La protection de la vie privée et les appareils mobiles

www.ipc.on.ca

Table des matières

Introduction

La possibilité de communiquer et d'utiliser des renseignements de façon transparente et continue est devenue un élément essentiel de notre vie quotidienne. Il y a quelques années, le moyen le plus pratique de transporter de grandes quantités de données consistait à les stocker dans des ordinateurs portables ou des clés USB. De nos jours, il y a sur le marché une foule d'appareils et de services (comme l'infonuagique) dont on peut se servir pour stocker et transmettre de grandes quantités de renseignements identificatoires. La technologie continue d'évoluer rapidement, et les atteintes à la sécurité des renseignements identificatoires sont de plus en plus fréquentes. Plus que jamais, il est important que les organisations et leurs employés soient *proactifs, et non réactifs*, lorsqu'il s'agit de protéger les renseignements identificatoires qui sont stockés dans des appareils mobiles et utilisés au moyen de tels appareils.

Les renseignements identificatoires sont des renseignements qui peuvent permettre d'identifier un particulier. En Ontario, on entend souvent parler d'atteinte à la sécurité de renseignements identificatoires insuffisamment protégés découlant de la perte ou du vol d'appareils mobiles. Ces appareils comprennent les ordinateurs portables, les téléphones mobiles et intelligents, les tablettes, les clés USB, les cartes mémoire et même les appareils que l'on porte sur soi et qui peuvent prendre des photos ou consigner et transmettre des renseignements biologiques (comme la glycémie ou le rythme cardiaque).

C'est grâce à leur *portabilité* que les appareils mobiles sont si utiles pour consulter et stocker des renseignements identificatoires, mais c'est elle aussi qui les rend si vulnérables à la perte et au vol. Cependant, il est possible d'éviter les atteintes à la sécurité des renseignements identificatoires en prenant des mesures de précaution proactives.

LE SAVIEZ-VOUS?

Pour sécuriser les renseignements identificatoires dans votre appareil mobile, un mot de passe d'accès ne suffit pas, même s'il est fort. Lorsqu'un appareil mobile contenant des renseignements identificatoires est perdu ou volé, il y a atteinte à la sécurité de ces renseignements à moins que l'appareil soit non seulement protégé par mot de passe, mais également **chiffré**.

Une atteinte à la sécurité se répercute sur tout le monde. Pour l'organisation, qui voit sa réputation entachée, il en coûte du temps et de l'argent. Les particuliers concernés (qui se comptent souvent par milliers), quant à eux, courent un risque de vol d'identité, de fraude et de discrimination, et

perdent confiance dans l'organisation et ses employés, sur qui ils comptaient pour protéger leur vie privée.

Lorsque des renseignements identificatoires sont stockés ou consultés sur un appareil mobile hors du réseau sécurisé de l'organisation, celle-ci et l'employé en question se doivent de protéger ces renseignements. Les organisations sont responsables de la sécurité des renseignements identificatoires qui leur sont confiés tout au long de leur cycle de vie (collecte, utilisation, communication et élimination ou destruction), et elles doivent adopter et communiquer à leurs employés des politiques et pratiques solides en matière de sécurité de l'information.

Le principe AVEC (« apportez votre équipement personnel de communication ») est de plus en plus populaire; il consiste pour les employés à utiliser leurs appareils mobiles personnels (surtout les téléphones intelligents et tablettes) à des fins professionnelles. Tant l'organisation que l'employé doivent protéger les renseignements identificatoires stockés dans l'appareil et consultés au moyen de ce dernier, qu'il appartienne à l'une ou à l'autre.

LE SAVIEZ-VOUS?

Peu importe que l'appareil appartienne à l'organisation ou à l'employé : les deux doivent veiller à protéger les renseignements identificatoires qui leur sont confiés dans le cadre de leur travail.

Les employés doivent respecter les politiques de leur organisation en matière de sécurité de l'information, et éviter de les contourner, c'est-à-dire de consulter, de partager et de stocker des renseignements identificatoires hors du réseau informatique de l'organisation, les rendant ainsi vulnérables. Un exemple de contournement serait d'envoyer des renseignements identificatoires à son adresse courriel personnelle pour y accéder plus tard hors du réseau sécurisé de l'organisation. Cette pratique pourrait sembler efficace, mais elle remet en cause la sécurité des renseignements identificatoires. Les organisations et leurs employés doivent travailler de concert pour améliorer la circulation des renseignements afin d'éviter ces contournements.

Il est important de sécuriser le mieux possible les appareils mobiles utilisés pour accéder à des renseignements identificatoires. Certains pourraient être tentés de « débrider » leur appareil (c.-à-d. de contourner les limitations imposées à certains téléphones intelligents) pour le personnaliser ou utiliser des applications ou fonctions qui seraient autrement interdites, mais ce faisant, leur appareil sera beaucoup plus exposé aux logiciels malveillants et à la fuite de données. C'est pourquoi les personnes qui débrident leur appareil ne devraient pas s'en servir pour

stocker ou consulter des renseignements identificatoires à des fins professionnelles.

Conseils pour sécuriser les appareils mobiles

Avant d'utiliser votre appareil mobile pour stocker des renseignements identificatoires, envisagez des solutions de rechange. Est-il possible d'accéder à ces renseignements sur un serveur au moyen d'une connexion protégée (p. ex., un réseau privé virtuel)?

Avant d'apporter des renseignements identificatoires hors de votre lieu de travail, obtenez l'autorisation nécessaire et respectez les politiques de votre organisation en matière de sécurité de l'information. Apportez uniquement les renseignements identificatoires dont vous avez besoin pour votre travail, et dans toute la mesure du possible, utilisez plutôt des données anonymisées.

Assurez-vous que l'accès aux renseignements identificatoires sur votre appareil mobile est sécurisé en utilisant des mots de passe forts et le chiffrement. De nombreuses atteintes à la sécurité des renseignements survenues en Ontario ont fait intervenir des appareils mobiles sécurisés uniquement par mot de

LE SAVIEZ-VOUS?

On peut protéger les clés USB et les autres appareils de stockage portatifs par les moyens suivants :

- Envisagez des solutions de rechange. Stockez uniquement les renseignements identificatoires dont vous avez besoin pour votre travail. Utilisez plutôt des données anonymisées dans toute la mesure du possible.
- Assurez-vous que les renseignements identificatoires font l'objet d'un chiffrement fort chaque fois qu'ils sont stockés dans des appareils de stockage portatifs, et utilisez des mots de passe forts pour sécuriser les renseignements identificatoires chiffrés.
- Protégez l'appareil contre le vol et la perte et sachez toujours quels renseignements identificatoires s'y trouvent.
- Signalez la perte ou le vol d'appareils contenant des renseignements identificatoires à votre employeur dès que possible.
- Supprimez de façon sécurisée les renseignements identificatoires stockés dans votre appareil dès que vous n'en avez plus besoin.

COMMENT SÉCURISER LES APPAREILS MOBILES

Vous pouvez protéger les renseignements identificatoires que vous stockez dans un appareil mobile ou consultez avec cet appareil à des fins professionnelles par les moyens suivants :

- ☐ **Envisagez des solutions de rechange sécuritaires**

  Y a-t-il une solution de rechange sécuritaire qui vous permettrait de faire votre travail sans avoir à stocker de renseignements identificatoires dans votre appareil mobile (p. ex., accès à distance)?

- ☐ **Confirmez que vous êtes autorisé à stocker des renseignements identificatoires dans un appareil mobile ou à accéder à ces renseignements au moyen avec cet appareil**

  Êtes-vous autorisé à stocker des renseignements identificatoires dans un appareil mobile ou à utiliser ce dernier pour accéder à ces renseignements?

- ☐ **Utilisez le moins possible de renseignements identificatoires ou anonymisez-les**

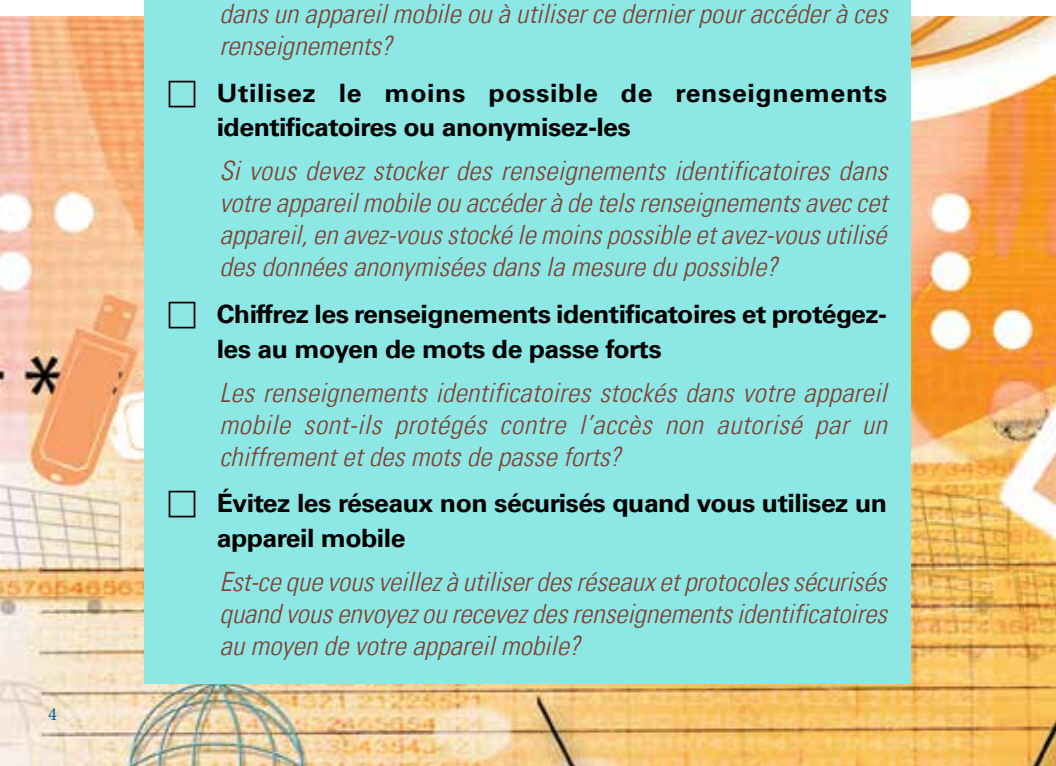
  Si vous devez stocker des renseignements identificatoires dans votre appareil mobile ou accéder à de tels renseignements avec cet appareil, en avez-vous stocké le moins possible et avez-vous utilisé des données anonymisées dans la mesure du possible?

- ☐ **Chiffrez les renseignements identificatoires et protégez-les au moyen de mots de passe forts**

  Les renseignements identificatoires stockés dans votre appareil mobile sont-ils protégés contre l'accès non autorisé par un chiffrement et des mots de passe forts?

- ☐ **Évitez les réseaux non sécurisés quand vous utilisez un appareil mobile**

  Est-ce que vous veillez à utiliser des réseaux et protocoles sécurisés quand vous envoyez ou recevez des renseignements identificatoires au moyen de votre appareil mobile?



☐ **Dans le cas des appareils informatiques mobiles, utilisez des logiciels de protection et réglez bien les paramètres**

Dans votre ordinateur portable, téléphone intelligent, tablette ou autre appareil informatique mobile, avez-vous installé et utilisez-vous des coupe-feu et des logiciels antivirus et antivol? Les paramètres de votre appareil sont-ils réglés de façon à protéger les renseignements identificatoires contre l'accès non autorisé?

☐ **Assurez la sécurité physique de votre appareil mobile**

Veillez-vous à transporter et à utiliser votre appareil mobile de façon sécuritaire pour éviter la perte, le vol, l'espionnage par-dessus l'épaule et l'interception non autorisée de renseignements?

☐ **Sachez quels renseignements identificatoires contient votre appareil mobile**

Si votre appareil mobile était perdu ou volé, pourriez-vous décrire tous les renseignements identificatoires qu'il contient?

☐ **Signalez immédiatement la perte ou le vol d'un appareil mobile**

Si votre appareil mobile était perdu ou volé, savez-vous à quelle personne-ressource de votre organisation vous devriez le mentionner et dans quelles circonstances vous devriez le signaler à la police?

☐ **Retirez dans les plus brefs délais les renseignements identificatoires stockés dans votre appareil**

Est-ce que vous supprimez de façon sécurisée tous les renseignements identificatoires stockés dans votre appareil dès que possible?

Pour sécuriser les ordinateurs portables, téléphones intelligents, tablettes, clés USB et autres appareils mobiles…

Un mot de passe ne suffit pas!

passe. Seuls, les mots de passe ne soustraient pas les organisations et les employés aux responsabilités que la loi leur impose en cas d'atteinte à la sécurité, notamment celle d'informer les particuliers dont les renseignements identificatoires ont été perdus, volés ou consultés par des personnes non autorisées.

Les mots de passe forts doivent être uniques, et ne pas être employés pour protéger d'autres appareils, programmes ou services (p. ex., courriel, médias sociaux, autres comptes). Le mot de passe utilisé pour protéger un appareil doit être différent de celui employé pour accéder à des dossiers de renseignements identificatoires contenus dans cet appareil. Un mot de passe fort se compose d'au moins huit caractères (mais d'au moins 14 de préférence) et devrait contenir des lettres majuscules et minuscules, des chiffres et des symboles (comme $, # ou !). Évitez les mots qui se trouvent dans un dictionnaire, quelle que soit leur langue, même s'ils sont épelés à l'envers.

LE SAVIEZ-VOUS?

Des précautions supplémentaires doivent être prises pour protéger les renseignements identificatoires stockés dans les ordinateurs portables, téléphones intelligents, tablettes et autres appareils informatiques mobiles :

- Installez un coupe-feu et des logiciels antivirus et antivol.
- Réglez les paramètres de sécurité au maximum (p. ex., verrouillage automatique).
- Évitez de vous connecter à Internet par l'entremise de réseaux non sécurisés.

Veillez à installer des logiciels de protection dans vos appareils informatiques mobiles. Dans votre ordinateur portable, téléphone intelligent et tablette, installez un coupe-feu et des logiciels antivirus et antivol qui sont à jour, avec les derniers correctifs de sécurité. Il existe des programmes et services qui permettent de localiser les appareils mobiles perdus et d'en effacer les données à distance; vous ou le service de TI de votre organisation pourriez alors supprimer les renseignements identificatoires de votre appareil mobile avant que quiconque puisse y accéder.

Les appareils informatiques mobiles peuvent aussi être réglés de façon à mieux protéger les renseignements qu'ils contiennent. Par exemple, avec la fonction de verrouillage automatique, l'appareil peut demander un mot de passe après un délai préétabli. Vous pourriez également être en mesure de régler l'appareil pour que les données qu'il contient soient automatiquement supprimées après un certain nombre de tentatives d'accès infructueuses. Ces

paramètres sont peut-être déjà prévus dans les politiques de sécurité de l'information de votre organisation.

Ne laissez pas un appareil mobile contenant des renseignements identificatoires sans surveillance dans un endroit public (p. ex., à une conférence ou dans un café), et évitez d'accéder à ces renseignements en public, où des gens pourraient regarder par-dessus votre épaule. Envisagez d'utiliser un boîtier protecteur avec serrure pour protéger votre appareil mobile, et d'y inscrire vos coordonnées afin qu'on puisse vous le rendre si vous le perdez.

Attention aux réseaux que vous utilisez pour connecter votre appareil informatique mobile à Internet lorsque vous n'utilisez pas le réseau sécurisé de votre organisation. Évitez les réseaux Wi-Fi (également appelés points d'accès sans fil) non sécurisés. Sinon, les données que vous transmettez et recevez pourraient l'être sous forme de texte clair qui pourrait être intercepté. Si vous utilisez un réseau Wi-Fi non sécurisé, ne consultez de renseignements identificatoires que par l'entremise de sites Web qui offrent une connexion chiffrée pendant toute la durée de la session (confirmez qu'il y a ***https*** au lieu de *http* au début de l'adresse URL dans la barre d'adresse de votre navigateur).

La technologie Bluetooth permet à deux appareils de se transmettre des données sans fil sur une courte distance (comme pour le Wi-Fi, mais uniquement pour les appareils jumelés). Dans toute la mesure du possible, n'utilisez Bluetooth qu'avec des appareils qui permettent le chiffrement des données (depuis la version 2.1 de Bluetooth, le chiffrement est activé implicitement). Mettre un appareil mobile en mode « recherche » pour le jumeler à un autre appareil pourrait rendre les renseignements identificatoires vulnérables; vous devriez donc interdire ce mode quand vous avez établi la connexion Bluetooth.

Vous devriez toujours être prêt à composer avec une atteinte à la sécurité des renseignements identificatoires en sachant toujours ceux qui se trouvent dans votre appareil mobile. Lors d'un tel incident, communiquez aussitôt avec votre organisation. Si vous savez quels renseignements identificatoires l'appareil contient et qui ils concernent, il sera plus facile

d'en aviser les personnes concernées. Si l'appareil n'est pas chiffré et si vous n'êtes pas en mesure d'en supprimer les données à distance, envisagez de signaler l'incident à la police.

Les renseignements identificatoires qui sont stockés dans un appareil mobile ne devraient y être conservés que le temps nécessaire pour être utilisés aux fins prévues. Quand vous n'en avez plus besoin, supprimez-les de façon sécurisée avec un utilitaire de nettoyage de données, ou demandez conseil à votre service de TI.

Enfin, le simple fait de connaître vos responsabilités en matière de protection des renseignements identificatoires contribuera grandement à protéger la vie privée des personnes concernées. Soyez conscient des circonstances où vous utilisez des renseignements identificatoires, et protégez-les en prenant des mesures proactives.

Autres ressources

Le CIPVP met à votre disposition les documents suivants; vous pouvez en obtenir une copie papier ou les télécharger à partir de notre site Web à www.ipc.on.ca.

Le chiffrement des renseignements personnels sur la santé dans les appareils mobiles (feuille-info), mai 2007

Le chiffrement fort dans les soins de santé (feuille-info), juillet 2010

Protocole en cas de violation de la vie privée : Lignes directrices pour les institutions gouvernementales (document), mars 2012

Safeguarding Personal Health Information When Using Mobile Devices for Research Purposes, septembre 2011

Que faire en cas d'atteinte à la vie privée : Lignes directrices pour le secteur de la santé (document), juin 2006

Ordonnance HO-004 (ordonnance en matière de santé concernant le vol d'un ordinateur portable contenant des renseignements personnels sur la santé), mars 2007

Ordonnance HO-007 (ordonnance en matière de santé concernant la nécessité de chiffrer les appareils mobiles), janvier 2010

Ordonnance HO-008 (ordonnance en matière de santé concernant le vol d'un ordinateur portable non chiffré contenant des renseignements personnels sur la santé), juin 2010

La destruction sécurisée de renseignements personnels (feuille-info), décembre 2005

Elections Ontario's Unprecedented Privacy Breach: A Special Investigation Report, juillet 2012

Au sujet du CIPVP

Le rôle du commissaire à l'information et à la protection de la vie privée est décrit dans trois lois : la *Loi sur l'accès à l'information et la protection de la vie privée*, la L*oi sur l'accès à l'information municipale et la protection de la vie privée* et la *Loi sur la protection des renseignements personnels sur la santé*. Le commissaire est nommé par l'Assemblée législative de l'Ontario et est indépendant du gouvernement au pouvoir.

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Renseignements :
Commissaire à l'information et à la protection de la vie privée de l'Ontario, Canada
2, rue Bloor Est, bureau 1400
Toronto (Ontario) M4W 1A8 CANADA

Tél : 416 326-3333 ou 1 800 387-0073
Téléc : 416-325-9195 ATS : 416 325-7539
info@ipc.on.ca www.ipc.on.ca

This document is also available in English.

Mise à jour : mai 2014