CYBER READINESS
INSTITUTE

# Una nueva razón para temer la temporada de impuestos: los ataques a la ciberseguridad

El plazo de presentación de impuestos está muy próximo. Busca entre los papeles esparcidos por la mesa del comedor tratando de encontrar el formulario de impuestos que falta. Durante la última semana, ha recibido un flujo constante de correos electrónicos de su contable pidiéndole la información que falta. Necesitan este formulario; necesitan ese recibo; necesitan que clasifique un gasto. Se está frustrando y distrayendo.

Llega otro correo electrónico de su contable. En este se le pide que haga clic en un enlace y facilite su número de la seguridad social. Deja de buscar en los papeles y, por reflejo, empieza a hacer clic en el enlace.

Pero algo le invade y hace una pausa. “Mi empresa de contabilidad conoce mi número de la seguridad social. Hicieron mi declaración el año pasado”. Por tanto, en lugar de hacer clic en el enlace, empieza a responder al correo electrónico, pero entonces cae en la cuenta. “Si es un correo de phishing y respondo, volverá a los piratas informáticos”.

Usted decide sabiamente coger el teléfono y llamar a su empresa de contabilidad. Le dicen desesperadamente que han sido hackeados y que ese mismo correo electrónico de phishing le llegó a todos sus clientes. No pueden utilizar el correo electrónico para avisar a sus clientes, así que los han estado llamando uno por uno y rezando para que nadie haga clic en el enlace.

En la empresa de contabilidad, el caos es total. La temporada de impuestos siempre es una locura, pero los ciberataques la está llevando al límite. No solo se puso en peligro su correo electrónico, sino que los piratas informáticos exigen un rescate para desbloquear todos los datos de sus clientes.

Cuando comenzó el ataque, nadie sabía qué hacer. Nunca habían oído hablar de un plan de respuesta a incidentes cibernéticos. Llamaron desesperadamente a su consultor de TI, que les preguntó si tenían copias de seguridad actualizadas de los datos del cliente. “¡Creía que tú te encargabas de eso!”, le gritaron al consultor de TI. “No. Esa es tu responsabilidad”, fue la tranquila respuesta.

El consultor de TI dijo que todo el software estaba actualizado, así que es probable que los piratas informáticos entrasen en el sistema de la empresa de contabilidad debido a contraseñas débiles o porque alguien hizo clic en un enlace.

La empresa de contabilidad comenzó a llamar a sus clientes para informarles del correo electrónico falso de solicitud del número de la seguridad social. Tuvieron que avisar a cada cliente de que sus datos personales podrían ponerse en peligro y explicar que tendrían que solicitar una prórroga para presentar sus impuestos. Veinte años de creación de una base de clientes de confianza se pusieron en peligro en un día horrible. Los socios prometieron estar preparados para la preparación cibernética siguiendo los consejos que se indican a continuación.



guide@cyberreadinessinstitute.com

# 6 consejos esenciales de ciberseguridad para la temporada de impuestos

## Consejos para personas físicas y preparadores de impuestos

**Utilizar contraseñas seguras:** asegúrese de utilizar una frase de contraseña de 15 caracteres o más para sus programas y de que cada frase de contraseña sea única para cada una de sus cuentas. Active la autenticación de múltiples factores en sus cuentas, siempre que sea posible.

**Actualizar el software:** active la actualización automática y asegúrese de que sus parches de software estén instalados, sobre todo antes de la temporada impositiva de cada año. Dada la cantidad de negocios que se realizan en línea durante la temporada de impuestos, todos somos vulnerables.

**Intercambio seguro de archivos:** nunca facilite ni pida un número de la seguridad social, ni ningún otro dato financiero confidencial, por correo electrónico o en línea. Valide cualquier transacción financiera solicitada (por ejemplo, transferencia bancaria, depósito directo) o solicitud de datos personales con una llamada telefónica a la persona que la solicita. Asegúrese de que su intercambio de archivos o portal en línea sea seguro y esté cifrado.

**Realizar copias de seguridad y pruebas:** realice una copia de seguridad de sus datos críticos con regularidad y pruebe sus copias de seguridad todos los meses.

**Tener un plan:** asegúrese de tener un plan de respuesta a incidentes probado para su organización. En caso de que se produzca una vulneración, es esencial disponer de un plan de respuesta y recuperación que pueda activar de inmediato. La comunicación entre usted y sus clientes también es fundamental en caso de vulneración.

**Ser prudente:** ya sabe que el IRS (Servicio de Impuestos Internos de los Estados Unidos) nunca se comunicará con personas por teléfono o correo electrónico. No obstante, tenga cuidado con los correos electrónicos de su preparador de impuestos. Si algo no parece correcto, llámelo para verificar que el correo electrónico sea legítimo antes de abrirlo. Esta es una época del año muy popular en la que los ciberdelincuentes tratan de engañar a las personas para que envíen información financiera personal.

## Acerca del CRI

**El Cyber Readiness Institute es una iniciativa sin fines de lucro que reúne a líderes empresariales de todos los sectores y zonas geográficas para compartir recursos y conocimientos que impulsan el desarrollo de herramientas de ciberseguridad gratuitas para las pequeñas y medianas empresas (pymes). Explore los elementos básicos de una buena ciberseguridad con nuestro Kit básico o cree una cultura de preparación cibernética en su organización con el Programa de Preparación Cibernética autodirigido y disponible en línea. Nuestras guías sobre Recursos de trabajo remoto y Lugar de trabajo híbrido ofrecen consejos oportunos para abordar los cambiantes retos cibernéticos de hoy en día. Para obtener más información, visite www.BeCyberReady.com.**