UTILISER SON DISPOSITIF MOBILE EN TOUTE SÉCURITÉ

DECEMBRE 2020 ITSAP.00.001

Votre dispositif mobile vous offre une façon commode et souple de travailler n'importe où, n'importe quand. Les dispositifs mobiles jouent un rôle essentiel dans les activités quotidiennes des organisations et des organismes, mais leur utilisation représente aussi une menace pour l'information et les réseaux.

Comme ils peuvent contenir d'énormes quantités de données sensibles et de renseignements personnels, les dispositifs mobiles sont une cible alléchante pour les auteurs de menace qui cherchent à recueillir de l'information. Un dispositif compromis peut fournir un accès non autorisé au réseau de votre organisation, ce qui menace à la fois la sécurité de votre information et de celle de votre organisation.

Et il ne faut pas oublier que le Canada est une cible attrayante pour les auteurs de cybermenace en raison de sa richesse, de ses ressources et de ses relations diplomatiques.

EN QUOI CONSISTE LE CONTEXTE DE CYBERMENACE DES DISPOSITIFS MOBILES?

Le contexte de cybermenace d'aujourd'hui est très différent d'il y a à peine cinq ans. Les menaces évoluent constamment et ont tendance à avoir une longueur d'avance sur les coupe-feux, les antimaliciels et les antivirus. Pour se défendre, il faut tenir compte de ce qui suit :

- les auteurs de menace s'adaptent rapidement, et les défenses doivent en faire de même;
- les outils de piratage informatique sont conviviaux et offerts gratuitement au grand public;
- les dispositifs mobiles sont de plus en plus ciblés par des auteurs de cybermenace expérimentés;
- les dispositifs mobiles sont des ressources précieuses pour les pirates, puisqu'ils peuvent contenir de l'information sensible.

QUI SONT LES CIBLES?

Bien que tous les employés, peu importe leur niveau, puissent être ciblés, les personnes ci-dessous sont souvent la cible des auteurs de menace :

- les cadres supérieurs et leurs adjoints;
- le personnel des services de soutien et les administrateurs de systèmes;
- les utilisateurs ayant accès à de l'information sensible;
- les utilisateurs disposant d'un accès à distance;
- les utilisateurs qui doivent interagir avec le public dans le cadre de leurs fonctions.

DE QUELLE MANIÈRE LES GENS, LES PROJETS ET LES SYSTÈMES SONT-ILS CIBLÉS?

Les auteurs de menace qui cherchent à obtenir de l'information sur les employés, 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 géolocalisation de votre dispositif mobile pour déterminer votre emplacement;
- l'envoi de messages texte qui comprennent des liens malveillants.

Le saviez-vous?

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

SÉRIE SENSIBILISATION

QUE PUIS-JE FAIRE?

Les employés peuvent réduire grandement le risque d'exposer de l'information sensible ou des renseignements personnels en prenant quelques mesures simples, dont les suivantes :

- utiliser un NIP ou un mot de passe pour accéder au dispositif;
- désactiver les fonctions non utilisées comme les capacités GPS, Bluetooth ou Wi-Fi;
- éviter de se connecter à des réseaux Wi-Fi inconnus ou non sécurisés;
- supprimer toute l'information stockée dans un dispositif avant de s'en débarrasser;
- 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;
- garder les logiciels à jour, y compris les systèmes d'exploitation et les applications;
- lire les politiques de protection des renseignements personnels et les évaluations laissées par les utilisateurs des applications avant de procéder au téléchargement afin de s'assurer qu'il s'agit d'une source fiable;
- ne pas utiliser la fonction « se souvenir de moi » des sites Web et des applications mobiles – toujours taper son mot de passe;
- chiffrer les données et les messages personnels ou sensibles;
- comprendre les risques, surveiller son dispositif (y compris les câbles, les chargeurs et les périphériques) et demeurer cons cient de la situation.

SUIS-JE UNE CIBLE?

Il y a de nombreuses façons d'avoir accès à de l'information stockée sur un dispositif mobile ou transmise par un tel dispositif. Soyez conscient de votre environnement lorsque vous utilisez votre dispositif et soyez constamment vigilant lorsque vous utilisez Internet et téléchargez des applications. Vous devez également vous rappeler que vous êtes bien une cible.

VOUS VOYAGEZ AVEC VOTRE DISPOSITIF?

Lorsque vous voyagez à l'étranger, vous devriez bien évaluer les risques potentiels liés à l'utilisation de vos dispositifs mobiles. Soyez au fait des politiques de votre organisation sur l'utilisation des dispositifs mobiles pendant les voyages, et tenez compte de ce qui suit :

- il faut prendre des mesures **avant**, **pendant** et **après** le voyage afin d'accroître la sécurité de l'information stockée sur les dispositifs mobiles;
- 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 supérieurs ou des personnes qui travaillent avec de l'information importante risquent plus d'être ciblés que les dispositifs des autres employés;
- les dispositifs mobiles sont des cibles de choix pour les voleurs. S'ils sont volés, l'information qu'ils contiennent pourrait être accessible et utilisée à des fins malveillantes.

Avant de partir en voyage à l'étranger, consultez le document ITSAP.00.087, ***Dispositifs mobiles et voyages d'affaires***. Vous y trouverez de précieux conseils sur la manière de protéger votre dispositif mobile avant, pendant et après votre voyage.

OÙ PUIS-JE EN APPRENDRE PLUS?

Le Centre pour la cybersécurité a élaboré d'autres publications offrant des conseils sur la façon d'utiliser votre dispositif mobile, dont les suivantes :

- ITSM.80.001, *Sécurisation de l'entreprise et des technologies mobiles*;
- ITSAP.30.032, *Pratiques exemplaires de création de phrases de passe et de mots de passe*;
- ITSAP.30.030, *Sécurisez vos comptes et vos appareils avec une authentification multifacteur*;
- ITSAP.00.015, *Êtes-vous victime de piratage?*
- ITSAP.10.116, *Conseils de cybersécurité pour le télétravail*;
- ITSAP.70.015, *Conseils de sécurité pour les dispositifs périphériques*;
- *La cybersécurité et les technologies sans fil (questionnaire en ligne).*

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**.