Pour la version complète du Guide de la cybersécurité pour les petites entreprises de Pensez cybersécurité, visitez le site **PensezCybersecurite.ca/PME**

GUIDE RAPIDE DE LA CYBERSÉCURITÉ POUR LES PETITES ENTREPRISES DE PENSEZ CYBERSÉCURITÉ

Commencez dès maintenant à protéger votre entreprise contre les cybermenaces grâce à ce guide rapide. En suivant les dix étapes énumérées ci-dessous, vous serez sur la bonne voie pour sécuriser votre entreprise contre les cybermenaces courantes.

1. FAITES LE POINT

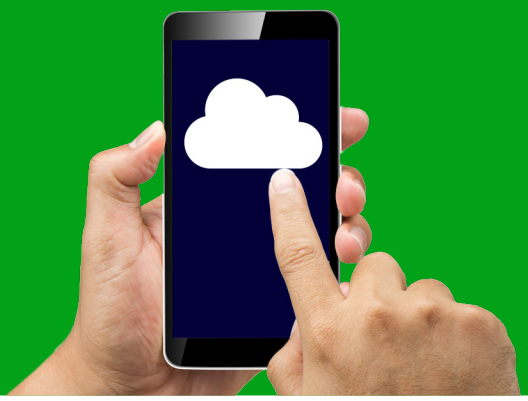
Dressez une liste de tous les appareils et biens connectés à Internet que votre entreprise utilise. Cette liste peut inclure :

- les appareils de bureau et mobiles (ordinateurs, ordinateurs portables, tablettes et téléphones)
- les appareils de stockage (disques durs et clés USB)
- les périphériques (imprimantes, numériseurs, écrans, claviers, souris et stations de recharge)
- les appareils connectés à Internet (appareils de point de vente, systèmes de sécurité intelligents et haut-parleurs intelligents)
- les actifs et services numériques (comptes de médias sociaux, sites Web, services de comptabilité en nuage et en ligne).

Notez l'emplacement de chaque article et qui a l'identifiant et le mot de passe pour y accéder.

2. SÉCURISEZ VOS APPAREILS

Sécurisez chacun des appareils de votre entreprise avec **une phrase de passe ou un mot de passe robuste** unique à chaque appareil. Veillez à mettre à jour les phrases de passe sur les appareils fournis avec un mot de passe par défaut, comme les routeurs et les appareils Bluetooth. Activez **l'authentification multifactorielle** dans la mesure du possible. Limitez les personnes ayant des privilèges d'administrateur, en vous assurant que l'accès est accordé exclusivement en fonction du principe d'accès sélectif.



3. SÉCURISEZ VOTRE RÉSEAU

Le réseau de votre entreprise est la passerelle vers tous vos appareils connectés. Protégez-le avec un **pare-feu** qui surveille le trafic réseau et filtre les sources malveillantes. Vous pouvez également installer le **Bouclier canadien de la CIRA**, un service gratuit de pare-feu DNS qui assure la confidentialité et la sécurité en ligne.

Ensuite, choisissez le meilleur **logiciel antivirus** pour votre entreprise. Assurez-vous qu'il recherche les maliciels connus et les retire, qu'il protège vos appareils des sites Web malveillants et qu'il supervise et signale les comportements suspects des programmes.

Si vos employés font du télétravail, mettez à leur disposition un **réseau privé virtuel** (RPV) afin qu'ils puissent se connecter en toute sécurité depuis l'endroit où ils travaillent.

5. PROTÉGER LES DONNÉES DES CLIENTS ET LES DONNÉES CONFIDENTIELLES DE L'ENTREPRISE

Une violation de vos systèmes de cybersécurité peut entraîner la perte des informations de vos clients. Cela pourrait coûter à votre entreprise la confiance et la réputation que vous avez travaillé à bâtir. Protégez toujours les données confidentielles de votre entreprise à l'aide de phrases de passe robustes. Si votre entreprise utilise une plateforme de commerce électronique, assurez-vous qu'elle inclut des caractéristiques de sécurité telles que l'authentification multifactorielle, le chiffrement des données, des alertes de menace en temps réel et des caractéristiques de conformité.

4. CRÉEZ UN SYSTÈME DE SAUVEGARDE

Il est essentiel d'avoir des sauvegardes de toutes les données, car cela assure à votre entreprise une récupération rapide en cas de perte de données due à une cyberattaque. Si vous choisissez de sauvegarder vos données en utilisant un **service de nuage**, examinez les politiques de confidentialité et les caractéristiques de sécurité proposées par votre fournisseur de nuage, et utilisez une phrase de passe robuste. Gardez à l'esprit que la meilleure **sauvegarde** a sa propre sauvegarde. Même si vous utilisez un service de nuage, sauvegardez vos données les plus importantes sur un appareil de stockage secondaire, tel qu'un disque dur externe ou une clé USB. Déterminez la fréquence à laquelle vous effectuerez des sauvegardes ou configurez les appareils pour qu'ils effectuent des sauvegardes automatiques, au moins une fois par semaine.

6. ACTIVEZ LES MISES À JOUR AUTOMATIQUES

Les **mises à jour** des systèmes d'exploitation et des logiciels contiennent souvent des éléments très importants pour la protection de la sécurité de votre entreprise grâce à des améliorations basées sur les virus et les cyberattaques récents. Activez l'installation automatique des mises à jour pour les systèmes d'exploitation et pour les logiciels. Si les mises à jour automatiques ne sont pas disponibles, installez-les dès que vous y êtes invité.

7. ÉLABOREZ UN PLAN DE CYBERSÉCURITÉ

Un **plan de cybersécurité** définit les règles que vous et vos employés devez suivre. Cela peut inclure :

- des exigences pour utiliser des phrases de passe et l'authentification multifactorielle sur les appareils et les comptes de l'entreprise
- des règles concernant les sites Web que les employés peuvent visiter et les logiciels qu'ils peuvent télécharger
- des conseils sur la sécurité du courriel, incluant la manière d'éviter les arnaques par **hameçonnage**
- des directives sur l'accès aux données de l'entreprise sur des appareils personnels
- un plan de médias sociaux décrivant ce qui peut être partagé sur les comptes de médias sociaux de l'entreprise
- des procédures pour le départ d'un employé, comme la révocation des accès et le changement des mots de passe.

8. FORMEZ VOS EMPLOYÉS

En faisant connaître aux employés ce qui est ou n'est pas cybersécuritaire, vous pouvez contribuer à les éduquer sur la manière dont ils peuvent protéger votre entreprise contre les cybermenaces. Partagez votre plan de cybersécurité avec vos employés et expliquez les raisons pour lesquelles il est en place. Prévoyez des séances de formation régulières pour rafraîchir la mémoire de vos employés et vous assurer que les nouveaux employés profitent de cette formation. Octobre est le mois de la sensibilisation à la cybersécurité et c'est une bonne occasion de parler de cybersécurité.

9. METTEZ EN PLACE UN PLAN D'INTERVENTION EN CAS D'INCIDENT

Un plan d'intervention en cas d'incident décrit comment votre entreprise détectera un cyberincident, y répondra et récupèrera. Votre plan doit inclure des éléments tels que :

DÉTECTER > procédures permettant aux employés de signaler les problèmes

RÉPONDRE > procédures pour isoler l'appareil ou le système affecté, et procédures (incluant éventuellement des services professionnels) pour résoudre le problème

RÉCUPÉRER > procédures pour restaurer vos systèmes à partir de votre sauvegarde

10. RESTEZ À JOUR SUR LA CYBERSÉCURITÉ

Des informations supplémentaires sur chacune de ces étapes sont disponibles dans le Guide complet de la cybersécurité pour les petites entreprises et sur le site Web **PensezCybersécurité.ca/PME**. Pour des informations plus approfondies sur les cybermenaces et les stratégies d'atténuation, visitez le **Centre canadien pour la cybersécurité**. Et, pour obtenir les derniers conseils et directives, suivez le Cyber Centre et Pensez cybersécurité sur les médias sociaux.

@PensezCybersecurite

Numéro de catalogue : D96-87/2022F-PDF | ISBN : 978-0-660-43026-3