Les assurances Federated

PRENEZ VOS APPAREILS PERSONNELS

Comment vous protéger lorsque vos employés utilisent leurs appareils personnels au travail?

Prenez vos appareils personnels:
Nouvelle approche en matière de mobilité

En affaires, on accorde aujourd'hui beaucoup de valeur à la disponibilité des données. Le fait d'obtenir l'information voulue au bon moment est tantôt pratique, tantôt essentiel. Si vous êtes comme la plupart des propriétaires d'entreprise canadiens, l'utilisation de téléphones cellulaires fait partie de votre quotidien.

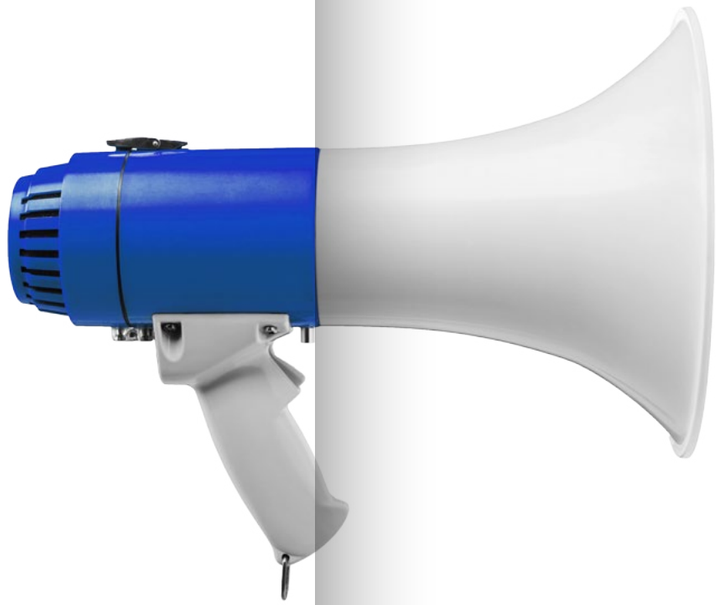
Pour les propriétaires d'entreprise, l'idée de faire assumer aux employés les coûts d'achat des téléphones cellulaires et des forfaits de téléphonie présente un attrait indéniable. La tendance est aux programmes « prenez vos appareils personnels » (PAP), lesquels permettent aux employés d'utiliser un appareil qu'ils connaissent bien et qu'ils ont choisi, et à l'employeur de communiquer avec eux « gratuitement ». Si cette méthode est très économique, | elle n'est toutefois pas sans risque, surtout quand vient le temps d'envoyer de l'information potentiellement sensible sur les horaires, les plans d'affaires ou les clients vers l'appareil d'un employé, qui n'est pas nécessairement fiable et pourrait être déjà compromis.

L'idée n'est pas forcément exclue. Il faut simplement connaître les risques et savoir les prévenir.

Des économies parfois coûteuses pour la réputation…

Ce qui peut coûter le plus cher à la réputation de votre entreprise, c'est la perte de données sensibles. Le bouche-à-oreille fonctionne dans les deux sens : si vous protégez bien les données de vos clients, on voudra faire affaire avec vous, mais si vous les compromettez, vos clients ne reviendront jamais et se feront un devoir de passer le mot. Plus grave encore : si vous êtes responsable d'une atteinte à la sécurité des renseignements personnels d'un partenaire ou d'un client important (comme dans le cas de Target et de Home Depot en 2014), votre marque pourrait subir des dommages irréversibles.

Que doit faire le propriétaire d'entreprise? Prendre le risque d'envoyer des données sensibles vers les appareils personnels de ses employés? Assumer le fardeau et les coûts associés à la remise d'appareils mobiles aux employés (qui préféreraient ne pas avoir à utiliser un deuxième appareil de toute façon)? Il existe une autre option : une solution de gestion des appareils mobiles qui vous permet de communiquer facilement avec vos employés tout en protégeant les données qui leur sont envoyées.



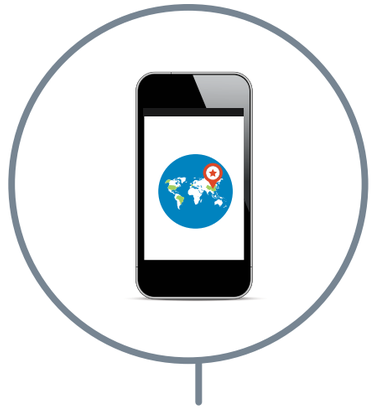
soyez conscient du type d'informations sensibles que vous envoyez en utilisant votre appareil

Gestion des appareils mobiles: communication facilitée et données protégées

Les solutions de gestion des appareils mobiles sont des services offerts sous forme d'abonnements ou de progiciels à installer vous-même. Elles vous permettent de faire ce qui suit:

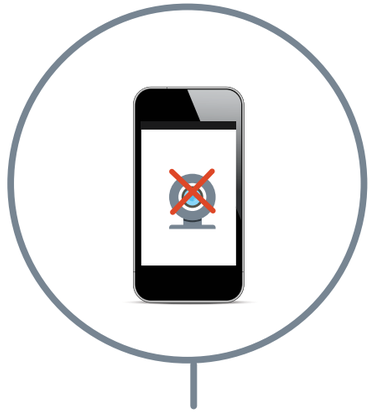
- Attribuer aux utilisateurs un mot de passe pour l'accès à leurs appareils.
- Retrouver un appareil perdu ou volé sur une carte du monde.
- Détruire à distance les données contenues dans un appareil, pourvu qu'il soit connecté à Internet. Vous pourrez soit effacer toutes les données, soit effacer seulement celles se rapportant à l'entreprise et laisser intacts le carnet d'adresses, les courriels et les photos d'usage personnel.
- Désactiver la fonction photo des appareils dans certains endroits. Par exemple, si vous voulez éviter que vos employés prennent des photos des renseignements personnels des clients sur les écrans des ordinateurs de votre entreprise, vous pouvez désactiver cette fonction lorsqu'ils sont au bureau ou durant leurs heures de travail.

Attribuer aux utilisateurs un mot de passe pour l'accès à leurs appareils



Retrouver un appareil perdu ou volé sur une carte du monde

Détruire à distance les données contenues dans un appareil, pourvu qu'il soit connecté à Internet

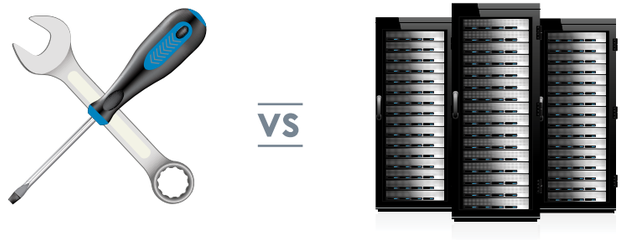


Désactiver la fonction photo des appareils dans certains endroits

L’installer soi-même ou faire appel à un fournisseur de services?

Le temps et les efforts nécessaires à la mise en œuvre d’une solution de gestion des appareils mobiles varient selon que vous achetez un logiciel et l’installez vous-même ou que vous faites appel à un fournisseur de services.

Si vous optez pour un fournisseur de services, vous éviterez le casse-tête associé notamment aux réseaux, aux serveurs et à la formation. Cependant, vous demeurerez tout de même responsable en cas de problème; le fournisseur de services vous aidera à gérer les risques, mais il ne les assumera pas à votre place.



Au moment de choisir une solution de gestion des appareils mobiles, recherchez les fonctions suivantes :

FONCTION	AVANTAGE
Conteneurisation	Permet de séparer les données par source ou par type
Mot de passe	Protège l’accès aux données de l’entreprise par un NIP ou un mot de passe
Cryptage	Rend les données illisibles sans la bonne clé, qui peut être le mot de passe de l’utilisateur
Vérification	Garde une trace de l’utilisation et de la consultation des données de l’entreprise. Pratique pour faire du dépannage et savoir qui a accédé aux données
Antivirus à jour et détection des anomalies	Permet d’échapper aux logiciels malveillants, qui frappent de plus en plus les appareils mobiles. Pour sécuriser les appareils mobiles qui contiennent les données de votre entreprise, vous devrez peut-être installer des logiciels antivirus, comme sur vos ordinateurs
Intégration aux solutions d’authentification existantes (ex. : Active Directory)	Réduit les coûts et facilite le déploiement; l’utilisation du service Active Directory existant de l’entreprise accélère la mise en œuvre, facilite l’utilisation et améliore ainsi l’adoption par les utilisateurs
Prise en charge multiplateforme pour les principaux appareils	Rend la solution de gestion compatible avec les appareils mobiles les plus courants, pour que l’appareil de chaque employé ait le même degré de protection

Ne pas oublier l'assurance des cyberrisques

L'exécution d'une stratégie de gestion des appareils mobiles est l'un des moyens de vous protéger contre les risques. Vous pouvez aussi ajouter une protection contre les cyberrisques (on parle parfois d'assurance protection des données) à votre police d'assurance.

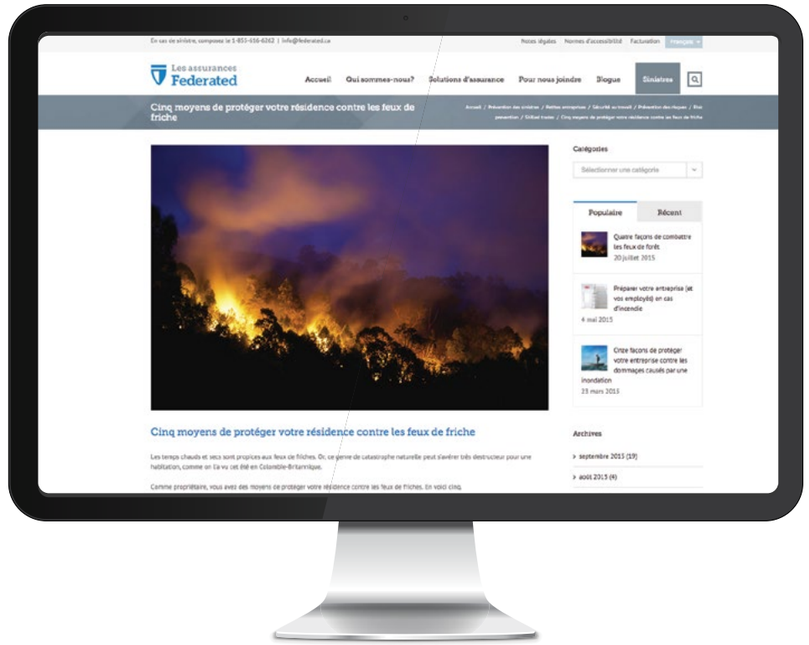
Avant de choisir une solution d'assurance des cyberrisques, assurez-vous qu'elle comprend une garantie pour les ordinateurs portables, les tablettes, les téléphones intelligents, les clés USB et les autres appareils portatifs semblables.

Une bonne police d'assurance des cyberrisques couvrira la responsabilité de votre entreprise non seulement en cas d'atteinte à la protection des données ou de téléchargement d'un virus, mais aussi en cas d'événement « hors ligne », si un document ou un fichier physique se retrouve dans les mauvaises mains.

Pour couronner le tout: les employés, paramètre essentiel de l'équation

Les solutions de gestion des appareils mobiles sont sans contredit très puissantes et donnent beaucoup de pouvoir à l'employeur. Or, il est tout aussi important que vos employés soient convaincus que vous n'utiliserez pas ces solutions pour suivre secrètement leurs déplacements et leurs activités. Ces solutions doivent être utilisées en connaissance de cause des utilisateurs finaux, qui devraient pouvoir y consentir à leur entière discrétion.

De plus, il vous incombe d'informer vos employés des risques associés à l'utilisation de leurs propres appareils et des mesures qu'ils peuvent prendre pour protéger les données de votre entreprise



Vous voulez en savoir plus sur la protection de votre entreprise contre les cyberrisques?

Rendez-vous au **www.federated.ca/fr**


Les assurances
Federated