Communications & Liaison
STAKEHOLDER LIAISON

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

1

1

Communications & Liaison
STAKEHOLDER LIAISON

2

2

Communications & Liaison
STAKEHOLDER LIAISON

3

3

Communications & Liaison
STAKEHOLDER LIAISON

4

4

Communications & Liaison
STAKEHOLDER LIAISON

5

5

Communications & Liaison
STAKEHOLDER LIAISON

Tax Professional Data Breaches and How Tax Pros Can Protect Themselves

6

6

Spear-phishing Scams Targeting Tax Professionals

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

Common Schemes

The most common schemes that target tax professionals are:

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

9

9

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

10

10

"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]

11

11

"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]

12

12

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.

IRS

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 provid 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

Case-Custo...120.txt

13

13

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

14

14

Account Takeover (cont.)

15

15

"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:

IRS

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 acc|ount 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 48hours 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 eServices

16

16

"Account on hold" Phishing Website

17

17

Ransomware

18

18

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)

19

19

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

20

20

Signs of Client Data Theft – cont.

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

21

21

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

22

22

Protect Your Business

Publication 4557(*Safeguarding Taxpayer Data*) at IRS.gov

***Small Business Information Security – The Fundamentals* at NIST.gov**

Subscribe to e-News for Tax Professionals

23

23

Resources

IRS.gov websites:

www.irs.gov/newsroom/irs2goapp

www.irs.gov/ProtectYourClients

www.irs.gov/identity-theft-central

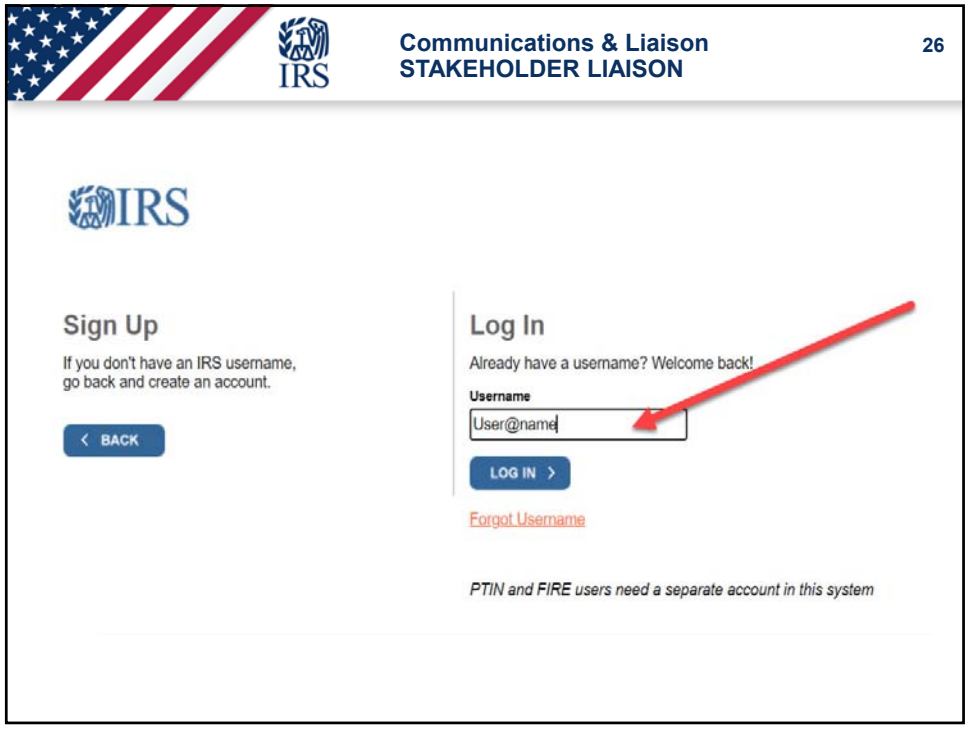
www.irs.gov/securitysummit

24

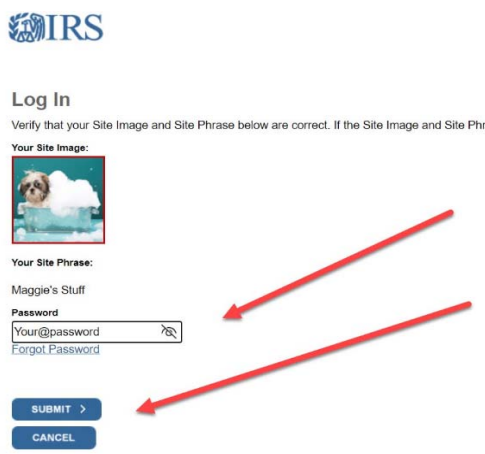
24

Multi-Factor Authentication

25



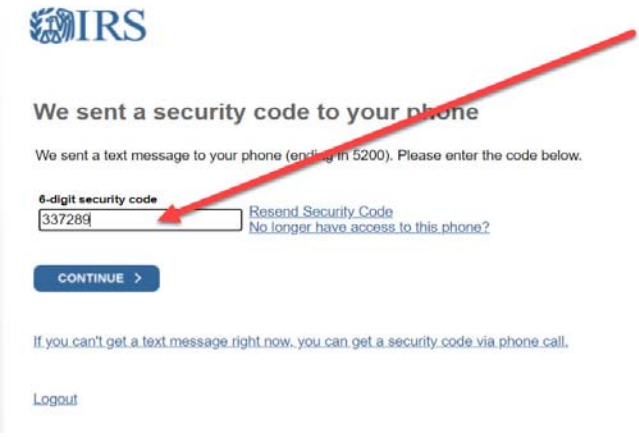
26


IRS
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

27


77958
IRS Password Service: Your security code is 337289. Only enter this code on IRS.gov. Don't share this code with anyone. - Reply HELP for more information.
IRS

28



29

IRS

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

IRS Publication 5708

30

30

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.

33

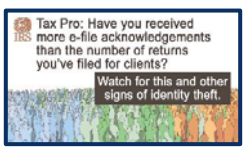
33

Communications & Liaison
STAKEHOLDER LIAISON

Data Breach/Ransomware Attacks

Reporting a Data Breach or Ransomware Attack

- Contact your local Stakeholder Liaison (SL)
  - o 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



34

34

Communications & Liaison
STAKEHOLDER LIAISON

35

35

Communication & Liaison
STAKEHOLDER LIAISON

National Security Awareness Week

December 2, 2024 – December 6, 2024

Tax Scams, Identity Theft, Refund Fraud

36

STAY SAFE WHILE SHOPPING ONLINE

- 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

37

STAY SAFE ON SOCIAL MEDIA

Pub 5461 Protect Personal and Financial Information Online

- 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

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

38

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

Pub 5461-B Get an Identity Protection PIN

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

- 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

39

BUSINESSES STAY SAFE BY SAFEGUARDING INFORMATION

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

40

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

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

41

Communications & Liaison STAKEHOLDER LIAISON

All that glitters isn't gold.

Report scams to the IRS.

irs.gov/scams

IRS

42

42

e-News Subscriptions

IRS.gov/subscribe

43

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

GET IT ON Google Play

Download on the App Store

Available at amazon

IRS2Go offers many features

44

Richard Furlong, Jr.

Senior Stakeholder Liaison

267-941-6343

richard.g.furlong@irs.gov