CYBER-SÉCURITÉ

Une déclaration typique que l'on entend dans le secteur de la sécurité des technologies est : « La question n'est pas de savoir si vous serez piraté, mais quand. » La réalité, c'est que si quelqu'un veut entrer, il trouvera la manière de le faire. La seule question est de savoir si vous leur rendez la tâche plus aisée ou si vous contribuez à devenir leur prochaine victime. Une fois qu'un pirate dispos de vos information, il peut les utiliser pour vous faire chanter, vous ou d'autres personnes, pour voler votre identité ou votre argent, tenir vos systèmes en otage jusqu'à ce que qu'une rançon soit payée, ou encore détruire vos données ou vos systèmes.

En ce qui concerne la cyber-sécurité, beaucoup d'entre nous pouvons éprouver de l'incertitude quant à la manière de protéger nos églises, nos écoles et nos ministères contre les menaces existant dans monde numérique. Voici les mesures que vous pouvez prendre afin de protéger les systèmes et les données de votre ministère contre les cyber-risques.

SÉCURISEZ VOTRE RÉSEAU WIFI

Le wifi est souvent l'un des points les plus vulnérables d'un ministère numérique. Les réseaux wifi non-sécurisés peuvent être utilisés pour des activités délictueuses ou pour accéder à d'autres dispositifs connectés au même réseau, tels que les ordinateurs de la société. Il existe plusieurs façons de renforcer la sécurisation de votre réseau :

1. Restreignez-en l'accès en ne postant pas et en ne partageant pas votre mot de passe wifi.
2. Ayez un réseau d'invités pour la congrégation et un autre réseau d'affaires pour les ordinateurs de l'église.
3. Activez l'isolement de votre dispositif. Cela empêche les utilisateurs de voir les autres utilisateurs qui y sont connectés.
4. Modifiez le mot de passe wifi tous les trois mois pour limiter toute utilisation abusive du réseau.

FORMEZ VOS MEMBRES ET VOS EMPLOYÉS

Il est essentiel d'aider les membres à comprendre l'importance que revêt la protection du réseau privé et de ses informations. Demandez aux membres de ne pas partager le wifi de la société ou toute autre information en relation avec la connectivité avec les visiteurs ou les personnes qui ne sont pas autorisées à y accéder.

UTILISEZ DES MOTS DE PASSE EFFICACES

Utilisez des mots de passe pour empêcher tout accès non autorisé à vos ordinateurs, dispositifs ou réseaux, et modifiez-les tous les trois mois. Un mot de passe doit avoir un minimum de 8 à 10 caractères et inclure une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial.

PROTÉGEZ LES INFORMATION DES MEMBRES

Si votre église décide de publier en ligne son annuaire de membres, ajoutez certains obstacles pour garantir que les pirates n'auront pas accès à l'information. Par exemple, créez un accès uniquement réservé aux membres pour accéder à ces informations.

Soyez vigilant et attentif à toute activité suspecte. Si une personne vous appelle pour vous demander des informations au sujet des membres de l'église ou le nom d'un individu, notez le nom de votre interlocuteur et demandez-lui pourquoi il recherche cette information. Soyez prudent et faites attention avec qui vous partagez l'information de l'église, que ce soit des noms, des numéros ou des mots de passe.

CRYPTEZ LES APPAREILS DES EMPLOYÉS

Cryptez toutes les informations sensibles de l'église, particulièrement celles qui sont sur les supports portatifs de la société et les ordinateurs portatifs. Les appareils portatifs sont vulnérables au vol en raison de leur portabilité. Une fois que l'on a accès physiquement à un dispositif, il n'est pas difficile de s'y introduire. Il est fortement recommandé d'utiliser un système de chiffrage sur tous les dispositifs mobiles. Des applications payantes et gratuites sont disponibles. Évaluez soigneusement chaque programme pour identifier celui qui est le plus approprié pour votre église.

LLEN POUR SÉCURISER LES SITES DE PAIEMENT DE LA DÎME

Pour protéger les transactions électroniques liées à la dîme, vérifiez que les systèmes que vous utilisez soient sécurisés. Le lien doit commencer par « https » pour indiquer qu'il s'agit d'une connexion sécurisée. La Division nord-américaine des adventistes du septième jour fournit un site de dons en ligne à chaque église pour recueillir des fonds. Le site est AdventistGiving.org. Le département TI de la Division nord-américaine supervise la sécurité de ce site. Incitez les membres de votre congrégation à ne stocker nulle part les informations relatives à leurs cartes de débit ou de crédit.

TENEZ À JOUR VOTRE PARE-FEU

Le pare-feu est une autre manière de rendre le piratage de votre système plus difficile. Il y trois choses à faire avec soin pour tenir à jour votre pare-feu.

1. Protéger tous les mots de passe.
2. Ne pas utiliser les paramètres par défaut.
3. Toujours tenir les logiciels et microprogrammes à jour. Trop souvent, ces dispositifs sont utilisés selon la configuration initiale et sont ensuite oubliés.

TENEZ À JOUR VOS SYSTÈMES DE SÉCURITÉ

Évaluez régulièrement vos systèmes de sécurité des technologies, en les incluant dans vos mises à jour trimestrielles. Deux questions à se poser:

- Il y a-t-il une mise à jour que je devrais faire ?
- Est-ce que mon logiciel est obsolète (il n'est plus commercialisé, plus utilisé ou périmé) ?

Remplacez ou mettez à jour votre équipement avant que le vendeur ne cesse d'offrir le support technique pour ce dernier, sinon l'équipement ne pourra plus vous protéger contre les risques du moment. Les menaces sont en constante évolution ; il est donc important que vous aussi, vous soyez constamment sur vos gardes.

AYEZ UN NIVEAU DE SÉCURITÉ ADÉQUAT

Il existe de nombreux logiciels de cyber-sécurité qui renforcent la protection de vos systèmes et qui les rendent moins vulnérables aux attaques. Le niveau d'assurance de cyber-sécurité dont votre ministère a besoin dépend de la taille de votre ministère. Évaluez :

1. la taille de votre église,
2. l'étendue et le niveau de technologie que vous avez,
3. la quantité d'information que vous conservez dans ce support technologique.

Cela devrait vous donner une idée plus claire sur la quantité à investir dans les efforts en matière de cyber-sécurité.

VÉRIFIEZ SI VOTRE CONFÉRENCE EST COUVERTE PAR UNE ASSURANCE CYBER-RESPONSABILITÉ

Une assurance cyber-responsabilité permet à votre ministère de se remettre d'une cyber-attaque et elle l'aide à avertir et à assister tous les participants qui ont également été touchées par l'attaque, telles que des membres ou des employés dont les données sont enregistrées par votre ministère. Si votre conférence est couverte par une assurance cyber-responsabilité d'Adventist Risk Management, Inc., tous les ministères de l'église de votre conférence bénéficient de cette couverture. Prenez contact avec les bureaux de votre conférence pour savoir si vous disposez d'une couverture cyber-responsabilité.

DÉCLAREZ IMMÉDIATEMENT VOTRE SINISTRE
1.888.951.4276 • CLAIMS@ADVENTISTRISK.ORG

TENEZ-VOUS INFORMÉ
ADVENTISTRISK.ORG/SOLUTIONS