CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Utiliser son dispositif mobile en toute sécurité

Octobre 2024

ITSAP.00.001

Votre dispositif mobile vous offre une simple façon de travailler n'importe où, n'importe quand. Bien qu'il s'avère bien utile au travail, il constitue une menace pour l'information et les réseaux de votre organisation, s'ils sont compromis.

Le contexte de menace visant les applications mobiles

Le contexte de cybermenace évolue très rapidement. Les menaces changent constamment. De plus, les auteures et auteurs de menace peuvent :

- utiliser de nouvelles tactiques et techniques changeantes;
- accéder à des outils de piratage informatique conviviaux à la disposition du grand public.

Les dispositifs mobiles sont principalement visés par des auteures et auteurs de menace qui veulent recueillir de l'information à votre sujet ou au sujet de votre organisation. Un dispositif compromis pourrait permettre à ces personnes d'accéder au réseau de votre organisation et d'obtenir ses renseignements.

Le saviez-vous?

Il existe des technologies qui permettent aux pirates d'activer et d'utiliser votre dispositif à votre insu.

Cibles

Les organisations et les particuliers du Canada sont les principales cibles des auteures et auteurs de menace en raison de la richesse et des ressources du pays, et des bonnes relations qu'il entretient avec les autres nations. Les employées et employés, peu importe leur niveau, peuvent être des cibles. Cela dit, les auteures et auteurs de menace visent souvent :

- les cadres de direction et leurs adjointes et adjoints;
- le personnel des services de soutien et les administratrices et administrateurs de système;
- les personnes ayant accès à de l'information sensible;
- les personnes disposant d'un accès à distance;
- les personnes qui traitent avec les membres du public.

Méthodes de ciblage

Les auteures et auteurs de menace qui cherchent à obtenir de l'information sur les membres du personnel, les projets et les systèmes utilisent de nombreuses méthodes différentes, dont :

- l'accès et l'utilisation à distance de votre dispositif;
- le trafiquage matériel de votre dispositif;
- l'utilisation de la fonction de localisation de votre dispositif mobile pour savoir où vous êtes;
- l'envoi de messages par texto, par courriel ou par l'entremise des médias sociaux et qui contiennent des liens malveillants.

N'oubliez pas que n'importe qui peut être une cible, vous compris.

Il y a de nombreuses façons d'avoir accès à de l'information stockée sur un dispositif mobile ou transmise par un tel dispositif. Portez toujours attention à votre environnement lorsque vous utilisez votre dispositif et faites preuve de vigilance lorsque vous utilisez Internet et téléchargez des applications.

SÉRIE SENSIBILISATION

No de cat. D97-1/00-001-2024F-PDF
ISBN 978-0-660-72986-2

Mesures à prendre pour protéger vos dispositifs mobiles

Vous pouvez réduire considérablement le risque de communiquer de l'information sensible ou des renseignements personnels en prenant quelques mesures simples :

- Établir une connexion par réseau privé virtuel dans toute la mesure du possible.
- Utiliser un NIP ou une phrase de passe pour protéger votre dispositif.
- Désactiver certaines fonctions du dispositif, comme le système GPS ou les technologies Bluetooth ou Wi-Fi, lorsqu'on ne s'en sert pas.
- Éviter de se connecter à des réseaux Wi-Fi inconnus, non sécurisés ou publics.
- Supprimer toute l'information stockée sur un dispositif avant de s'en défaire.
- Éviter d'ouvrir des fichiers, de cliquer sur des liens ou de composer des numéros contenus dans des messages texte ou des courriels non sollicités.
- Mettre à jour les logiciels, ainsi que les systèmes d'exploitation et les applications.
- Lire les politiques de protection des renseignements personnels et les évaluations laissées par les utilisatrices et utilisateurs des applications avant de procéder au téléchargement afin de s'assurer qu'il s'agit d'une source fiable.
- Utiliser des phrases ou des mots de passe uniques et complexes, et activer la fonction d'authentification multifacteur (AMF), si elle est accessible.
- Éviter d'utiliser des gestionnaires de mots de passe gratuits qui ne relèvent pas du système d'exploitation ou du navigateur utilisé.
- Limiter le recours à la fonction « Souvenez-vous de moi » des sites Web et des applications mobiles – si la fonction d'AMF n'est pas accessible, taper son nom d'utilisateur et sa phrase ou son mot de passe pour ouvrir une session. Procéder ainsi pour les comptes importants.
- Utiliser des fonctions de chiffrement pour sécuriser les données personnelles et les messages de nature délicate.
- Toujours surveiller ses dispositifs, ainsi que les câbles, les chargeurs et les périphériques.

Facteurs à considérer lors de voyager avec votre dispositif

Lorsque vous voyagez à l'étranger, il conviendrait de bien évaluer les risques liés à l'utilisation de dispositifs mobiles. Soyez au fait des politiques de votre organisation concernant les voyages avec des dispositifs mobiles appartenant à cette dernière et prenez note de ce qui suit :

- Renforcer la sécurité de l'information stockée sur votre dispositif en vous conformant à ces politiques avant, pendant et après votre voyage.
- Dans certains pays, les centres d'affaires et les réseaux téléphoniques des hôtels sont surveillés, et les chambres d'hôtel sont même parfois fouillées.
- Les dispositifs mobiles des cadres de direction et des personnes qui travaillent avec de l'information importante risquent davantage d'être ciblés que les dispositifs mobiles des autres membres du personnel.
- Les dispositifs mobiles sont des cibles de choix; le vol de ces dispositifs pourrait permettre d'accéder à l'information qu'ils contiennent et de l'utiliser à des fins malveillantes.

Consultez la page Dispositifs mobiles et voyages d'affaires (ITSAP.00.087) pour en savoir plus sur les voyages avec votre dispositif.

Pour en savoir plus

- La cybersécurité à la maison et au bureau – Sécuriser vos dispositifs, vos ordinateurs et vos réseaux (ITSAP.00.007)
- 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 cybersécurité pour le télétravail (ITSAP.10.116)
- Conseils de sécurité pour les dispositifs périphériques (ITSAP.70.015)
- Application des mises à jour sur les dispositifs (ITSAP.10.096)

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**.