Adventist Risk Management, Inc.

By: Tony Vargas - ARM.JobTitle.VPChiefInformationOfficer

Seguridad en línea: ya no es algo opcional

marzo 16, 2021

Reconocemos la rápida y constante digitalización de la información que nos rodea hoy. Independientemente de quién sea la persona responsable de la seguridad de los datos, comúnmente se cree que el robo de nuestra información es solo cuestión de tiempo.

Dada esta expectativa, debemos hacer todo lo posible por minimizar el riesgo para nosotros mismos y para los demás. A menudo lo logramos a través de las decisiones que tomamos a diario. Sin embargo, también es necesario que implementemos los protocolos de seguridad adecuados y nos aseguremos de que nuestro personal y nuestros voluntarios tengan la capacitación apropiada para ayudar a prevenir los ciberataques.

Conocimiento

Conocer cómo y con qué interactuamos a través de correo electrónico, sitios web y mensajes de texto es fundamental para protegernos. Estos representan algunos de los métodos más comunes que los piratas informáticos usan para infiltrarse en nuestro sistema. Algunas de las medidas específicas que debería tomar son:

- Cuando reciba un correo electrónico, siempre verifique el remitente. Puede hacerlo de diferentes maneras. Comience pasando el cursor sobre el nombre del remitente para confirmar su dirección de correo electrónico. Si parece diferente de lo que esperaba, podría no ser de quien dice ser. Verifique el cuerpo del mensaje de correo electrónico para ver si la redacción parece la de la persona que envió el correo. Si algo no concuerda, comuníquese con el remitente por otro medio y confirme si envió el mensaje.
- Tenga cuidado con usar enlaces dentro de un correo electrónico o en un sitio web. El solo hecho de que un enlace diga adventistrisk.org no significa que vaya a remitirlo a nuestro sitio web. Pase el cursor sobre el enlace para ver la dirección URL a la que el enlace lo dirige y verifique si tiene sentido.
- El protocolo de transferencia de hipertexto (HTTP, por sus siglas en inglés) es el «lenguaje» que utilizan los sitios web. Cualquier sitio que contenga datos sensibles debería estar protegido por un protocolo seguro de transferencia de hipertexto (HTTPS). Puede confirmar si un sitio está encriptado buscando el HTTPS en la URL o dirección web.
- No dé más información que la necesaria. A menudo, los remitentes dudosos usan la información que usted publica sobre sí mismo u otras personas en las redes sociales para crear perfiles falsos con esa información. Luego esa información se utiliza para hacer que los

correos electrónicos o mensajes de texto parezcan legítimos y enviados por usted. Cuando sea posible, configure sus cuentas de redes sociales como privadas para ayudar a reducir el riesgo.

Credenciales

La persona promedio tiene acceso a cientos de cuentas en línea, tanto personales como de trabajo. Recuerde que sus credenciales de nombre de usuario y contraseña son su primera línea de defensa para proteger datos personales críticos. Algunas cosas que debe recordar:

- Nunca use las mismas credenciales en más de un sistema. Si ese sistema sufre un ataque informático, los remitentes dudosos se apropian de esas credenciales robadas. Luego intentan utilizarlas en cientos de sitios de uso común con la esperanza de que usted las haya vuelto a usar en otro sitio. Si así fue, ahora tienen acceso a numerosos sistemas en lugar de solo a uno.
- Use siempre contraseñas complejas de por lo menos 10 caracteres o más. Complejas significa que su contraseña incluya como mínimo una letra mayúscula, una letra minúscula, un número y un carácter especial.
- La mayoría de los sistemas en línea ahora ofrecen autenticación de dos factores para proteger su cuenta. Elija esta opción cada vez que se la ofrezcan. Al usar la autenticación de dos factores, a los remitentes dudosos les resulta aún más difícil tener acceso a sus datos. Que la autenticación sea de dos factores significa que usted debe usar más que simplemente un nombre de usuario y una contraseña para ingresar al sitio. Por ejemplo, podría ser necesario conocer un código de acceso de un solo uso, acusar recibo de una notificación enviada a su teléfono o correo electrónico, u otro método similar.

Proteja sus conexiones

Asegúrese de proteger sus conexiones, ya sea que navegue por una red conocida como la de su casa o en modo de itinerancia.

- Proteja su computadora con una contraseña y asegúrese de bloquear su dispositivo si se aleja de él, aunque esté en su casa. Una persona solo demora un minuto en ingresar a su computadora si no está bloqueada.
- Utilice un cortafuegos moderno para proteger la conexión entre internet y su red en casa o en el trabajo.
- Cuando sea posible, no use una conexión wifi pública. En general, estas conexiones públicas no son seguras, y los remitentes dudosos pueden controlarlas y robar su información mientras usted usa su dispositivo.
- Si debe usar wifi público, al menos utilice una aplicación de Red privada virtual (VPN, por sus siglas en inglés). Una aplicación de VPN encripta los datos de su conexión de internet y dificulta el robo de información a los remitentes dudosos. Existen numerosas VPN disponibles, pero asegúrese de leer las reseñas y elegir una acreditada.

Utilice métodos de protección adecuados

En la actualidad existe una lista completa de métodos de protección de acuerdo con los sistemas que utilice. Sin embargo, estos son algunos de los métodos universales más comunes.

- Use un *software* antivirus acreditado. Numerosas aplicaciones de *software* antivirus incluyen protección contra *malware* (programas maliciosos), *ransomware* y protección contra sitios web malintencionados.
- Considere el uso de un bloqueador de anuncios para su explorador. De esta manera bloqueará anuncios que se utilizan comúnmente con el objetivo de engañarlo para que haga clic en un enlace que podría infectar su computadora.
- Configure su explorador web de manera que borre automáticamente la memoria caché, o hágalo con regularidad en forma manual. Borrar la memoria caché lo protege de los remitentes dudosos, que podrían utilizarla para recopilar sus hábitos de navegación y usar los datos para perjudicarlo.
- Utilice filtros de correo no deseado y de correo electrónico. Un buen sistema de filtrado de correo electrónico puede ayudarlo a detectar correos de suplantación de identidad o infectados antes de recibirlos. De esta manera se reducen las posibilidades de que lo engañen para hacer clic en un enlace incorrecto o de que responda por error a un correo electrónico falso. Estas dos acciones pueden hacer que su computadora se infecte o que comparta información con una persona equivocada.
- Con tantos sistemas que se utilizan en la vida cotidiana, elija un administrador de contraseñas acreditado para ayudarlo a almacenar sus contraseñas con seguridad. De esta manera podrá usar una contraseña compleja y única para cada cuenta o sistema.
- Mantenga su sistema operativo actualizado y revisado. Incluso una computadora Mac posee vulnerabilidades.
- Además, mantenga sus aplicaciones revisadas y actualizadas. Asegúrese de quitar todas las aplicaciones que no utilice para evitar que lo expongan a vulnerabilidades.
- Ya sea que haya o no niños que utilizan las computadoras, asegúrese de usar un filtro DNS. El filtrado DNS le permite bloquear categorías específicas de exploración web indeseadas y lo protege impidiéndole visitar sitios web con infecciones conocidas.

La ciberseguridad es un tema serio que enfrentan nuestras iglesias, escuelas y ministerios de todo el mundo. Adventist Risk Management, Inc. (ARM) dedicará el Safety Sabbath de este año para ayudar a los ministerios a estar mejor protegidos contra los ataques. Con la inscripción de su iglesia para participar, recibirá recursos gratuitos que ayudarán a su iglesia a identificar riesgos potenciales y a saber qué hacer para mitigarlos.

ARM ha trabajado con expertos líderes en el campo de la ciberseguridad para desarrollar los recursos disponibles para el Safety Sabbath. Inscríbase hoy para ayudar a proteger su ministerio.

Referencia

Créditos de imagen: iStock/Marco_Piunti