Parlons prévention

Des conseils pour vous et votre entreprise

Sept conseils pour protéger votre entreprise contre les risques liés au télétravail

Étant donné la hausse soudaine du nombre de personnes qui font du télétravail, chaque appareil, chaque serveur, chaque réseau Wi-Fi utilisé en dehors de l'entreprise devient un nouveau point d'accès et possiblement une nouvelle vulnérabilité que les pirates peuvent exploiter. Les dirigeants d'entreprise doivent mettre en place des politiques et des directives strictes à l'intention des employés pour éviter une crise de cybercriminalité en cette période inédite de recours au télétravail.

Suivez ces sept conseils pour réduire les risques d'attaque :

- **Publiez des conseils et des règles en lien avec votre politique de sécurité**
  Les formations annuelles et les courriels de rappel du service des TI ne suffisent pas pour que les employés aient toujours à l'esprit les bonnes mesures de cybersécurité à suivre. Des rappels périodiques peuvent contribuer grandement à l'application des pratiques exemplaires en matière de sécurité.

- **Établissez un réseau virtuel privé**
  Un réseau virtuel privé (VPN en anglais) agit comme un tunnel chiffré dans lequel votre trafic Internet circule à l'abri des tiers. Configurer un réseau virtuel privé peut sembler un défi de taille, pourtant cela ne nécessite que quelques heures et est théoriquement peu complexe. Il faut également privilégier un réseau VPN avec authentification multifacteur, car c'est le moyen de défense le plus puissant.

- **Exigez l'utilisation d'une méthode de chiffrement et de la technologie WPA (Wi-Fi Protected Access) pour protéger les réseaux**
  Même si aucun réseau Wi-Fi n'est jamais complètement impénétrable, les réseaux privés et protégés par un mot de passe sont beaucoup plus sûrs que les réseaux Wi-Fi publics, surtout ceux dans les cafés, les hôtels et autres endroits publics. Il est toujours possible de demander à une entreprise qui offre un réseau public si elle a également des réseaux protégés par un mot de passe que vous pourriez utiliser.

- **Exigez l'utilisation par les employés et les tiers d'appareils protégés par un mot de passe**
  Exigez que vos employés choisissent des mots de passe forts contenant des lettres, des chiffres et des caractères spéciaux. Ils doivent aussi éviter d'utiliser le même mot de passe pour plusieurs appareils ou comptes.

- **Utilisez des logiciels antivirus et antimaliciels**
  Rappelez aux employés de faire l'installation de logiciels de sécurité appropriés sur tous les appareils qu'ils utilisent en télétravail, y compris les téléphones cellulaires et les tablettes électroniques, et d'en faire la mise à jour régulièrement. Certains employeurs ne permettent plus aux employés d'utiliser leurs propres appareils et exigent qu'ils utilisent seulement les appareils d'entreprise.

- **Éteignez les ordinateurs**
  Encouragez les employés à éteindre leur ordinateur quand ils ne l'utilisent pas. Lorsqu'ils sont éteints, les ordinateurs sont inaccessibles et à l'abri des attaques et des intrusions provenant d'Internet.

- **Sauvegardez vos données**
  Sauvegardez régulièrement vos renseignements confidentiels et chiffrez les données importantes. Avoir accès à des sauvegardes sécurisées est le meilleur moyen de prévenir l'interruption des activités importantes en cas d'attaque par rançongiciel.

Pour savoir comment rendre votre entreprise encore plus sécuritaire, communiquez avec le Service de prévention au **1.833.692.4112** ou rendez-vous au **www.federated.ca**.