RETOUR

Surveillez vos appareils pour détecter tout comportement inhabituel. Les événements inhabituels, comme la lenteur de votre appareil ou des fenêtres surgissantes qui disparaissent avant que vous ayez le temps de les lire, doivent être signalés à votre équipe de sécurité des TI.

Comparez l'image de votre appareil à celle d'une sauvegarde pour détecter les signes d'activités malveillantes.

Advenant la compromission de votre appareil, il est recommandé de procéder à une enquête de criminalistique et d'effectuer la réinitialisation aux paramètres d'usine afin de restaurer l'appareil.

Employez une sauvegarde sûre pour restaurer l'appareil avant de continuer de l'utiliser.

Si vous remarquez des activités suspectes sur votre appareil durant ou après votre voyage, suivez les mesures de sécurité ci-dessous :

1. Déconnectez votre appareil d'Internet et de tout autre appareil.
2. Utilisez un autre appareil pour communiquer avec votre fournisseur de services et votre équipe des TI pour entamer les processus de gestion des incidents appropriés.
3. Laissez votre appareil hors connexion pendant la durée de votre voyage.
4. Examinez l'appareil dans l'environnement sécurisé de votre organisation à votre retour.
5. Éliminez la menace de l'appareil et utilisez la sauvegarde sûre la plus récente pour restaurer ce dernier.
6. Remplacez la carte SIM de l'appareil.

POUR EN SAVOIR PLUS

Consultez notre site Web (**cyber.gc.ca**) pour obtenir notre liste de publications, notamment :

- *Dispositifs mobiles et voyages d'affaires (ITSAP.00.087)*
- *Considérations de sécurité pour les modèles de déploiement de dispositifs mobiles (ITSAP.70.002)*
- *Application des mises à jour sur les dispositifs (ITSAP.10.096)*
- *Utiliser le chiffrement pour assurer la sécurité des données sensibles (ITSAP.40.016)*
- *Les réseaux privés virtuels (ITSAP.80.101)*

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada