IRS Nationwide Tax Forum 2020

Construyendo el Plan de Seguridad de Datos para sus Contribuyentes

IRS Nationwide Tax Forum 2020

Preguntas de Seguridad

1. ¿Cuántos en la audiencia creen que su software de presentación de impuestos tiene incorporado medidas de seguridad?

2. ¿Cuántos de ustedes saben si sus equipos tienen protección contra malware integrada en su software?

IRS Nationwide Tax Forum 2020

Objetivos de aprendizaje

Después de completar este seminario, usted será capaz de:

- ✓ Mejorar el conocimiento sobre la ciberseguridad y superar las lagunas de seguridad en su ordenador
- ✓ Establecer un plan de protección de seguridad de datos
- ✓ Aprenderá a proteger los planes y procesos de negocio y a proteger la información personal de los clientes
- ✓ Podrá sensibilizar sobre las amenazas emergentes de seguridad

IRS Nationwide Tax Forum 2020

Proteger los datos del contribuyente es la ley

La ley federal otorga a la Comisión Federal de Comercio la autoridad para establecer regulaciones de salvaguarda de datos para varias entidades, incluyendo preparadores profesionales de declaraciones de impuestos

- En virtud de la Regla de Salvaguardias, las instituciones financieras deben proteger la información de los consumidores que recopilan. La Ley Gramm-Leach-Bliley (GLB) exige que las empresas definidas por la ley como "instituciones financieras" garanticen la seguridad y confidencialidad de este tipo de información. La definición de "instituciones financieras" incluye preparadores de impuestos profesionales.
- La Regla de Salvaguardias requiere que las empresas desarrollen un plan de seguridad de la información por escrito que describa su programa para proteger la información de los clientes. El plan de seguridad de la información requerido debe ser adecuado al tamaño y complejidad de la empresa, la naturaleza y el alcance de sus actividades y la sensibilidad de la información del cliente que maneja.

IRS Nationwide Tax Forum 2020

Estadísticas de Crimes Cibernéticos

- El robo cibernético es el delito de más rápido crecimiento en los Estados Unidos y le costó a la economía global casi $600 mil millones, con casi dos tercios de las personas que utilizan servicios en línea (más de 2 mil millones) de registros personales robados.
- Para 2021, el costo de los daños a la ciberdelincuencia podría alcanzar los 6 billones de dólares anuales, según un informe de CyberSecurity Ventures
- Las 5 industrias más atacadas cibernéticamente en los últimos 5 años son la atención médica, la manufactura, los servicios financieros, el gobierno y el transporte.
- Para la temporada 2018 de preparación de impuestos, el 59% de los profesionales de impuestos dijeron que uno o más de sus clientes fueron víctimas de robo de identidad fiscal durante el año.

IRS Nationwide Tax Forum | 2020

¿Cuál es el riesgo?

IRS Nationwide Tax Forum 2020

Que amenaza la información empresarial

- Uso indebido
- Desastres
- Intercepción de datos
- Robo de computadoras
- Identidad/Robo de contraseña
- Software malicioso
- Robo de datos/corrupción
- Vandalismo
- Error humano

IRS Nationwide Tax Forum | 2020

Consejos de seguridad cibernética para empresas

- Capacitar a los empleados en principios de seguridad
- Proteja la información, los ordenadores y las redes de los Ataques
- Proporcione seguridad de firewall para su conexión a Internet
- Crear un plan de acción móvil
- Haga copias de seguridad de datos empresariales importantes y Información

IRS Nationwide Tax Forum 2020

Consejos de seguridad cibernética para empresas

- Controle el acceso físico a los equipos y cree cuentas de usuario para cada empleado.
- Proteja sus redes Wi-Fi
- Emplear las mejores prácticas en tarjetas de pago
- Limite el acceso de los empleados a los datos y la información, y limitar la autoridad para instalar software.
- Contraseñas y autenticación

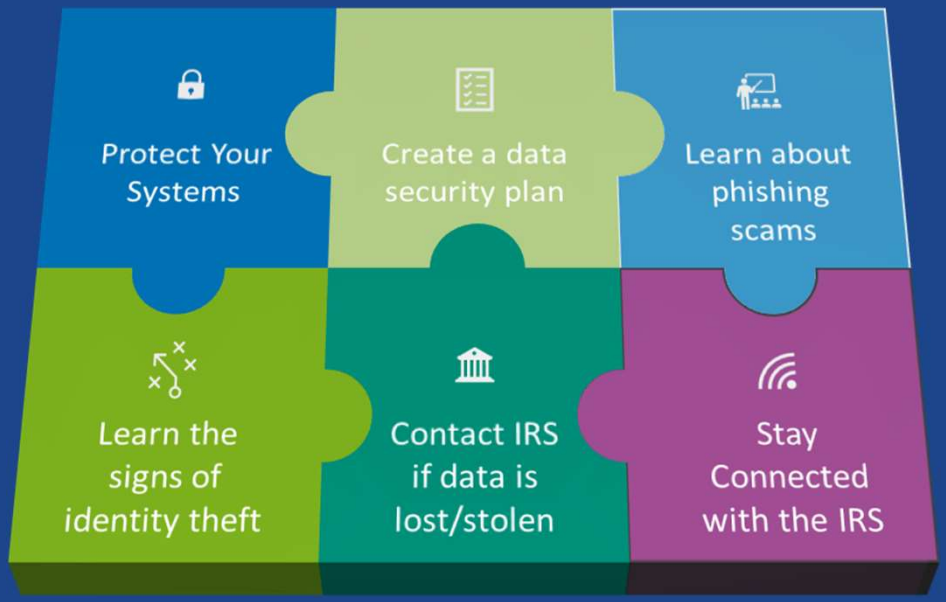
IRS Nationwide Tax Forum | 2020

Poniéndolo Todo Junto

IRS Nationwide Tax Forum | 2020

La lista de verificación "Impuestos-Seguridad-Juntos"

- Los socios de la Cumbre de Seguridad del IRS instan a la comunidad tributaria a revisar estos pasos básicos de seguridad.



IRS Nationwide Tax Forum 2020

FTC: Ciberseguridad para las pequeñas empresas

PROTECT
YOUR FILES & DEVICES

Update your software

This includes your apps, web browsers, and operating systems. Set updates to happen automatically.

Secure your files

Back up important files offline, on an external hard drive, or in the cloud. Make sure you store your paper files securely, too.

Require passwords

Use passwords for all laptops, tablets, and smartphones. Don't leave these devices unattended in public places.

Encrypt devices

Encrypt devices and other media that contain sensitive personal information. This includes laptops, tablets, smartphones, removable drives, backup tapes, and cloud storage solutions.

Use multi-factor authentication

Require multi-factor authentication to access areas of your network with sensitive information. This requires additional steps beyond logging in with a password — like a temporary code on a smartphone or a key that's inserted into a computer.

Require strong passwords

A strong password is at least 12 characters that are a mix of numbers, symbols, and capital lowercase letters.

Never reuse passwords and don't share them on the phone, in texts, or by email.

Limit the number of unsuccessful log-in attempts to limit password-guessing attacks.

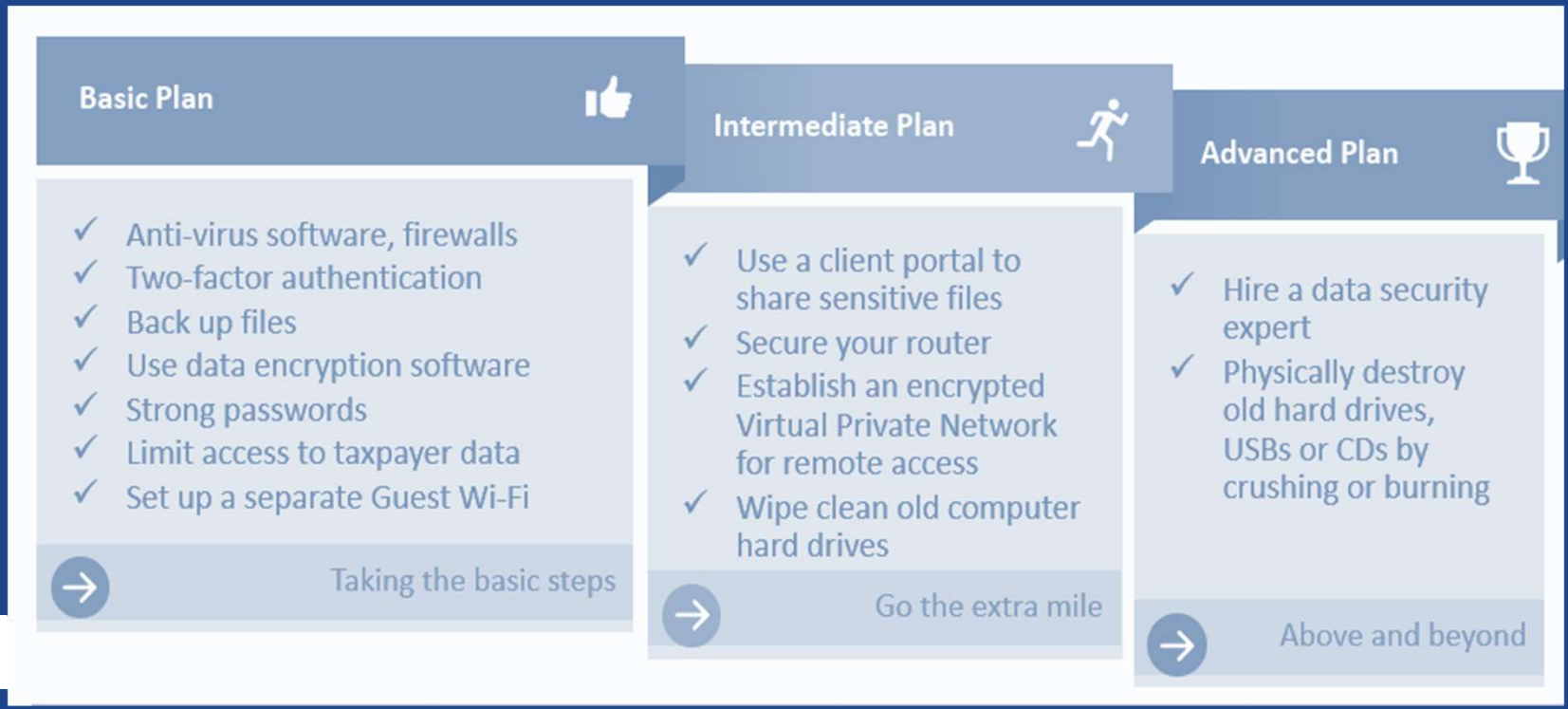
IRS Nationwide Tax Forum 2020

Recursos de ciberseguridad para profesionales de impuestos

- Publication 4557, Safeguarding Taxpayer Data
- Publication 5293, Data Security Resource Guide
- Publication 4524, Security Awareness For Taxpayers (PDF)
- Protect Your Clients; Protect Yourself: Tax Security 101
- Tax Security 2.0 The Taxes-Security-Together Checklist
- FTC Cybersecurity for Small Business
- Basic Security Steps/Signs of Data Loss
- Data Theft Information for Tax Professionals
- Identity Theft Information for Tax Professionals
- Publication 5199, Tax Preparer Guide to Identity Theft (PDF)
- Tax Practitioner Guide to Business Identity Theft
- Publication 4600, Safeguarding Taxpayer Information: Quick Reference Guide for Business

IRS Nationwide Tax Forum 2020

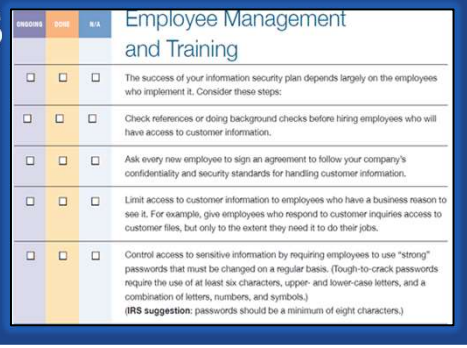
Proteja sus sistemas



Utilice la lista de verificación de reglas de seguridad

IRS Publication 4557

- La Regla de Salvaguardas requiere que las empresas evalúen y aborden los riesgos para la información de los clientes en todas las áreas de su operación, incluidas tres áreas que son particularmente importantes para la seguridad de la información:
- ▪ Gestión y Capacitación de Empleados
- Sistemas de información ▪
- ▪ Sistema de Detección y Gestión
- Fallas



ONGOING	DONE	N/A	Employee Management and Training
☐	☐	☐	The success of your information security plan depends largely on the employees who implement it. Consider these steps:
☐	☐	☐	Check references or doing background checks before hiring employees who will have access to customer information.
☐	☐	☐	Ask every new employee to sign an agreement to follow your company's confidentiality and security standards for handling customer information.
☐	☐	☐	Limit access to customer information to employees who have a business reason to see it. For example, give employees who respond to customer inquiries access to customer files, but only to the extent they need it to do their jobs.
☐	☐	☐	Control access to sensitive information by requiring employees to use "strong" passwords that must be changed on a regular basis. (Tough-to-crack passwords require the use of at least six characters, upper- and lower-case letters, and a combination of letters, numbers, and symbols.) **(IRS suggestion:** passwords should be a minimum of eight characters.)

IRS Nationwide Tax Forum 2020

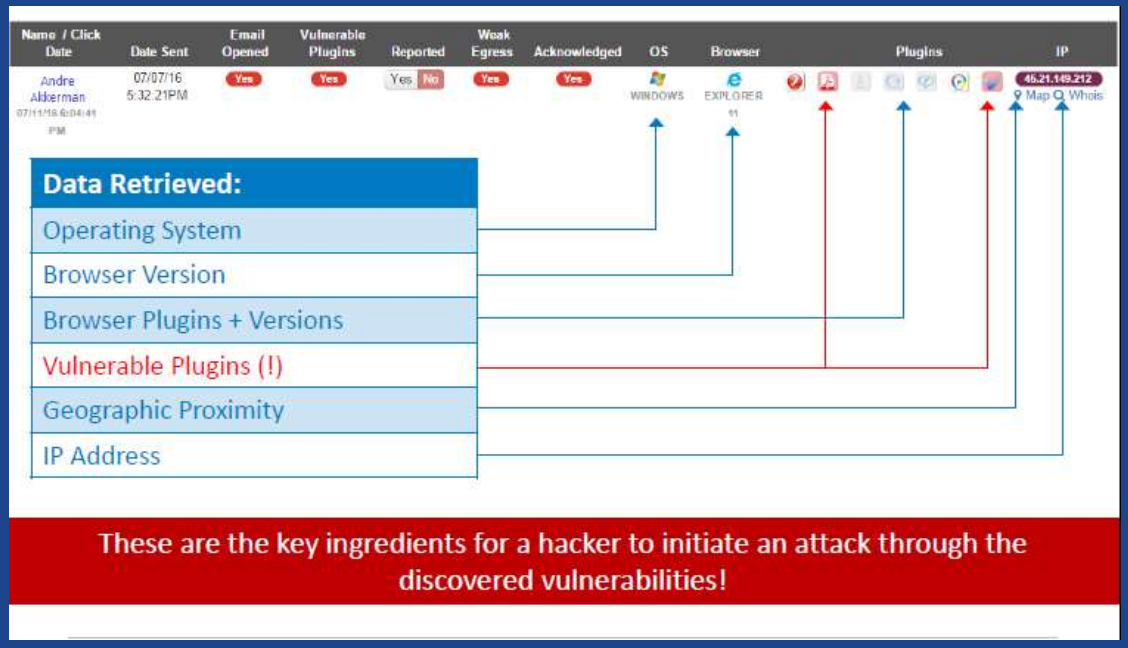
Crear un Plan de Seguridad de Data

IRS Nationwide Tax Forum | 2020

Protéjase de los ataques de Correos Electrónicos

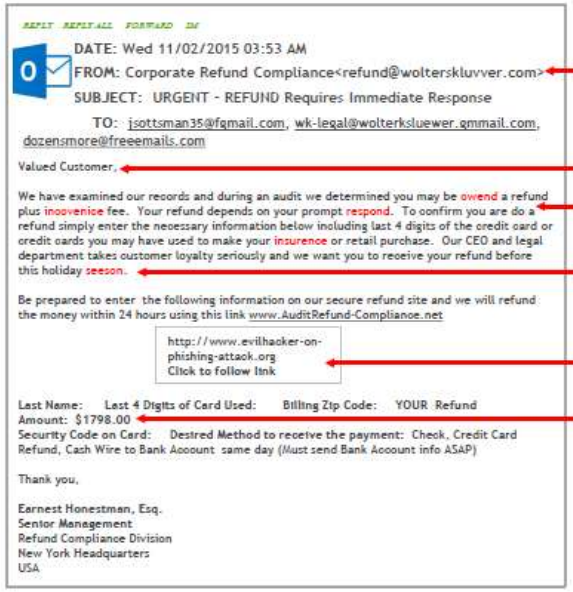
IRS Nationwide Tax Forum 2020

Que se puede recuperar con este clic de un ratón...



IRS Nationwide Tax Forum 2020

Phishing – ¡Que No te atrapen!



REPLY REPLY ALL FORWARD IM

DATE: Wed 11/02/2015 03:53 AM

FROM: Corporate Refund Compliance<refund@wolterskluver.com>

SUBJECT: URGENT - REFUND Requires Immediate Response

TO: jsottsman35@fgmail.com, wk-legal@wolterksluewer.gmmail.com, dozensmore@freeemails.com

Valued Customer,

We have examined our records and during an audit we determined you may be owend a refund plus inoovenice fee. Your refund depends on your prompt respond. To confirm you are do a refund simply enter the neoessary information below inoluding last 4 digits of the oredit oard or oredit oards you may have used to make your insurence or retail purchase. Our CEO and legal department takes customer loyalty seriously and we want you to reoeive your refund before this holiday seeson.

Be prepared to enter the following information on our secure refund site and we will refund the money within 24 hours using this link www.AuditRefund-Compliance.net

http://www.evilhacker-on-phishing-attack.org
Click to follow link

Last Name: Last 4 Digits of Card Used: Billing Zip Code: YOUR Refund Amount: $1798.00
Security Code on Card: Desired Method to receive the payment: Check, Credit Card Refund, Cash Wire to Bank Account same day (Must send Bank Account info ASAP)

Thank you,

Earnest Honestman, Esq.
Senior Management
Refund Compliance Division
New York Headquarters
USA

Validate the SENDER's e-mail Address
If the NAME of the Sender is a legitimate organization but the actual FROM email address is a personal email such as @hotmail.com, or @yahoo.com it is most likely a phishing attack.

Generic Greeting
If a trusted organization needs to contact you they should address you by name.

Read the Message Content
If the message is unexpected or irrelevant to your work or personal matters, do not open attachments or click on any links.

Consider Grammar and Spelling
Be suspicious of grammar and spelling errors; professionals and organizations carefully proofread messages before sending them.

Examine the Links
Before clicking, hover your mouse over the link to reveal the actual destination. If the destination is different from what's written, this may very likely be an attack.

Too Good To Be True
Be suspicious of lottery winning or wealth inheritance "Notification Messages". Most "too good to be true" messages are Phishing Attacks.

IRS Nationwide Tax Forum | 2020

Ejemplo de Correo de Phishing

From: Wells Fargo <Ruedi.Klein@t-online.de>
Date: September 18, 2018 at 2:50:44 PM EDT
To: "no-reply@wellsfargoalert.com" <no-reply@wellsfargoalert.com>
Subject: Your Debit Card Transactions Refund
Reply-To: Wells Fargo <Ruedi.Klein@t-online.de>

Dear Valued Customer,

We discovered a duplicate charges on your recent transactions and a refund process has been initiated. We require some additional information to proceed with your refund. Please logon to https://wellsfargo/refund/wellsfargo.com to enable us complete your refund process.

Wells Fargo Security | Terms of Use 2018

Your privacy is important to us. Wells Fargo Privacy Operations,
270 Park Avenue New York,NY 10017 U.S© 2017 Wells Fargo & Company.

https://goldenlikecourier.com/LoginWellso/index.php

From: admin@reply8647.user.ebaybid.com
Date: Wednesday, October 11, 2006 7:50 AM
To: @hotmail.com
Subject: RE: Alert Message 99820565515184

1. Questionable Sender's Address

eBay sent this message originated from eBay.
Your registered (member).
Learn more.

2. Sense of Urgency

Hurry! Message for @hotmail.com. Update Now!

Dear @hotmail.com,

We are contacting you to remind you that on 10 OCT 2006 we identified some unusual activity in your account coming from a foreign IP address: 201.8.43.167 (IP address located in China) . We have been notified that a card associated with your account has been reported as lost or stolen and involved in fraudulent transactions, or that there were additional problems with your card.

3. Non-US Dating Format

According to our site policy you will have to confirm that you are the real owner of the eBay account by completing the following form or else your account will be marked as fraudulent , and will remain open for investigation. You will pay for the fees wich will result from the financial transactions between eBay and FIT (Fraud Investigations Team) .

4. Threat!

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&co_partnerId=2&pUserId=&siteid=0&pageType=&pa1=&i1=&bshowgif=&UsingSSL=yes

eBay's Privacy Policy and Law Enforcement Disclosure: We care deeply about the privacy of the eBay community and will protect the privacy of our members even while working closely with law enforcement to prevent criminal activity. To learn more about how we protect your privacy, please visit eBay's Privacy Central for more information.

5. Link & URL in Status Bar Doesn't Match

http://user47id.com/.../

IRS Nationwide Tax Forum 2020

Infórmese Sobre las Estafas de Phishing

- Más del 90% de todos los robos de datos comienzan con un correo electrónico de phishing.
- El IRS a menudo ve a los profesionales de impuestos victimizados después de ser atacados con una táctica llamada “spear phishing”.
- Estafas comunes de phishing son vistas por el IRS incluyen ladrones haciéndose pasar por clientes potenciales, enviando correos electrónicos no solicitados a profesionales de impuestos.
- Un archivo adjunto de correo electrónico de phishing puede contener software malicioso llamado “keylogging”, que infecta secretamente los ordenadores y proporciona al ladrón la capacidad de ver cada pulsación de tecla.
- El IRS también ha visto ladrones que se hacen pasar por proveedores de software de impuestos o proveedores de almacenamiento de datos con correos electrónicos que contienen enlaces que van a páginas web que reflejan sitios reales.

IRS Nationwide Tax Forum 2020

Pongamos a prueba sus conocimientos

¿Cuál de estas declaraciones es correcta?

a) Si recibe un correo electrónico que parece de alguien que conoce, puede hacer clic en cualquier enlace siempre y cuando tenga un bloqueador de spam y protección antivirus.

b) Puede confiar en que un correo electrónico realmente proviene de un cliente si utiliza el logotipo del cliente y contiene al menos un hecho sobre el cliente que usted sabe que es verdadero.

c) Si recibe un mensaje de un colega que necesita su contraseña de red, nunca debe darlo a menos que el colega diga que es una emergencia.

d) Si recibe un correo electrónico de un familiar pidiéndole que proporcione información personal de inmediato, debe comprobarlo primero para asegurarse de que son quienes dicen ser.

IRS Nationwide Tax Forum 2020

Evitar estafas de phishing

Basic Plan

- ✓ Use separate personal and business email accounts
- ✓ Use two-factor authentication
- ✓ Keep your web browser software up to date so that it has the latest security features
- ✓ Never open or download attachments from unknown senders

Taking the basic steps

Intermediate Plan

- ✓ Install an anti-phishing tool bar to help identify known phishing sites
- ✓ Avoid accessing business emails or information from public wi-fi connections

Go the extra mile

Advanced Plan

- ✓ Disable stored password feature offered by some operating systems
- ✓ If IRS-related, forward suspicious or unknown emails to phishing@irs.gov

Above and beyond

IRS Nationwide Tax Forum 2020

RANSOMWARE

IRS Nationwide Tax Forum | 2020

Monitor EFIN/PTINs

Los preparadores de impuestos que son abogados, CPAs, agentes inscritos o participantes del Programa anual de temporada de presentación, y que presentan 50 o más declaraciones pueden obtener un informe semanal del número de declaraciones de impuestos presentadas con su EFIN o PTIN.

For EFIN totals:

- Acceda a su cuenta de e-Services y a su aplicación EFIN;
- Seleccione "Estado EFIN" en la aplicación;
- Comuníquese con el servicio de asistencia electrónica del IRS si los totales de devolución superan el número de devoluciones que ha presentado.

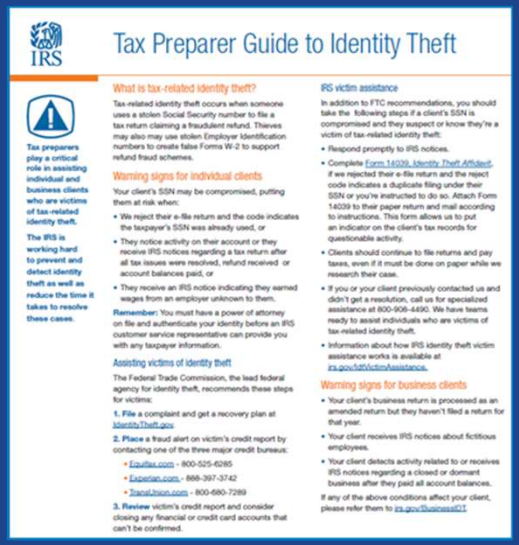
Para totales de PTIN

- Acceder a su cuenta PTIN en línea;
- Seleccione "Ver devoluciones archivadas por PTIN;“
- Complete el Formulario 14157, Queja: Preparador de Declaraciones de Impuestos, para reportar el uso excesivo o mal uso de PTIN.

IRS Nationwide Tax Forum | 2020

Educar a sus clientes

IRS Pub 5199: Tax Preparer Guide to Identity Theft
IRS Pub 4524: Security Awareness for Taxpayers



IRS

Tax Preparer Guide to Identity Theft

Tax preparers play a critical role in assisting individual and business clients who are victims of tax-related identity theft.

The IRS is working hard to prevent and detect identity theft as well as reduce the time it takes to resolve these cases.

What is tax-related identity theft?

Tax-related identity theft occurs when someone uses a stolen Social Security number to file a tax return claiming a fraudulent refund. Thieves may also may use stolen Employer Identification numbers to create false Forms W-2 to support refund fraud schemes.

Warning signs for individual clients

Your client's SSN may be compromised, putting them at risk when:

- We reject their e-file return and the code indicates the taxpayer's SSN was already used, or
- They notice activity on their account or they receive IRS notices regarding a tax return after all tax issues were resolved, refund received or account balances paid, or
- They receive an IRS notice indicating they earned wages from an employer unknown to them.

Remember: You must have a power of attorney on file and authenticate your identity before an IRS customer service representative can provide you with any taxpayer information.

Assisting victims of identity theft

The Federal Trade Commission, the lead federal agency for identity theft, recommends these steps for victims:

1. File a complaint and get a recovery plan at IdentityTheft.gov.

2. Place a fraud alert on victim's credit report by contacting one of the three major credit bureaus:

- Equifax.com - 800-525-6285
- Experian.com - 888-397-3742
- TransUnion.com - 800-680-7289

3. Review victim's credit report and consider closing any financial or credit card accounts that can't be confirmed.

IRS victim assistance

In addition to FTC recommendations, you should take the following steps if a client's SSN is compromised and they suspect or know they're a victim of tax-related identity theft:

- Respond promptly to IRS notices.
- Complete Form 14039, *Identity Theft Affidavit*, if we rejected their e-file return and the reject code indicates a duplicate filing under their SSN or you're instructed to do so. Attach Form 14039 to their paper return and mail according to instructions. This form allows us to put an indicator on the client's tax records for questionable activity.
- Clients should continue to file returns and pay taxes, even if it must be done on paper while we research their case.
- If you or your client previously contacted us and didn't get a resolution, call us for specialized assistance at 800-908-4490. We have teams ready to assist individuals who are victims of tax-related identity theft.
- Information about how IRS identity theft victim assistance works is available at irs.gov/Individuals/Identity-Protection.

Warning signs for business clients

- Your client's business return is processed as an amended return but they haven't filed a return for that year.
- Your client receives IRS notices about fictitious employees.
- Your client detects activity related to or receives IRS notices regarding a closed or dormant business after they paid all account balances.

If any of the above conditions affect your client, please refer them to irs.gov/BusinessID1T.

IRS

Security Awareness For Taxpayers

TAXES. SECURITY. TOGETHER.

The IRS, the states and the tax industry are committed to protecting you from identity theft. We've strengthened our partnership to fight a common enemy – the criminals – and to devote ourselves to a common goal – serving you. Working together, we've made many changes to combat identity theft, and we are making progress. However, cybercriminals are constantly evolving, and so must we. The IRS is working hand-in-hand with your state revenue officials, your tax software provider and your tax preparer. But, we need your help. We need you to join with us. By taking a few simple steps, you can better protect your personal and financial data online and at home.

Please consider these steps to protect yourselves from identity thieves:

Keep Your Computer Secure

- Use security software and make sure it updates automatically; essential tools include:
  - Firewall
  - Virus/malware protection
  - File encryption for sensitive data
- Treat your personal information like cash, don't leave it lying around
- Check out companies to find out who you're really dealing with
- Give personal information only over encrypted websites – look for "https" addresses.
- Use strong passwords and protect them
- Back up your files

Avoid Phishing and Malware

- Avoid phishing emails, texts or calls that appear to be from the IRS and companies you know and trust, go directly to their websites instead
- Don't open attachments in emails unless you know who sent it and what it is
- Download and install software only from websites you know and trust
- Use a pop-up blocker
- Talk to your family about safe computing

Protect Personal Information

Don't routinely carry your social security card or documents with your SSN. Do not overshare personal information on social media. Information about past addresses, a new car, a new home and your children help identity thieves pose as you. Keep old tax returns and tax records under lock and key or encrypted if electronic. Shred tax documents before trashing.

Avoid IRS Impersonators. The IRS will not call you with threats of jail or lawsuits. The IRS will not send you an unsolicited email suggesting you have a refund or that you need to update your account. The IRS will not request any sensitive information online. These are all scams, and they are persistent. Don't fall for them. Forward IRS-related scam emails to phishing@irs.gov. Report IRS-impersonation telephone calls at www.tigta.gov.

Additional steps:

- Check your credit report annually; check your bank and credit card statements often;
- Review your Social Security Administration records annually: Sign up for My Social Security at www.ssa.gov.
- If you are an identity theft victim whose tax account is affected, review www.irs.gov/identitytheft for details.

Publication 4524 (Rev. 9-2015) Catalog Number 48359Q Department of the Treasury **Internal Revenue Service** www.irs.gov

IRS Nationwide Tax Forum 2020

Comuníquese con el IRS si los datos se pierden/roban

IRS Nationwide Tax Forum 2020

Comuníquese con el IRS si los datos se pierden/roban

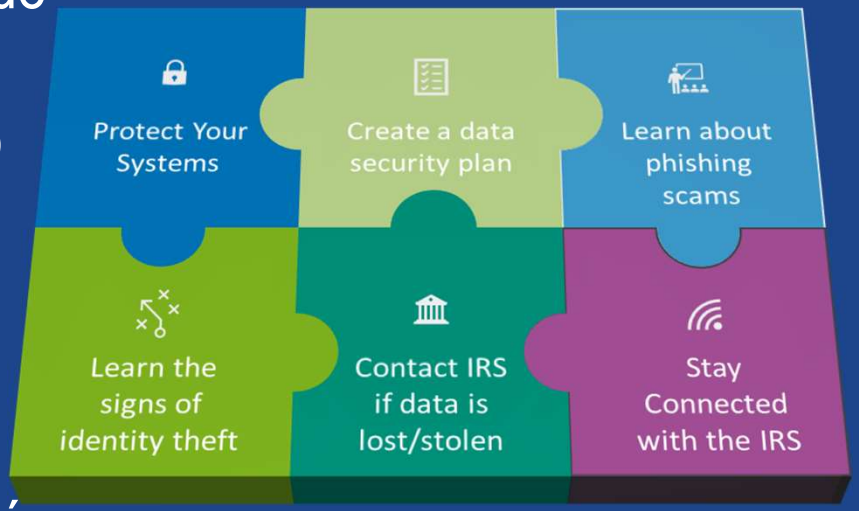
- ✓ **Comuniquese con IRS Stakeholder Liasion cuando se detecte una intrusion**
  - ✓ Stakeholder referirá la información dentro del IRS
- ✓ **Siga los requisitos de informes estatales**
  - ✓ (i.e. State Attorney General, State Consumer Protection Bureaus, State Police)
- ✓ **Reportar el incidente al FBI, Servicio Secreto de EE.UU., Comisión Federal de Comercio**

Source: IRS Pub. 4557; www.nist.gov/cyberframework

IRS Nationwide Tax Forum 2020

La lista de verificación "Impuestos-Seguridad-Juntos"

- ✓ Mantenga su software actualizado
- ✓ Adiestre a su personal
- ✓ Configura un Wi-Fi para invitado
- ✓ Revise la Pub. 4557 del IRS
- ✓ Utilice contraseñas seguras
- ✓ Cifrar archivos
- ✓ Crear y mantener un plan de seguridad de datos de información por escrito



IRS Nationwide Tax Forum 2020

Seguridad de los datos: ¿es la nube más segura?

- **Seguridad integrada:** el software basado en la nube limita la necesidad de supervisar y mantener constantemente los servidores locales
- **Almacenamiento de datos y copia de seguridad**: facilidad de acceso, recuperación de datos, costos flexibles
- **Cifrado de datos:** muchos proveedores de software basados en la nube utilizan varias capas de cifrado de datos para proteger la información del usuario.
- **Autenticación de dos factores:** añade una capa adicional de protección más allá de una contraseña

IRS Nationwide Tax Forum | 2020

Recursos

- **Publicaciones**
  - Publ. 4557, Safeguarding Taxpayer Data
  - Publ. 4524 Security Awareness for Taxpayers
  - Publ. 5293, Protect Your Clients; Protect Yourself
- **Tax Tips** (https://www.irs.gov/uac/irs-security-awareness-ta-tips)
  - Safeguarding Taxpayer Data: Create Strong Passwords
  - What to do If You Suffer a data Breach or Other Security Incident
- **References:**

- https://www.dhs.gov/sites/default/files/publications/FCC%20Small%20Biz%20Tip%20Sheet_0.pdf
- https://www.irs.gov/identity-theft-central