Protecting Your Clients and Your Practice From Cyber Criminals

Richard Furlong, Jr.
Senior Stakeholder Liaison

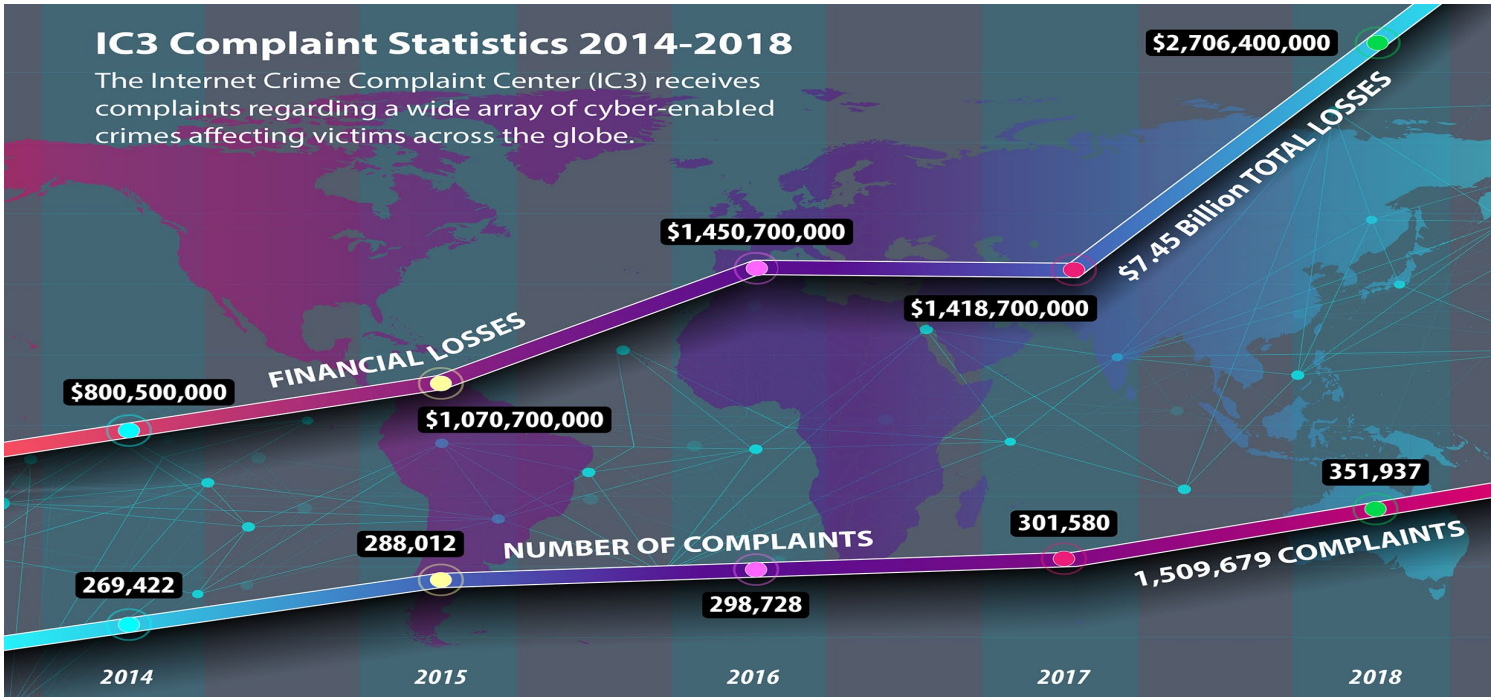
CPA Continuing Education Society of PA
June 22, 2022

Safeguarding Client Data

Federal Laws Apply to Preparers:

- **Gramm-Leach-Bliley Act, the "Safeguards Rule" requires you to ensure the security and confidentiality of customer records and information.**
- **Gramm-Leach-Bliley Act, the "Financial Privacy Rule" deals with privacy notices and information collection and sharing.**
- **Internal Revenue Code (IRC) imposed criminal and monetary penalties for knowingly or recklessly making unauthorized disclosures.**

What is the Problem?



Source: FBI 2018 Internet Crime Report- IC3

More of the Problem

Business Email Compromises- BEC

2018- 20,373 Complaints

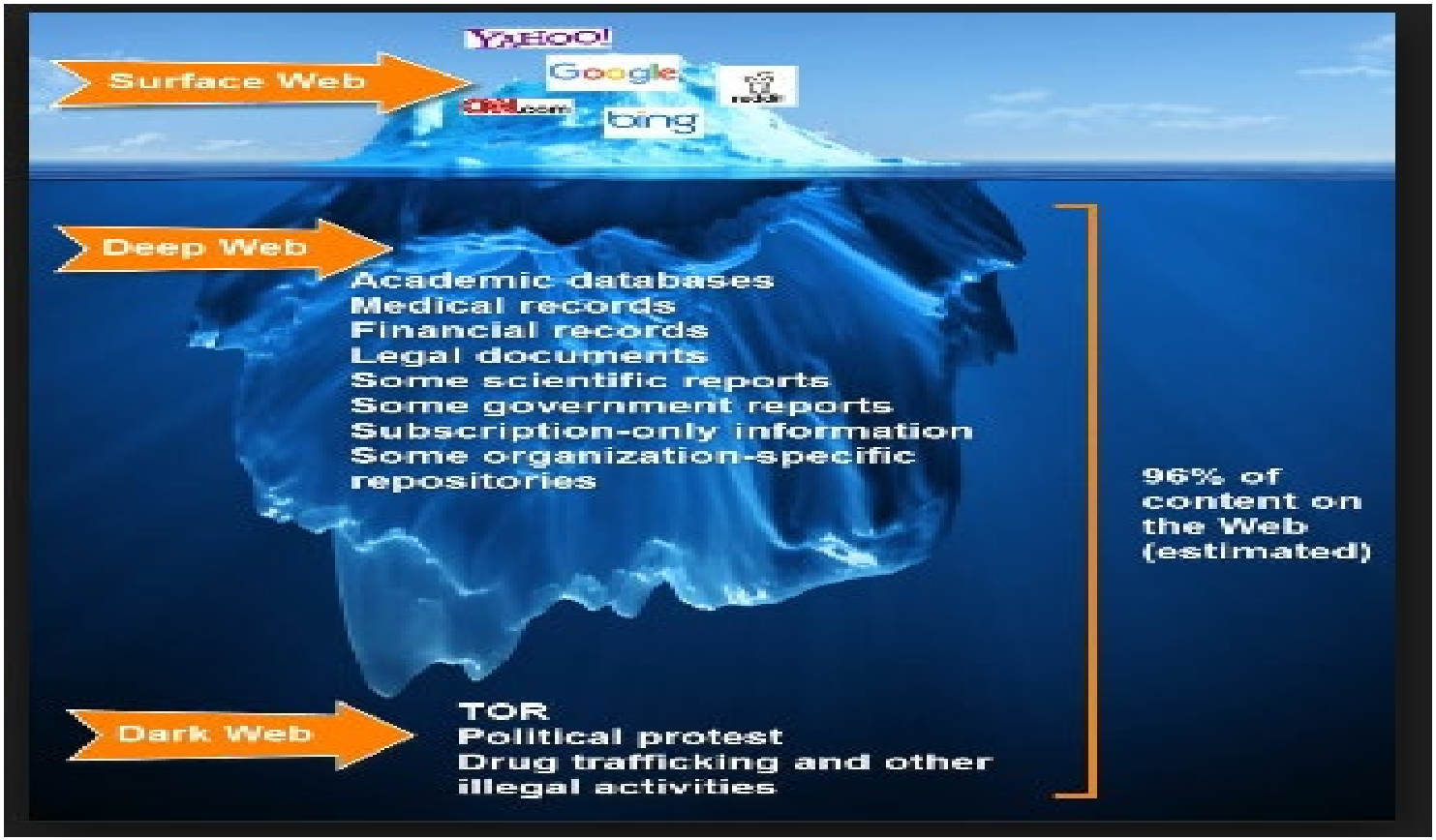
$1.2 billion in adjusted losses

IRS- 118 incidents with over 88,374 TINs

and over $17M in revenue protected.

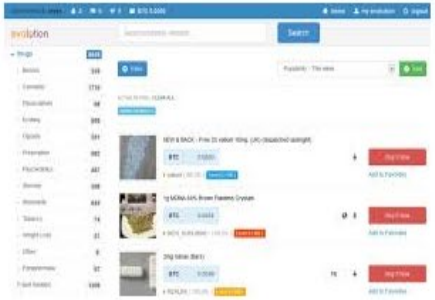
Enhances the Problem

What is the Dark Web?



Examples of the Markets

silk road | alphabay | agora | evolution | sale | drugs | market | ship | utopia | black | hansa | usd | silkroad | stolen | agora marketplace



NIST Cybersecurity Framework

Five key pillars of the successful and holistic cybersecurity program

Source: www.nist.gov/cyberframework

Tax Security 2.0 – A Tax Pro's Security Checklist

Taxes-Security-Together Checklist

- Outline the “Security Six” basic protections
- Create a written data security plan
- Educate yourself on phishing scams
- Recognize the signs of client data theft
- Create a data theft recovery plan

Step 1: "Security Six" Protections

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)

"Security Six" # 1 – Anti-virus Software

- **Scans computer files for malicious software**
  - Automatic scans
  - Manual scans of email attachments, web downloads, and portable media
- **Protection against spyware and phishing**

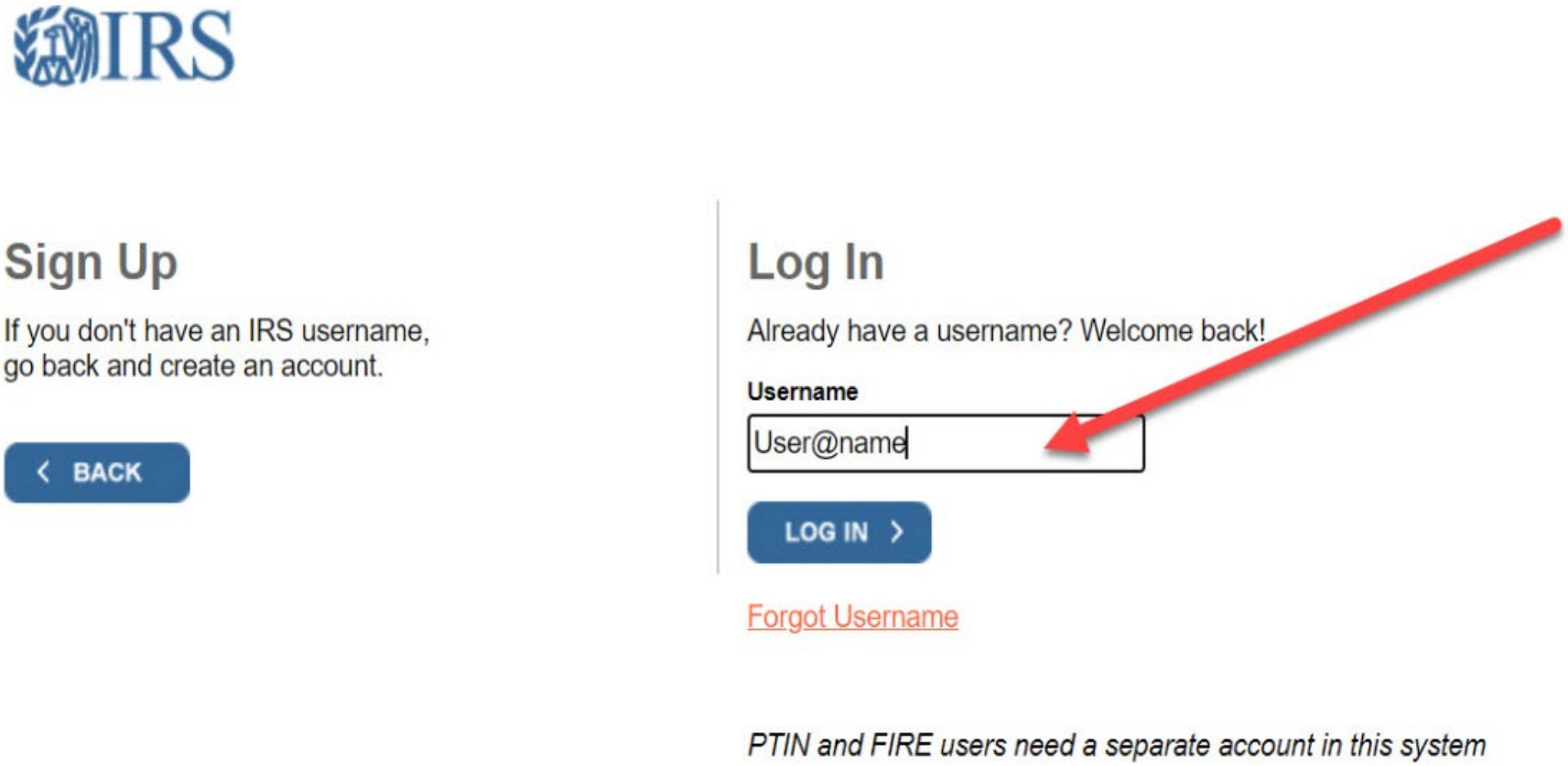
"Security Six" # 2 – Firewalls

- **Provide protection against outside attackers**
  - Shield computer or network
- **Firewalls are categorized as:**
  - Hardware – external devices
  - Software – built-in or purchase

"Security Six" # 3 – Two-factor authentication

- **Adds an extra layer of protection beyond a password**
- **User must enter credentials**
  - username and password plus another step (such as a security code sent via text to a mobile phone)

Multi-Factor Authentication


IRS
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
User@name
LOG IN
Forgot Username
PTIN and FIRE users need a separate account in this system

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

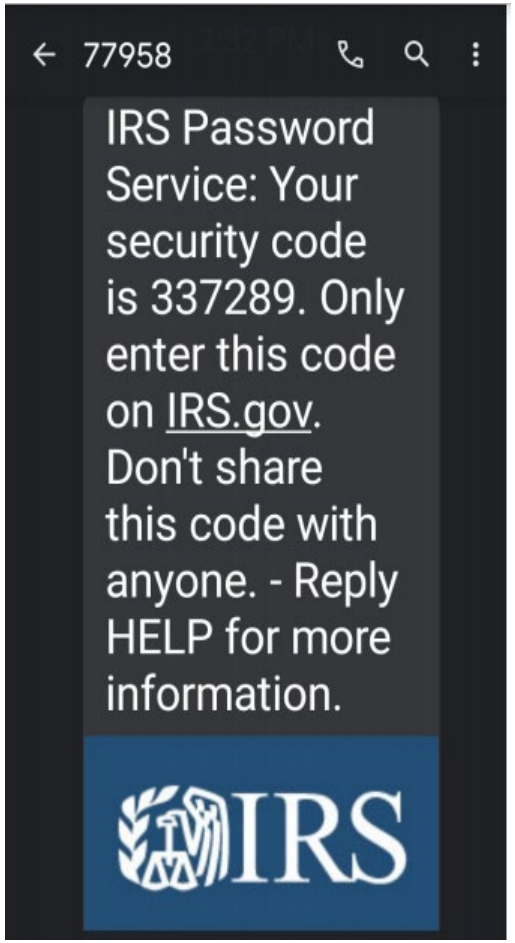
Password

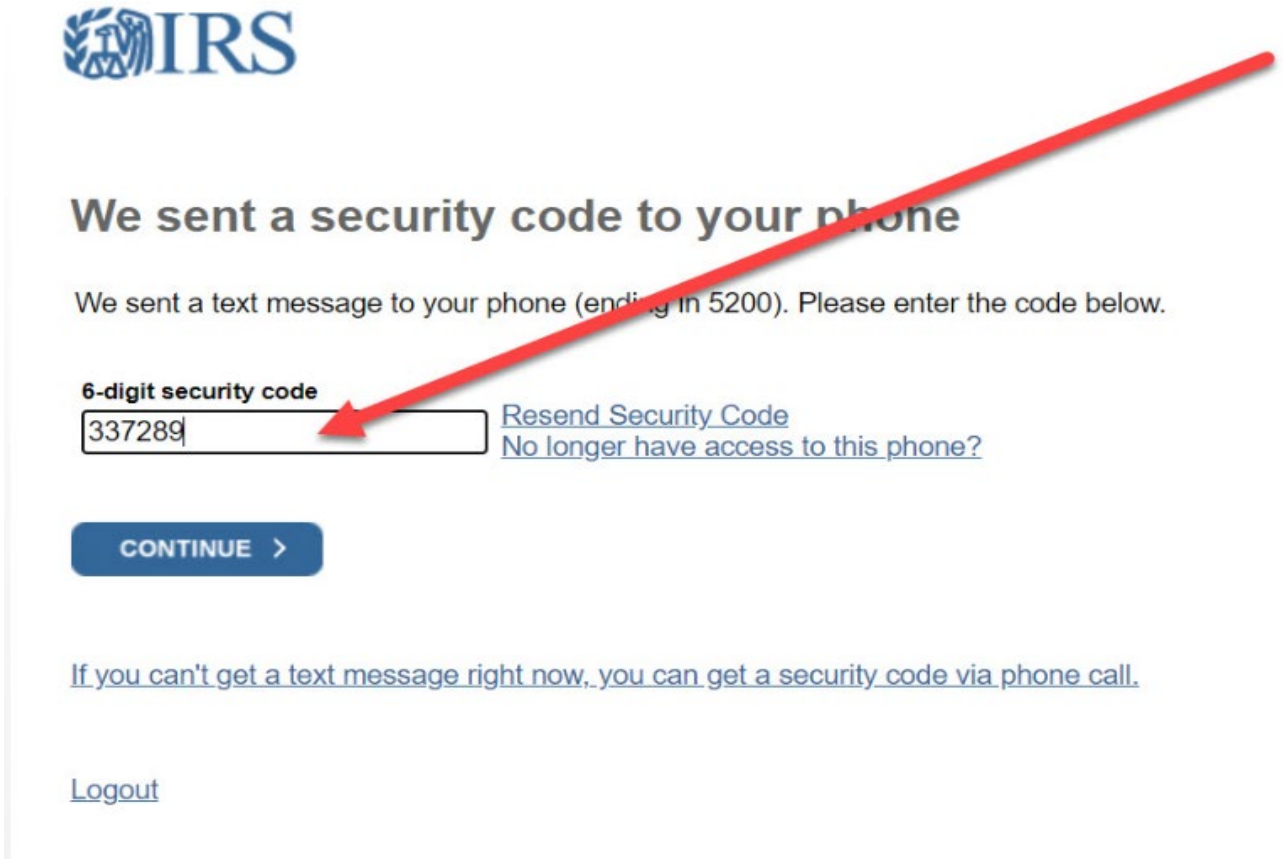
Your@password

Forgot Password

SUBMIT >

CANCEL


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


IRS
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
337289
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

"Security Six" # 4 – Backup Software/Services

- Critical files on computers should routinely be backed up to external sources
- Backup files may be stored either using an online service or on an external disk
- Encrypt the back-up data for the safety of the information

"Security Six" # 5 – Drive Encryption

- Use drive or disk encryption software for full-disk encryption
- Transforms data on the computer into unreadable files for an unauthorized person

"Security Six" # 6 – Virtual Private Network (VPN)

A VPN provides a secure, encrypted tunnel to transmit data between a remote user via the internet and the company network

Search for "Best VPNs" to find a legitimate vendor

How to get started with the "Security Six"

- **Review professional insurance policy**
  - Some offer coverage for data thefts
- **Review IRS Publication 4557, Safeguarding Taxpayer Data**
- **Small Business Information Security: The Fundamentals by NIST – www.nist.gov**

Step 2: Create a Data Security Plan

- **Required under federal law**
  - The Gramm-Leach-Bliley (GLB) Act
  - Federal Trade Commission (FTC) Safeguards Rule
- **IRS Revenue Procedure 2007-40 for Authorized IRS e-file Provider**

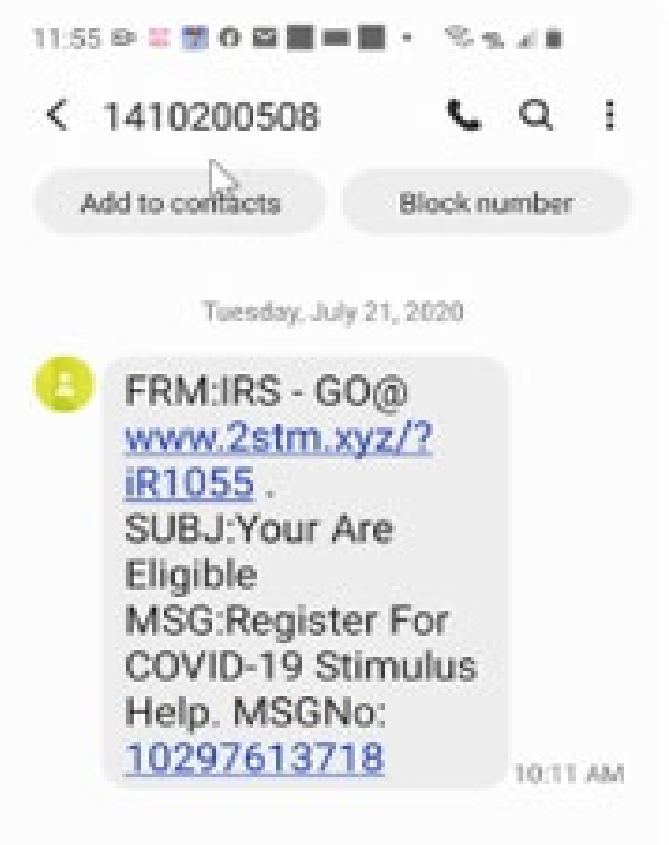
Step 3: Educate yourself on phishing scams

- **Many data thefts start with a phishing email**
  - Click on a link to a fake website
  - Open an attachment with embedded malware
- **Spear phishing email to pose as a trusted source**
  - Account Takeover
  - Ransomware

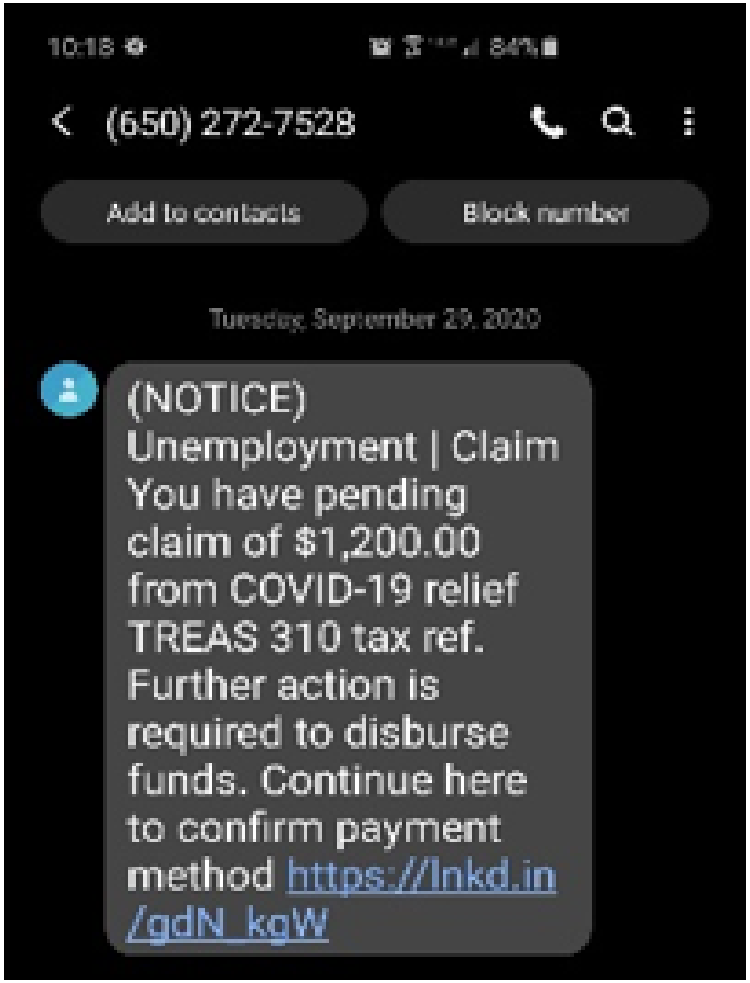
Cybercriminal Threats

- Cybercriminals have attempted to exploit COVID-19 concerns this year
- Cybercriminals use a variety of techniques and tools

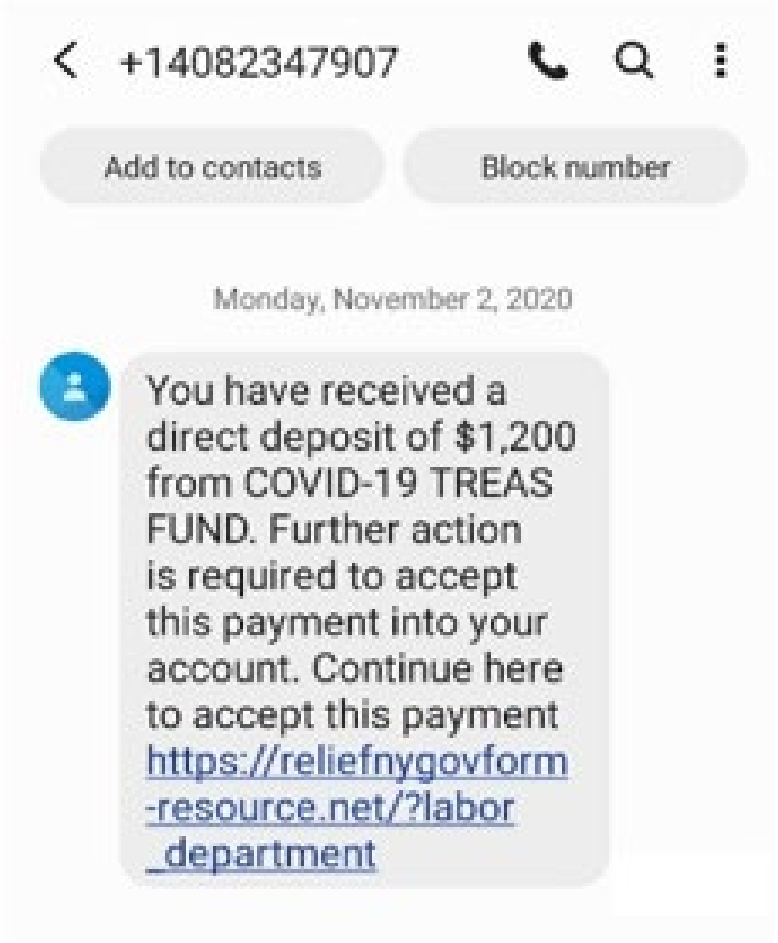
Short Message Service – Example



Phishing Text Message – Example



Phishing Text Message – Example 2



Example: Scam Email

Dear Tax Pro,

Your electronic filling identification number (EFIN) has temporary been put on hold due to suspicious activity with your PTIN user.

Did you transmit the below 1040 form?

TranscriptPDF

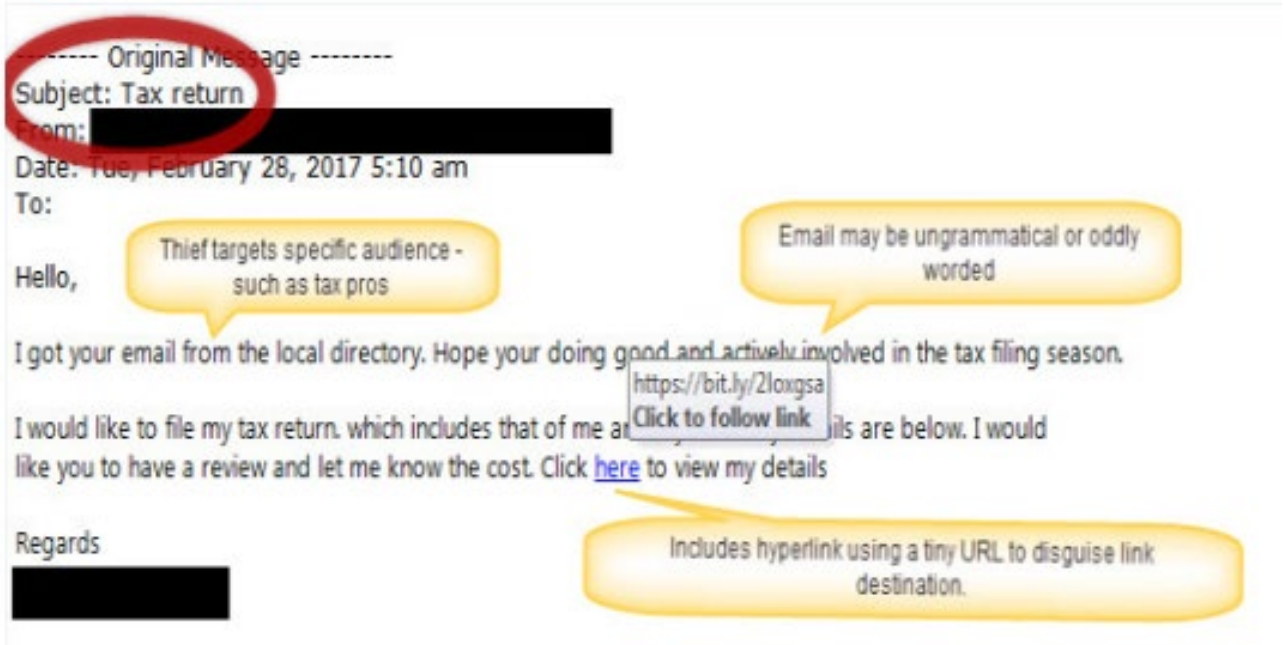
If this was you, please ignore this message.
If it was not you, please immediately change your password.
Failure to confirm this request will leads to EFIN suspended.

We are trying to protect your e-service and EFIN account.

Sincerely.

Carol A Campbell
IRS.gov e-service

Recognize a Phishing Scam



Source: www.nist.gov/cyberframework

Phishing Email – Example

Subject: 2020 tax season inquiry
Date: [REMOVED] 2020 [REMOVED]
From: [REMOVED]
To: [REMOVED]

Happy New year,
I am currently in search for a new tax preparer. I usually file these federal forms 1040, Schedule A , Schedule B, Schedule C, Schedule D, Schedule SE. My former preparer typically charged around $600. Is that the typical fee that you would charge? I talked to a large tax group in the area, and they said that they do more complicated returns and charge a minimum of $3,000!.

I also have to amend my 2018 tax return i got a notice regarding these latenovember. I will also like to have a quote on what you will charge to help resolve the issue with the IRS.
I hope to hear from you soon

Sincerely,
[REMOVED]

Phishing Email – Example 2

Hello [REMOVED],

Thanks for your response, I am sorry for not getting back to you immediately. I have been out of my office and wont be back till the 27th of Jan. I am spending some time with my daughter. I hope you are still willing to help? Your pricing seems fair and within my budget. How do I sign up as a Tax client with your firm?

Below is a ShareFile access to my prior year tax return and the letter I received. Hopefully this gives you a better understanding of the complexity of my tax situation. I hope we can get started immediately. Would you need a retainer?

[REMOVED]

[REMOVED]

COVID 19 Scams

- Cybercriminals have attempted to exploit COVID-19 concerns this year by using it as their “bait’ in phishing scams
- Cybercriminals pose as government agencies with “urgent” messages promising help

Steps to Help Protect Data

- **Use separate personal and business emails**
  - Protect with strong passwords
  - Two-factor authentication
- **Install anti-phishing tools**
- **Use security software**

Steps to Help Protect Data – continued

- **Never open or download attachments from unknown senders**
- **Password-protect and encrypt documents**
- **Do not respond to suspicious or unknown emails; if IRS related, forward to phishing@irs.gov**

Business Email Compromise

- **Cybercriminals are able to identify chief operating officers, school executives or others in position of authority (Social Engineering).**
- **Fraudsters mask themselves as executives or people in authoritative positions and send emails to payroll or human resources requesting copies of Forms W-2. (Grooming)**

Source: www.nist.gov/cyberframework

Business Email Compromise

- **Form W-2 contains the following (Exchange of Information)**
  - **Employment Identification Numbers (EIN)**
  - **Social Security Numbers**
  - **Income / Withholdings (Federal, State, Local)**
  - **Address**
  - **Retirement Plan**
  - **Health Benefits Plan**

Source: www.nist.gov/cyberframework

Business Email Compromise

-----Original Message-----

From: Mickey Mouse <mk@mu.se>

Sent: Tuesday, January 22, 2019 1:03 PM

To: Minnie Mouse <minnie@realbusiness.org>

Subject: Request

Hi Minnie,

I need you to email me 2018 W2s of all employees. How soon can you get me those?

Regards

Mickey Mouse

Source: www.nist.gov/cyberframework

Example: Warning Labels

From: [redacted] [mailto: [redacted]]
Sent: Tuesday, June 12, 2018 2:01 AM
To: [redacted] . <[redacted]>
Subject: Final Reminder for Notice of Tax Overpayment

**** This is an EXTERNAL email. Exercise caution. DO NOT open attachments or click links from unknown senders or unexpected email. ****

1

Source: www.nist.gov/cyberframework

Internal Revenue Service Does Not:

- Call Demanding Payment and Making Threats of jail or lawsuits
- Demand payment via gift, debit, or iTunes cards
- Send unsolicited e-mails about refunds
- Request login credentials, Social Security Numbers or other sensitive information
- irs.gov/phishing

Other Government Agencies Investigate Scams

- TIGTA investigates IRS impersonation Scams
- TIGTA phone number: 1-800-366-4484
- TIGTA web address: www.tigta.gov
- Federal Trade Commission: www.FTC.gov

Step 4: 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

Signs of Client Data Theft – continued

- **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**

Signs of Client Data Theft – continued

- **The number of returns filed with tax practitioner's Electronic Filing Identification Number (EFIN) or their Practitioner Tax Identification Number (PTIN) exceeds number of clients assisted.**

Monitor Your EFIN, PTIN and CAF Numbers

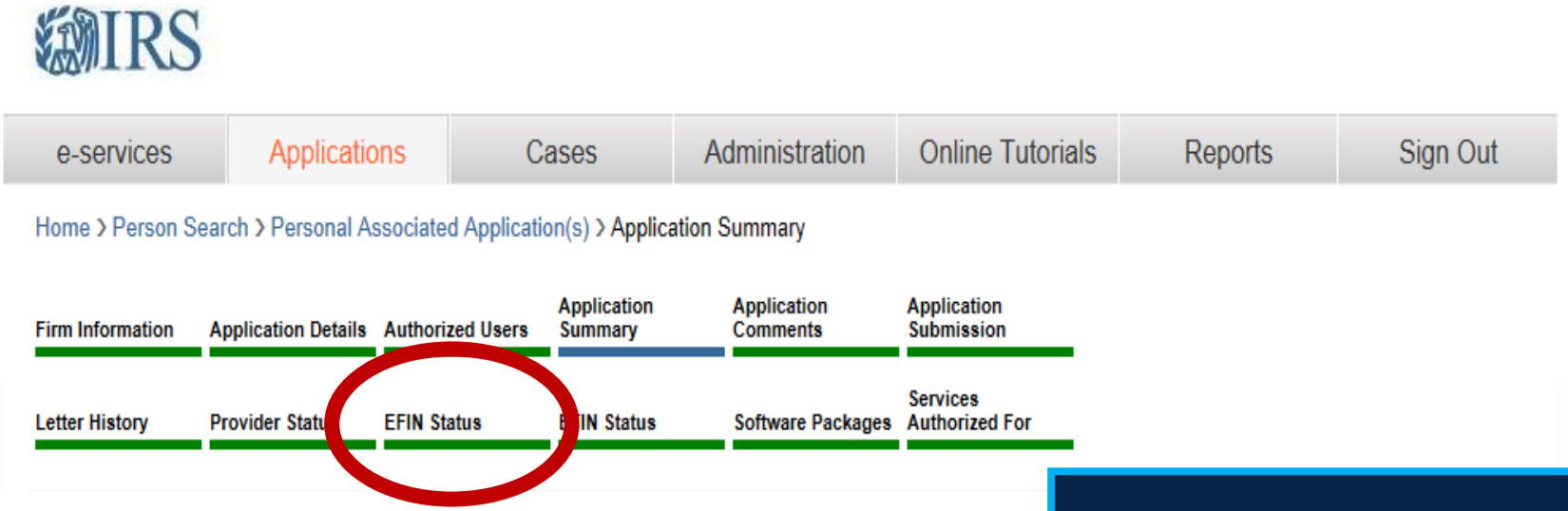
Stolen EFINs, PTINs and CAFs

- Thieves impersonate tax pros to:
  - File fraudulent returns
  - Submit Power of Attorney forms
  - Call Practitioner Priority Service line
  - Attempt to access client accounts
  - Attempt to access e-Services
- IRS responses include:
  - 2-factor authentication for e-Services accounts
  - Authorization requirements for PPS callers
  - Redacted tax transcripts

Maintain Your EFIN Application

- Only the IRS can issue EFINs
- Review periodically for accuracy and updates
- Update change in business operations within 30 days
  - Changes in address, phone numbers or personnel
  - Add or remove authorized users (responsible officials, principal consent, delegated users, etc.)
- Know when a new EFIN is needed
  - New ownership of a firm (EFIN not transferable)
  - New location that transmits e-File returns

Monitor returns filed under your EFIN



For EFIN weekly totals:

- Go to e-Services
- Access e-File Application
- Search by name
- Select “EFIN Status”

Report Suspected EFIN Abuse

Electronic Return Originator (ERO) Activity by EFIN/Return Type

The activity shown below by EFIN and Return Type represents the total YTD counts for returns submitted electronically to the IRS.

Customize | Find | View All | First 1-5 of 5 Last

	EFIN	Return/Form Type	Processing Year	Transmitted YTD	Accepted YTD	Rejected YTD
1	555555	1040	2016	51	50	1
2		1041	2016	9	9	0
3		1065	2016	12	12	0
4		1120	2016	10	10	0
5		1120S	2016	10	10	0

- **Too many returns filed with your EFIN? Contact e-Help Desk (866) 255-0654**

Monitor Your PTIN

- Monitor “Returns Filed per PTIN”
- Information available via online PTIN system for tax preparers who meet both of the following criteria:
  - Have a professional credential or are an Annual Filing Season Program participant, and
  - Have at least 50 Form 1040 series tax returns processed in the current year

How to Access PTIN Information

- To access “Returns Filed Per PTIN” information, follow these steps:

1. Log into your PTIN account

2. From the Main Menu, find “Additional Activities”

3. Under Additional Activities, select “Summary of Returns Filed.”

Summary of Returns Filed Chart

IRS

*Logged in as **Doe, John***

Main Menu | Edit Login Information | Logon

Summary of Returns Filed

See the chart below for the number of tax returns with your PTIN processed by the IRS **this year**. The data is updated weekly and includes only Form 1040 series returns **processed** through the date specified.

If the number is **substantially higher** than the number of tax returns you've prepared and you suspect possible misuse of your PTIN, complete Form 14157.

If the number is **substantially lower** than the number of tax returns you've prepared, you need to verify that you are entering your PTIN correctly on returns. The most common cause of this problem is the entry of an incorrect PTIN during tax preparation software setup.

Definitions:

- Processing Year: the current calendar year
- Tax Year: the tax year of the returns
- 1040s Processed: includes **only** 1040 series returns (1040, 1040-PR, 1040-SS, 1040A, 1040EZ, 1040EZ-T, 1040NR, and 1040NR-EZ)

51 Returns as of 5/14/2019

Processing Year	Tax Year	1040s Processed
2019	2018	49
	2017	2

Report Misuse of your PTIN

11a. Review the complaints below and check all that apply

- ☐ Theft of Refund *(Diverted refund to unknown account; return filed does not match taxpayer's copy)*
- ☐ E-File *(e-filed returns using pay stub, non-commercial software or Free File without properly securing taxpayer's signature)*
- ☐ Preparer Misconduct *(Failed to provide copy of return, return records, sign returns or remit payments for taxes due; misrepresentation of credentials; agreed to file return but did not; filed return without authorization or consent.)*
- ☐ PTIN Issues *(Failed to include Preparer Tax Identification Number (PTIN) on tax return; improperly used a PTIN belonging to another individual)*
- ☐ False Items/Documents *(False expenses, deductions, credits, exemptions or dependents; false or altered documents; false or overstated Form W-2 or 1099; incorrect filing status)*
- ☐ Employment Taxes *(Failed to file forms 940, 941, 943, or 945 or remit Employment Tax payment)*
- ☒ Other *(explain below)*

I checked my PTIN return numbers from IRS.gov and there is a discrepancy

Section D - Your Information *(do not complete if you are the taxpayer)*

(We never share this information with the person or business you are reporting)

This information is not required to process your complaint but is helpful if we need to contact you for additional information.

18. Name *(Last, First, MI)*	19. Date of complaint
20. Mailing address *(street, city, state, ZIP code)*	21. Telephone number(s) *(include area code)*
	22. Email address

23. Your relationship to Preparer

- ☐ Client
- ☐ Return preparer working for a different firm*
- ☐ Return preparer working for the same firm*
- ☐ IRS employee
- ☒ Other *(specify)* Self

Maintain Your POA Files

- A CAF number is assigned the first time you file a third-party authorization with IRS.
- Review your Power of Attorney submissions annually
- Withdraw your POA for clients you no longer represent by mailing or faxing the existing POA to the IRS using the “Where to File” chart. Write “Withdraw” at the top.

Monitor Your CAF Number

- Using stolen CAF numbers to try to obtain tax transcripts is the latest ID theft trend.
- Receiving unexpected tax transcripts is a sign of identity theft.
- Contact the IRS if there is suspected abuse of your CAF number.
- Review Publication 4557, Safeguarding Taxpayer Data, for additional security steps

Step 5: Create a Data Theft Recovery Plan

- An action plan can save valuable time and protect your clients and yourself
- Make calling the IRS an immediate action item

Data Compromise Action Items

Contact IRS and law enforcement

- **Tax professionals contact IRS Stakeholder Liaisons immediately**
  - Search “stakeholder liaisons” on IRS.gov

Data Compromise Action Items – continued

Contact State Agencies:

- State revenue agencies – email Federation of Tax Administrators for state agency contacts at StateAlert@taxadmin.org
- State Attorneys General

Contact experts:

- Security expert
- Insurance company

Data Compromise Action Items – continued

Contact Clients and Other Services

- FTC for guidance for businesses
  - Email: **idt-brt@ftc.gov**
- Credit Bureaus
- Clients

Review guidance at IRS.gov/identitytheft

Recap

- Recognize and avoid phishing scams
- Do not open links or attachments from suspicious e-mails
- Don’t respond to unsolicited e-mails requesting your password or account information
- Use Multi-Factor authentication for all of your accounts

Resources – IRS YouTube Video

Resources

- **Publication 4557, Safeguarding Taxpayer Data**
- **Publication 5293, Data Security Resource Guide for Tax Professionals**
- **Small Business Information Security: The Fundamentals at NIST.gov**
- **Subscribe to e-News for Tax Professionals**

Use the Safeguard Rule Checklist

ONGOING	DONE	N/A	
☐	☐	☐	Employee Management and Training
☐	☐	☐	
			Information Systems
			Information systems include network and software design, and information processing, storage, transmission, retrieval, and disposal. Here are some FTC suggestions on maintaining security throughout the life cycle of customer information, from data entry to data disposal:
☐	☐	☐	
☐	☐	☐	
			Detecting and Managing System Failures
			Effective security management requires your company to deter, detect, and defend against security breaches. That means taking reasonable steps to prevent attacks, quickly diagnosing a security incident, and having a plan in place for responding effectively. Consider implementing the following procedures:
☐	☐	☐	Monitor the websites of your software vendors and read relevant industry publications for news about emerging threats and available defenses.

Resources – continued

IRS.gov websites:

- www.IRS.gov/securitysummit
- www.IRS.gov/ProtectYourClients
- www.IRS.gov/IdentityTheft

Key Points

- **Review and use the "Security Six" for measures to protect your firm.**
- **Have a security plan and refresh your staff on security measures often.**
- **If working remotely, have a secure VPN.**
- **Contact SL if you become a victim of Data Loss or Ransomware.**

Richard Furlong, Jr.

Senior Stakeholder Liaison

267-941-6343

richard.g.furlong@irs.gov