



Data Security Requirements for Tax Professionals

Richard Furlong, Jr.
Senior Stakeholder Liaison

Leslie Chambers
Senior Stakeholder Liaison

**48th Annual Delaware Federal and State Tax Institute
December 10, 2024**



Can you feel it in the air?

It's the time of year
when Tax Pros
begin renewing
their Preparer
Tax ID Numbers.



It's PTIN renewal season. Get started at:



irs.gov/ptin



Communications & Liaison STAKEHOLDER LIAISON



No time like
the *present* to
get ready for
tax season.

irs.gov/getready





Communications & Liaison STAKEHOLDER LIAISON



**Time waits for
snowman.
Get ready
now for
a smooth
filing season.**

irs.gov/getready





**Getting ready
for tax season
now will save
you time tater.**



IRS *irs.gov/getready*



Tax Professional Data Breaches and How Tax Pros Can Protect Themselves



Spear-phishing Scams Targeting Tax Professionals



Current Data Breach Statistics

The recent Verizon Data Breach Investigations Report (DBIR) found:

“82% of breaches involved a human element” (e.g.,

Phishing, Misuse, or Error)

Phishing was one of the four main entry points into an organization

The recent Internet Crime Complaint Center (IC3) report Phishing/Vishing/Smishing/Pharming was listed as a Top 5 Crime Type reported over the last five (5) years



The most common schemes that target tax professionals are:

- **spear phishing**
- **ransomware**
- **unauthorized access**



Phishing Lifecycle

A Lure: enticing email content

A Hook: an email-based exploit (e.g., a phishing URL or malicious attachment)

A Catch: a transaction conducted by an actor following a successful attempt



“New Client” Scam 1st Email

From: [REMOVED]

To: [TAX PREPARER]

Sent: Thu, Apr 21, 2024 3:06 pm

Subject: Extension Client Intake

Good Morning,

I am [REMOVED], married, father of three teenage boys and a business owner. My family and I have lagged behind in filing our taxes and I am hoping you are not at capacity and willing to take on a new client? I have all by books and forms in place, don't owe taxes and usually make estimated tax payments.

Please write back if you are open to new tax clients and how to proceed. Regards[REMOVED]



“New Client” Scam 2nd Email

From: [REMOVED]

To: [TAX PREPARER]

Sent: Wed, May 4, 2022 6:14 am

Subject: Re: Extension Client Intake

Hi [TAX PREPARER], Sorry for the late response, things haven't been going as planned lately. I won't want to bore you with personal issues. As for my taxes, I usually don't owe taxes, applied my prior year refund and also made estimated tax payments to cushion effects of situations like these.

****[REMOVED]_1040_ScanCopy.pdf***

<hxxps://example[.]example/file/[REMOVED]>*

Above is a secure and SSL excerpted copy of my prior year returns for your perusal. Kindly review and advise on way forward... I look forward to talking with you.Regards[REMOVED]



IRS-themed Phishing Email

From: IRSOffice <noreply.mailadmin@prwire360.com>

Date: November 23, 2021 at 6:29:11 AM CST

To:

Subject: Re: You are eligible to receive a tax status on Nov 23, 12:29:02 pm.



Third Round of Economic Impact Payments Status Available.

After the last annual calculations of your fiscal activity we have determined that you are eligible to receive a payment of \$532.00

We understand the challenges your business is facing due to the massive disruption caused by the Coronavirus (COVID-19) pandemic and want to provide you with funds to help you weather these difficult times.

Please click below to submit your application.

[Get Started](#)

Questions? We're here to help. Call us at 1-800-659-2955 | TTY/TDD: 1-800-877-8339 Office of Disaster Assistance U.S. Small Business Administration





Spear Phishing

Targets a specific audience

Appears as a familiar or trusted contact:

- **Fellow tax practitioner**
- **Tax software provider**
- **Potential or current client**

The goal is to convince you to open a URL or download an attachment



Account Takeover (cont.)

An official website of the United States Government



Help

News

English



Charities & Nonprofits



Tax Pros

File

Pay

Refunds

Credits & Deductions

Forms & Instructions

Search



[Home](#) / [News](#) / [News Releases](#) / Latest spearphishing scams target tax professionals

Latest spearphishing scams target tax professionals

English | [Español](#) | [中文\(简体\)](#)

Topics in the News

News Releases

News Releases for Frequently Asked Questions

Multimedia Center

Tax Relief in Disaster Situations

IR-2022-36, February 16, 2022

WASHINGTON — With tax season in full swing, the Internal Revenue Service, state tax agencies and tax industry today warned tax professionals of new email scams that attempt to steal their tax software preparation credentials.

The Security Summit partners warned these scams serve as a reminder that [tax professionals](#) remain prime targets for thieves. These thieves try to steal client data and tax preparers' identities in an attempt to file fraudulent tax returns for refunds.

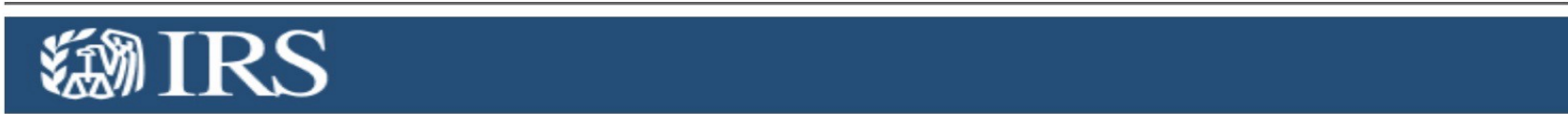
The latest phishing email uses the IRS logo and a variety of subject lines such as "Action Required: Your account has now been put on hold." The IRS has observed similar bogus emails that claim to be from a "tax preparation application provider." One such variation offers an "unusual activity report" and a solution link for the recipient to restore their account.

"Scams continue to evolve, and this one is especially sinister since it threatens tax professional's accounts," said IRS



“Account on hold” Phishing Email

Subject: Action Required: Your account is on hold (TXP099497)
From: "IRS.gov" <notification_taxpro.irs.gov@spoe-essling.at>
Date: Thu, February 03, 2022 7:16 pm
To:



Your account has been put on hold

ALL tax preparers are required to apply a security feature to their Tax Pro account towards **2021 Tax Returns** processing.

- You have not updated your account

It is mandatory that you update your account immediately.

Please click <https://www.irs.gov/pro-service/Update.asp> to update your account now.

Important

Failure to update your account within the next 48 hours will lead to your account being terminated and be barred from filing tax returns claims for 2021 tax season. Your access will be restored once you have updated your details.

Sincerely,
[IRS.gov](https://www.irs.gov) eServices



“Account on hold” Phishing Website

An official website of the United States Government



[Español](#) | [Exit](#)

Please select your software below to get started





Ransomware

Wana Decrypt0r 2.0

Ooops, your files have been encrypted! English



Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send \$300 worth of bitcoin to this address:




Deploy the “Security Six” Protections

- 1. Anti-virus software**
- 2. Firewalls**
- 3. Two-factor authentication**
- 4. Backup software/services**
- 5. Drive encryption**
- 6. Virtual Private Network (VPN)**



Signs of Client Data Theft

Client e-filed returns begin to reject

Clients who haven't filed tax returns begin to receive authentication letters (5071C, 4883C, 5747C) from the IRS

Clients who haven't filed tax returns receive refunds





Clients/Practitioners receive tax transcripts that they did not request

Clients who created an IRS Online Services account are notified that their account was accessed or disabled

Another variation: Clients receive notice that an account was created in their names



Reporting Phishing Scams

IRS, Treasury and/or tax-related phishing scams:

Please send full email headers to phishing@irs.gov

If you click on a nefarious link, download a document, etc.: Contact Your Tax Software Provider

Tax preparers who experienced a data breach:

Contact Stakeholder Liaison (SL): (www.irs.gov search “Stakeholder Liaison”)

TIGTA.gov

FTC.gov or IdentityTheft.gov



Protect Your Business

**Publication 4557 (*Safeguarding Taxpayer Data*)
at [IRS.gov](https://www.irs.gov)**

***Small Business Information Security – The
Fundamentals* at [NIST.gov](https://www.nist.gov)**

Subscribe to e-News for Tax Professionals



IRS.gov websites:

www.irs.gov/newsroom/irs2goapp

www.irs.gov/ProtectYourClients

www.irs.gov/identity-theft-central

www.irs.gov/securitysummit



Multi-Factor Authentication



Sign Up

If you don't have an IRS username, go back and create an account.

[← BACK](#)

Log In

Already have a username? Welcome back!

Username



[LOG IN >](#)

[Forgot Username](#)

PTIN and FIRE users need a separate account in this system



Log In

Verify that your Site Image and Site Phrase below are correct. If the Site Image and Site Phrase are not correct, please do not proceed.

Your Site Image:



Your Site Phrase:

Maggie's Stuff

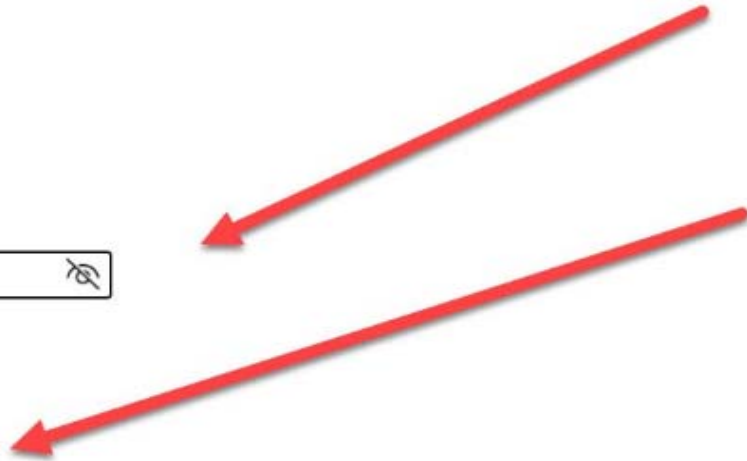
Password

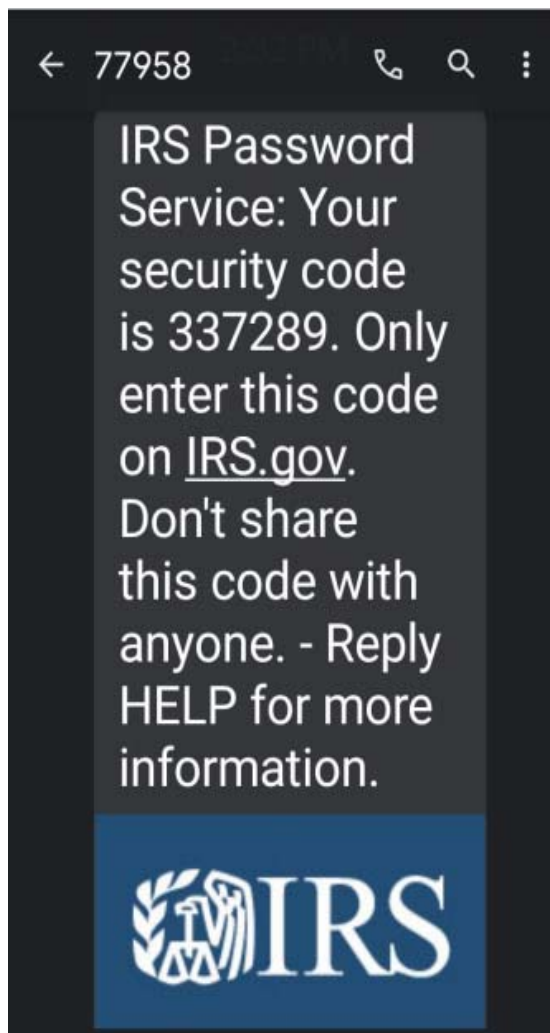
Your@password

[Forgot Password](#)

SUBMIT >

CANCEL







We sent a security code to your phone

We sent a text message to your phone (ending in 5200). Please enter the code below.

6-digit security code

[Resend Security Code](#)

[No longer have access to this phone?](#)

CONTINUE >

[If you can't get a text message right now, you can get a security code via phone call.](#)

[Logout](#)



Creating a Written Information Security Plan for your Tax & Accounting Practice



IRS Publication 5708



Creating a Written Information Security Plan (WISP) for your Tax & Accounting Practice

This document was prepared by the Security Summit, a partnership of the Internal Revenue Service, state tax agencies, private-sector tax groups as well as tax professionals. The mission of the Security Summit is to fight identity theft and tax refund fraud. •

This document is intended to provide sample information and to help tax professionals, particularly smaller practices, develop a Written Information Security Plan or WISP. It is not an exhaustive discussion of everything related to **WISPs** and it is not intended to replace your own research, to create reliance or serve as a substitute for developing your own plan based upon the specific needs and requirements of your business or firm. A written information security plan is just one part of what tax professionals need to protect their clients and themselves. Given the rapidly evolving nature of threats, the Summit also strongly encourages tax professionals to consult with technical experts to help with security issues and safeguard their systems.

There are many aspects to running a successful business in the tax preparation industry, including reviewing tax law changes, learning software updates, and managing and training staff. Creating a Written Information Security Plan or WISP is an often overlooked but critical component. Not only is a WISP essential for your business and a good business practice, the law requires you to have one. For many tax professionals, knowing where to start when developing a WISP is difficult. This guide provides multiple considerations necessary to create a security plan to protect your business, and your clients and comply with the law.



WISP - Outline

The bare essentials of a Written Information Security Plan are outlined below. Be sure you incorporate all the required elements in your plan, but scale the comprehensiveness to your firm's size and type of operation. The elements in the outline are there to provide your firm a narrower scope of purpose and define the limitations the document is meant to cover. Therefore, many elements also provide your firm with a level of basic legal protections in the event of a data breach incident. For a detailed explanation of each section, please review the detailed outline provided in this document.

- I. Define the WISP objectives, purpose, and scope**
- II. Identify responsible individuals**
 - a. List individuals who will coordinate the security programs as well as responsible persons.
 - b. List authorized users at your firm, their data access levels, and responsibilities.
- III. Assess Risks**
 - a. Identify Risks
 - List types of information your office handles
 - List potential areas for data loss (internal and external)
 - Outline procedures to monitor and test risks
- IV. Inventory Hardware**
 - a. List description and physical location of each item
 - b. Record types of information stored or processed by each item



Communications & Liaison STAKEHOLDER LIAISON



Basic Security Plan Considerations for Tax Professionals



- Know your customer information (names, addresses, email addresses, bank accounts/routing numbers)
- Have employee protocols
 - New hires (training, accesses, need to know)
 - Departing employees (physical and system accesses, keys/passwords/files/thumb drives)
- Protect passwords (length, upper case/lower case, numbers, special characters, phrases)
- Encrypt files and email; use anti-virus software and establish firewall protections
- Dispose properly (files, computers, printers, thumb drives)
- Know what your insurance covers and know who to contact in event of breach

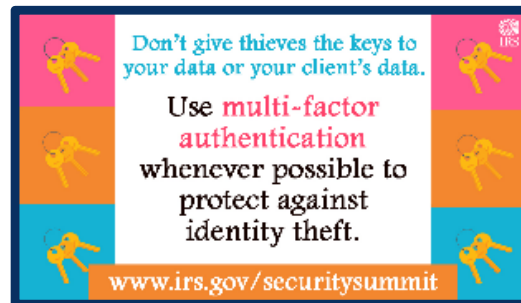
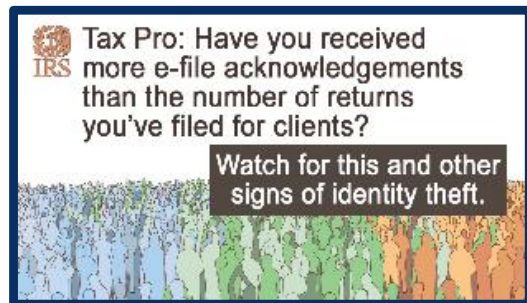
This document is not intended to be all inclusive, but as a starting point for security plan development. Security plans should be appropriate for the type and size of your business.



Data Breach/Ransomware Attacks

Reporting a Data Breach or Ransomware Attack

- Contact your local Stakeholder Liaison (SL)
 - Provide details promptly
- Follow the guidance from your SL, Pub 5293, Pub 4557 and the IRS Data Breach webpage
- Take steps to discover the cause of the attack
- Notify local and other federal agencies based on the type of attack





It's not luck: Fraudulent tax claims lead to penalties



Check with a tax pro before taking any social media tax advice.

irs.gov/scams  **IRS**



**Communication & Liaison
STAKEHOLDER LIAISON**

***National Security Awareness Week
December 2, 2024 – December 6, 2024***



Tax Scams, Identity Theft, Refund Fraud



STAY SAFE WHILE SHOPPING ONLINE

Avoid a holiday meltdown

Get tips to keep your data safe when shopping online from the IRS and Security Summit.

National Tax Security Awareness Week

 irs.gov/securitysummit



Shop only on secure sites

Use only secured networks

Update security software

Secure devices

Use malware stoppers and firewalls

Use strong, unique passwords


Use multi-factor authentication

2024 National Tax Security Awareness Week
www.irs.gov/NTSAW




STAY SAFE ON SOCIAL MEDIA

Wildly inaccurate tax advice often circulates on social media.



Following it has bad consequences.

 irs.gov/scams

#TaxSecurity

Follow IRS-verified social media accounts and e-news services

Don't provide personal or financial information

Verify eligibility for tax credits with a trusted tax professional

Use IRS.gov to fact check information

Stay aware of the latest scams by following @IRStaxsecurity on X

Pub 5461 Protect Personal and Financial Information Online

2024 National Tax Security Awareness Week
www.irs.gov/NTSAW



INDIVIDUALS STAY SAFE BY USING AN IDENTITY PROTECTION PIN (IP PIN)



Use an Identity Protection (IP) PIN when filing a tax return, including amended or prior year returns

The IRS will never ask you for your IP PIN

Protect your IP PIN and only share it with trusted tax software provider or tax preparer

Pub 5461-B Get an Identity Protection PIN

2024 National Tax Security Awareness Week
www.IRS.gov/NTSAW



BUSINESSES STAY SAFE BY SAFEGUARDING INFORMATION

Businesses, big and small, can help protect their employees, customers and enterprises.



#TaxSecurity
[irs.gov/securitysummit](https://www.irs.gov/securitysummit)

Pub 5461-C Businesses should watch out for tax-related scams and implement safeguards

2024 National Tax Security Awareness Week
www.irs.gov/NTSAW

Safeguard customer data by:

- Setting security software to update automatically
- Back up important files
- Require strong passwords with multi-factor authentication
- Encrypt all devices

Beware of phishing and impersonation schemes

Review tips in the business section of Identity Theft Central on [IRS.gov](https://www.irs.gov)



Tax Pros Stay Safe by having a WRITTEN INFORMATION SECURITY PLAN (WISP)

**Keep your data
away from thin ice.**

**Create and maintain
a strong Written
Information Security Plan.**

National #TaxSecurity Awareness Week

irs.gov/securitysummit

Pub 5461-D Tax professionals should review their security protocols

Pub 5461-F Review account details on secure portal

2024 National Tax Security Awareness Week
www.IRS.gov/NTSAW

Develop a written information security plan (WISP)

Use IRS Secure Online Tools (Tax Pro Account)

Use Multi-Factor Authentication

Know what to do if you have a data breach

Pub 5708 Creating a WISP



All that glitters isn't gold.

**Report scams
to the IRS.**

irs.gov/scams





e-News Subscriptions

IRS.gov/subscribe

The image shows two side-by-side screenshots of the IRS.gov website's e-News Subscriptions page. The left screenshot is in English, and the right is in Spanish. A red arrow points from the English page to the Spanish page, and another red arrow points from the Spanish page back to the English page. The English page has a red box around the 'English' language selector, and the Spanish page has a red box around the 'Español' language selector. The text 'in English' and 'in Spanish' are placed near their respective arrows. At the bottom, the text 'IRS.gov – keyword: e-News' is displayed.

in English

in Spanish

IRS.gov – keyword: e-News



IRS2Go Mobile App

IRS.gov/irs2go

IRS2Go is the official mobile app of the IRS

Check your refund status, make a payment, find free tax preparation assistance, sign up for helpful tax tips, and more!

IRS2Go is available in both English and Spanish.

Download IRS2Go for your mobile device



IRS2Go offers many features





Richard Furlong, Jr.

Senior Stakeholder Liaison

267-941-6343

richard.g.furlong@irs.gov