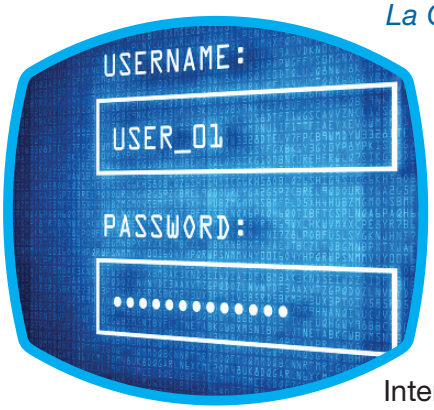
Proteja a sus clientes; Protéjase a sí mismo

Guía de Recursos de Seguridad de Datos para los Profesionales de Impuestos



La Guía de Recursos de Seguridad de Datos para los Profesionales de Impuestos, está diseñada para proporcionar un entendimiento básico de las medidas mínimas para proteger los datos de los clientes. Se anima a todos los profesionales de impuestos a trabajar con los profesionales de ciberseguridad para garantizar la seguridad de los sistemas. Es su responsabilidad proteger los datos de los contribuyentes del robo y la divulgación.

Cómo empezar

La Cumbre de Seguridad – la colaboración entre el Servicio de Impuestos Internos, las agencias tributarias estatales y la industria de impuestos – recuerda a todos los profesionales de impuestos que cada uno tiene un papel en la protección de los datos del contribuyente.

La ley de Modernización de los Servicios Financieros de 1999, también conocida como la Ley *Gramm-Leach-Bliley*, requiere que ciertas entidades – incluyendo los preparadores de declaraciones de impuestos – establezcan y mantengan un plan de seguridad para la protección de los datos de los clientes.

Las siguientes dos publicaciones pueden ayudarle a comenzar:

- ***Publicación 4557*** del *IRS*, ***Safeguarding Taxpayer Data*** (Cómo salvaguardar los datos del contribuyente), en inglés.
  Esta publicación proporciona un resumen general de las obligaciones de los profesionales de impuestos de proteger la información de los contribuyentes y proporciona una lista de comprobación paso a paso de cómo establecer y mantener un plan de seguridad para su red digital y oficina.
- ***NIST's Small Business Information Security – The Fundamentals*** (Seguridad de la Información de Negocios Pequeños del *NIST* – Los Fundamentos), en inglés.
  El Instituto Nacional de Estándares y Tecnología (*NIST*, por sus siglas en inglés) es una rama del Departamento de Comercio de los Estados Unidos. Establece el marco de seguridad de la información para las agencias federales. También produjo este documento para proporcionar a los negocios pequeños un resumen general de esos pasos para la seguridad de los datos. Se centra en cinco principios: identificar, proteger, detectar, responder y recuperar.

No se olvide de la ***Publicación 1345***, *Handbook for Authorized IRS e-File Providers* (Guía para los proveedores de *e-File* autorizados del *IRS*), en inglés, la cual describe su responsabilidad como un Originador de la Declaración Electrónica, incluso en el área de seguridad y privacidad de *e-File*.

¿Qué puede hacer?

- Aprenda a reconocer los correos electrónicos de *phishing*, sobre todo aquellos que fingen ser del *IRS*, de servicios electrónicos, un proveedor de software tributario o un proveedor de almacenamiento en la nube. Nunca pulse en un enlace ni abra cualquier anexo de un correo electrónico sospechoso. Recuerde: El *IRS* nunca inicia contacto inicial por correo electrónico con los profesionales de impuestos sobre las declaraciones, reembolsos o solicitudes de información financiera o de contraseñas confidenciales.

- Establezca un plan de seguridad de datos, utilizando la ***Publicación 4557*** del *IRS*, *Safeguarding Taxpayer Data* (Cómo salvaguardar los datos del contribuyente), en inglés, y ***Small Business Information Security – The Fundamentals*** (Seguridad de la Información de Negocios Pequeños – Los Fundamentos), en inglés, del Instituto Nacional de Estándares y Tecnología.
- Revise los controles internos:
  - Instale el software de seguridad *anti-malware/anti-virus* en todos los dispositivos (computadoras portátiles, computadoras de escritorios, enrutadores, tabletas y teléfonos) y mantenga el software configurado para que se actualice automáticamente.
  - Utilice contraseñas fuertes y únicas de 8 o más caracteres mixtos, las contraseñas protegen todos los dispositivos inalámbricos; utilice una frase o palabras que sean fáciles de recordar y cambie las contraseñas periódicamente.
  - Encripte todos los archivos/correos electrónicos y utilice contraseñas fuertes para protegerlos.
  - Haga una copia de seguridad de sus datos confidenciales y guárdela en un lugar externo y seguro que no esté conectado a tiempo completo a una red.
  - Haga una revisión final de la información de la declaración de impuestos – especialmente la información de depósito directo – antes de la presentación electrónica.
  - Borre o destruya los discos duros de las computadoras e impresoras anteriores que contengan datos confidenciales.
  - Limite el acceso a los datos de los contribuyentes a sólo a las personas que tienen que saberlos.
  - Verifique semanalmente la cuenta de los servicios electrónicos del *IRS*, para ver el número de declaraciones presentadas con el Número de Identificación para la Presentación Electrónica (*EFIN*, por sus siglas en inglés).
- Informe todo robo o pérdida de datos al ***Enlace del IRS con las partes interesadas (en inglés)*** apropiado.
- Manténgase conectado con el *IRS* a través de las inscripciones al ***Boletín electrónico para los Profesionales de Impuestos (en inglés)***, ***QuickAlerts*** (en inglés) y los ***Medios Sociales.***

Aprenda las señales de robo de datos

Usted o su empresa puede ser una víctima y no lo saben. A continuación, algunas señales comunes de robo de datos:

- Las declaraciones de los clientes que presenta electrónicamente empiezan a ser rechazadas, porque ya se habían presentado declaraciones con sus números de Seguro Social;
- Los clientes que todavía no han presentado sus declaraciones de impuestos empiezan a recibir cartas de autenticación (5071(C/SP), 4883(C/SP), 5747(C/SP)) del *IRS*;
- Los clientes que no han presentado declaraciones de impuestos reciben reembolsos;
- Los clientes reciben transcripciones de impuestos que no solicitaron;
- Los clientes que han creado cuentas en línea con el *IRS*, reciben un aviso del *IRS* de que su cuenta fue accedida, o los

correos electrónicos del *IRS* indicando que su cuenta ha sido desactivada; o, los clientes reciben un aviso del *IRS* de que una cuenta en línea del *IRS* fue creada en sus nombres;

- El número de declaraciones presentadas con el Número de Identificación de Presentación Electrónica (*EFIN*) excede el número de los clientes;
- Los profesionales de impuestos o clientes que responden a correos electrónicos que usted no envió;
- Las computadoras en su red funcionan más lentas de lo normal;
- Los cursores de las computadoras moviéndose o cambiando los números sin tocar el teclado;
- Las computadoras en su red bloquean a los preparadores de impuestos.

Manténgase alerta

Manténgase un paso más adelante de los ladrones, tomando ciertas acciones a diario o semanalmente, para asegurar que sus clientes y su negocio permanezcan seguros:

- Haga un seguimiento de sus acuses de recibo diarios de *e-File*. Si hay más acuses de recibo que declaraciones que usted sabe que presentó, investigue más a fondo.
- Haga un seguimiento de su uso semanal del *EFIN*. El número de declaraciones presentadas con su Número de Identificación de Presentación Electrónica (*EFIN*) se publica semanalmente. Entre a su cuenta de servicios electrónicos, acceda a su aplicación de *e-file* y verifique el "*EFIN Status*" (Estado del *EFIN*). Si los números están apagados, comuníquese con el servicio de ayuda electrónica. Mantenga su aplicación del *EFIN* actualizada con todos los cambios de teléfono, dirección o personal.
- Si usted es un preparador sujeto a la "Circular 230" o un "participante del programa anual de la temporada de presentación de impuestos" y presenta 50 o más declaraciones al año, puede consultar su cuenta del *PTIN* para obtener un informe semanal de las declaraciones presentadas con su Número de Identificación del Preparador de Impuestos (*PTIN*, por sus siglas en inglés). Acceda a su cuenta del *PTIN* y seleccione "*View Returns Filed Per PTIN*." (Ver las declaraciones presentadas por *PTIN*). Presente el Formulario 14157, *Complaint: Tax Return Preparer* (Queja: Preparador de declaraciones de impuestos), en inglés, para informar del uso excesivo o indebido del *PTIN*.
- Si tiene un Número de Archivo Centralizado de Autorizaciones (*CAF*, por sus siglas en inglés), asegúrese de mantener al día sus autorizaciones. Elimine las autorizaciones para los contribuyentes que ya no son sus clientes. Vea la ***Publicación 947***, *Practice Before the IRS and Power of Attorney* (Práctica ante el *IRS* y el poder legal), en inglés.
- Establezca sus cuentas en línea con el *IRS* utilizando la verificación de Acceso Seguro de dos factores, que ayuda a prevenir que se apoderen de su cuenta. Vea ***IRS.gov/secureaccess*** para revisar las acciones necesarias.

¿Datos perdidos o robados? Infórmelo rápidamente

Comuníquese con el *IRS* y los cuerpos policiales:

- ***Servicio de Impuestos Internos (en inglés)***, informe el robo de datos de los clientes a su Enlace local de las partes interesadas.
- ***Oficina Federal de Investigaciones (en inglés)***, su oficina local (si le indican hacerlo).
- ***Servicio Secreto (en inglés)***, su oficina local (si le indican hacerlo).
- Policía local – para presentar un informe policial sobre la filtración de datos.

Comuníquese con los estados de los que usted prepare declaraciones estatales:

- Envíe un correo electrónico a la Federación de Administradores Tributarios, en ***StateAlert@taxadmin.org***, para obtener información sobre cómo informar a los estados de la información de sus víctimas.
- ***El Procurador General Estatal (en inglés)*** para cada estado del cual usted prepare declaraciones. La mayoría de los estados requieren que el Procurador General sea notificado de las filtraciones de datos.

Comuníquese con los expertos:

- Experto en Seguridad – para determinar la causa y el alcance de la filtración, para detenerla y prevenir que ocurran más filtraciones.
- Compañía de seguros – para informar de la filtración y para verificar si su póliza de seguro cubre los gastos de mitigación de la filtración de datos.

Para obtener una lista completa, vea ***Data Theft Information for Tax Professionals*** (Información sobre el robo de datos para los profesionales de impuestos), en inglés.

Manténgase conectado

El *IRS* intenta alertar a los profesionales de impuestos lo más rápido posible cuando se entera de una nueva estafa, que son especialmente comunes durante la temporada de presentación de impuestos. Inscríbase para que pueda mantenerse al día con las últimas alertas y los problemas de la administración tributaria:

- ***e-News for Tax Professionals (Boletín electrónico para los Profesionales de Impuestos), en inglés*** – Un resumen semanal de noticias tributarias importantes dirigidas a los preparadores de impuestos
- ***QuickAlerts (en inglés)*** – Un sistema de mensajería urgente sobre *e-File* para los profesionales de impuestos que tienen cuentas de servicios electrónicos.
- ***Medios sociales del IRS*** – El *IRS* utiliza varios medios sociales para conectarse con los profesionales de impuestos y con los contribuyentes. Puede seguirnos en:
  - *Twitter.com/IRStaxpros.*
  - *Twitter.com/IRSnews.*
  - *Facebook.com/IRStaxpros.*

Marcadores de Seguridad del *IRS*

- ***Protección de Identidad: Prevención, Detección y Asistencia a las Víctimas*** – Página principal sobre el robo de identidad
- ***Información sobre el Robo de Datos para los Profesionales de Impuestos (en inglés)*** – Cómo informar al *IRS* la pérdida de datos de los clientes
- ***Proteja a sus clientes; Protéjase a sí mismo*** – Campaña de concientización y alertas de estafas para los profesionales de impuestos
- ***Impuestos. Seguridad. Unidos.*** – Campaña de concientización para los contribuyentes
- ***Información sobre el Robo de Identidad para los Profesionales de Impuestos (en inglés)*** – Resumen general
- ***Informe de Phishing y Estafas en Línea*** – Cómo informar sobre las estafas relacionadas con el *IRS*
- ***Cómo funciona la Asistencia del IRS a las Víctimas de Robo de Identidad*** – Lo que los clientes pueden esperar
- ***Mantener, Vigilar y Proteger su EFIN (en inglés)*** – Proteja sus números de identificación emitidos por el *IRS*
- ***Acceso Seguro*** – Cómo verificar su identidad para acceder a las herramientas en línea del *IRS*
- ***Cumbre de Seguridad*** – Haga un seguimiento de las protecciones promulgadas por el IRS, los estados y la industria
- ***Noticias en español*** – Manténgase informado al inscribirse a los comunicados de prensa del *IRS*
- ***Enlaces de Contacto Local con las Partes Interesadas (en inglés)*** – Encuentre su contacto local para informar la pérdida de datos