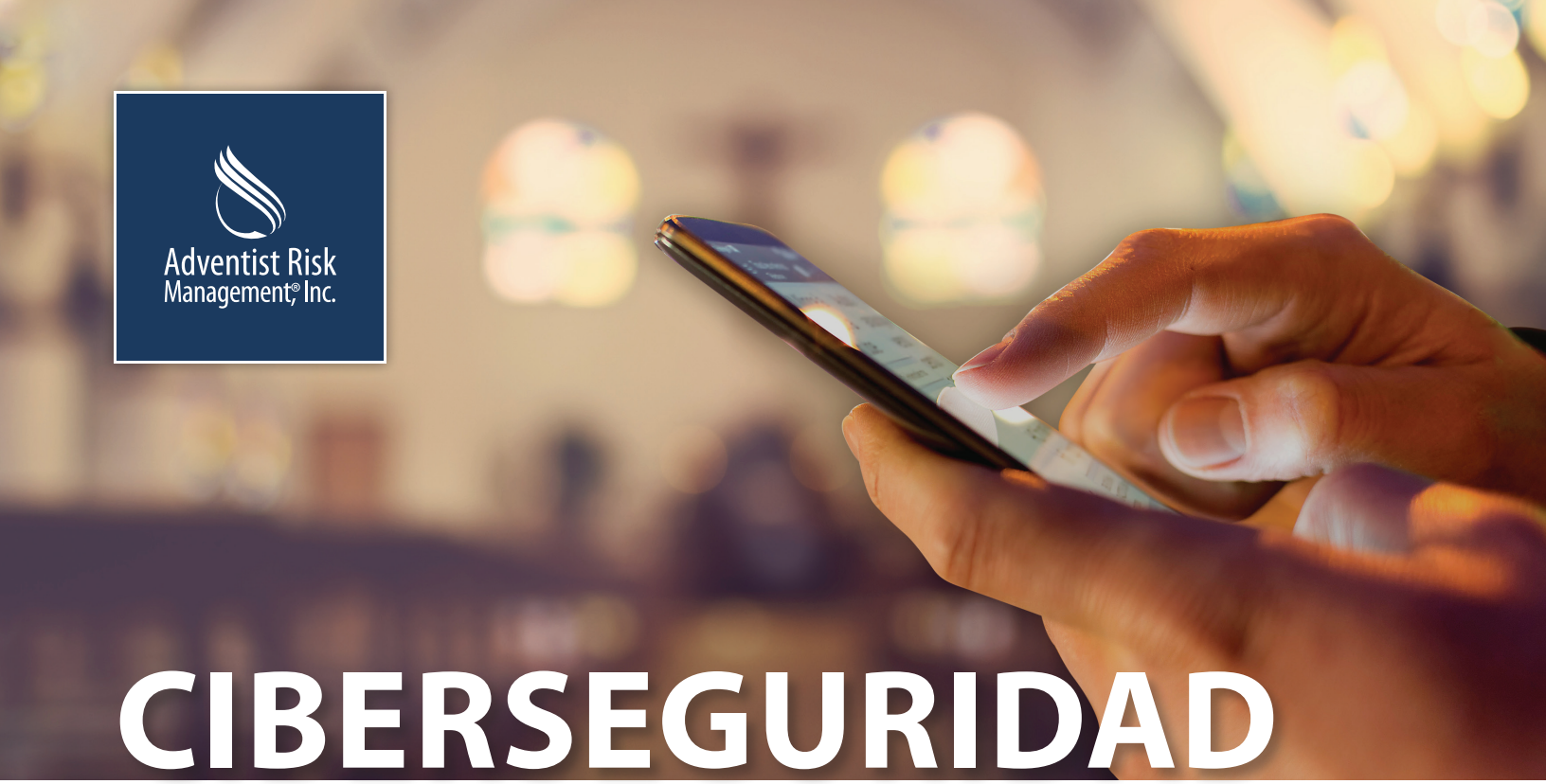

Adventist Risk Management® Inc.

CIBERSEGURIDAD

Una de las afirmaciones típicas en la industria de seguridad de tecnología es: «No se trata de si vas a ser víctima de un ataque informático, sino de cuándo». La realidad es que si alguien quiere ingresar, encontrará la manera de hacerlo. Es sólo cuestión del nivel de dificultad que usted presenta y de si es usted un objetivo probable. Una vez que el pirata informático se apodera de su información, puede usarla para chantajearlo a usted o a otras personas, robar su identidad o su dinero, tomar como rehén a sus sistemas hasta que se pague recompensa, o destruir sus datos o sistemas.

Cuando se trata de ciberseguridad, muchos de nosotros podemos sentirnos inseguros sobre cómo proteger a nuestras iglesias, escuelas y ministerios de los riesgos del mundo digital. Los siguientes son los pasos que puede dar para proteger los sistemas y datos de su ministerio de riesgos cibernéticos.

ASEGURE SU CONEXIÓN WIFI

El wifi suele ser uno de los temas más vulnerables en el ministerio digital. Las redes de wifi inseguras pueden usarse para perpetrar actividades delictivas o para ingresar a otros dispositivos que también están en la red, por ejemplo computadoras de empresas. Hay muchas maneras en que usted puede asegurar su red:

1. Restrinja el acceso; no publique ni comparta la contraseña de wifi.
2. Tenga una red aparte de invitados para la congregación y una red de trabajo para las computadoras de la iglesia.
3. Habilite el aislamiento del dispositivo. De este modo se evita que los usuarios vean a otros que se han conectado.
4. Cambie la contraseña de wifi cada tres meses para evitar el abuso de la red.

EDUQUE A SUS MIEMBROS Y EMPLEADOS

La educación es esencial para ayudar a los miembros a entender la importancia de proteger la red privada y su información. Instruya a los miembros que no deben compartir la red wifi de trabajo u otra información de conectividad con los visitantes u otras personas que no están autorizadas a ingresar.

UTILICE CONTRASEÑAS FUERTES

Use contraseñas para evitar el acceso no autorizado a sus computadoras, dispositivos o red, y cámbielas cada tres meses. La contraseña debe tener entre 8 y 10 caracteres como mínimo e incluir una letra mayúscula, una letra minúscula, un número y un carácter especial.

PROTEJA LA INFORMACIÓN DE LOS MIEMBROS

Si su iglesia decide publicar el directorio de miembros en línea, incorpore algunos obstáculos para asegurarse de que los piratas informáticos no tengan acceso a la información. Por ejemplo, cree un acceso sólo para miembros para ingresar a esa información.

Esté atento y alerta a cualquier actividad sospechosa. Si alguien llama y pregunta por miembros de la iglesia y por un nombre en particular, tome nota de la persona que llama y de por qué solicita información. Piense bien y sea cuidadoso con quién comparte información de la iglesia, que incluye nombres, números y contraseñas.

ENCRIPTE LOS DISPOSITIVOS DE LOS EMPLEADOS

Encripte toda la información confidencial de la iglesia, en especial la que está en dispositivos móviles y computadoras portátiles. Los dispositivos móviles son vulnerables al robo debido a su portabilidad. Una vez que alguien obtiene acceso físico a los dispositivos, no es difícil vulnerarlos. La encriptación de disco es algo que debería considerarse seriamente para todos los dispositivos móviles. Existen aplicaciones gratuitas y pagas. Evalúe cuidadosamente cada programa para encontrar el que mejor se adapte a su iglesia.se adapte a su iglesia.

ENLACE A SITIOS SEGUROS DE PAGO DE DIEZMO

Para proteger las transacciones electrónicas de diezmos, asegúrese de que los sistemas que está usando sean seguros. El enlace debería comenzar con «https», que indica que se trata de una conexión segura. La División Norteamericana de Adventistas del Séptimo Día tiene un sitio web de donación en línea para que cada iglesia recaude fondos. El sitio es AdventistGiving.org. El departamento de TI de la División Norteamericana supervisa la seguridad de este sitio. Recomiende a su congregación abstenerse de almacenar información de tarjetas de débito o crédito en cualquier lado.

MANTENGA SUS CORTAFUEGOS

Los cortafuegos son otro modo de hacer que sea más difícil piratear su sistema. Existen tres cosas que debe hacer con diligencia para mantener su cortafuego.

1. Proteja todas las contraseñas.
2. No utilice configuraciones por defecto.
3. Mantenga siempre actualizados los software y firmware. Muchas veces, a estos dispositivos se les realiza una configuración inicial y luego se olvidan.

MANTENGA SUS SISTEMAS DE SEGURIDAD

Evalúe los sistemas de seguridad de su tecnología en forma regular, como parte del mantenimiento estacional cada tres meses. Debe hacerse dos preguntas:

- ¿Hay algún mantenimiento que debería hacer?
- ¿Mi software es obsoleto (ya no se produce o utiliza, o está caducado)?

Sustituya o actualice su equipo antes de que el vendedor del producto deje de ofrecerle soporte técnico o de que el equipo ya no pueda protegerlo de las amenazas existentes. Las amenazas siempre cambian, de modo que es importante que usted también esté constantemente alerta. you are also constantly vigilant.

TENGA LA CANTIDAD ADECUADA DE PROTECCIÓN

M Existen numerosos programas de ciberseguridad para ampliar la protección de sus sistemas y hacer que sean menos vulnerables a los ataques. La cantidad de seguro de ciberseguridad que su ministerio necesita depende del tamaño de su ministerio. Evalúe:

1. el tamaño de su iglesia,
2. el alcance y la cantidad de tecnología que tiene y
3. cuánta información almacena en esa tecnología.

Con estos datos debería tener una idea más clara de cuánto invertir en ciberseguridad.

AVERIGÜE SI SU CONFERENCIA TIENE SEGURO DE RESPONSABILIDAD CIVIL CIBERNÉTICA

El seguro de responsabilidad civil cibernética puede ayudar a su ministerio a recuperarse de un ataque cibernético y ayudarlo a notificar y asistir a los miembros que también se hayan visto afectados por el ataque, como por ejemplo miembros o empleados cuyos datos guarda el ministerio. Si su conferencia tiene seguro de responsabilidad civil cibernética de Adventist Risk Management, Inc., los ministerios de la iglesia en su conferencia cuentan con cobertura de responsabilidad civil cibernética. Comuníquese con la oficina de su conferencia para averiguar si usted tiene cobertura de responsabilidad civil cibernética.

INFORME SU RECLAMO DE INMEDIATO

1.888.951.4276 • CLAIMS@ADVENTISTRISK.ORG

MANTÉNGASE INFORMADO

ADVENTISTRISK.ORG/SOLUTIONS