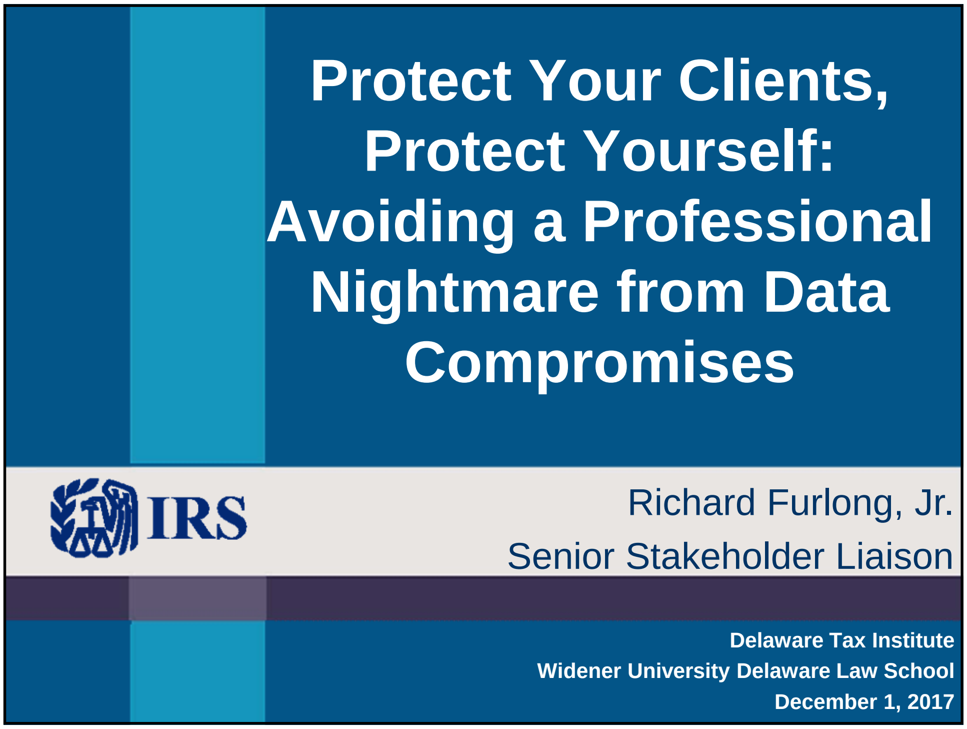
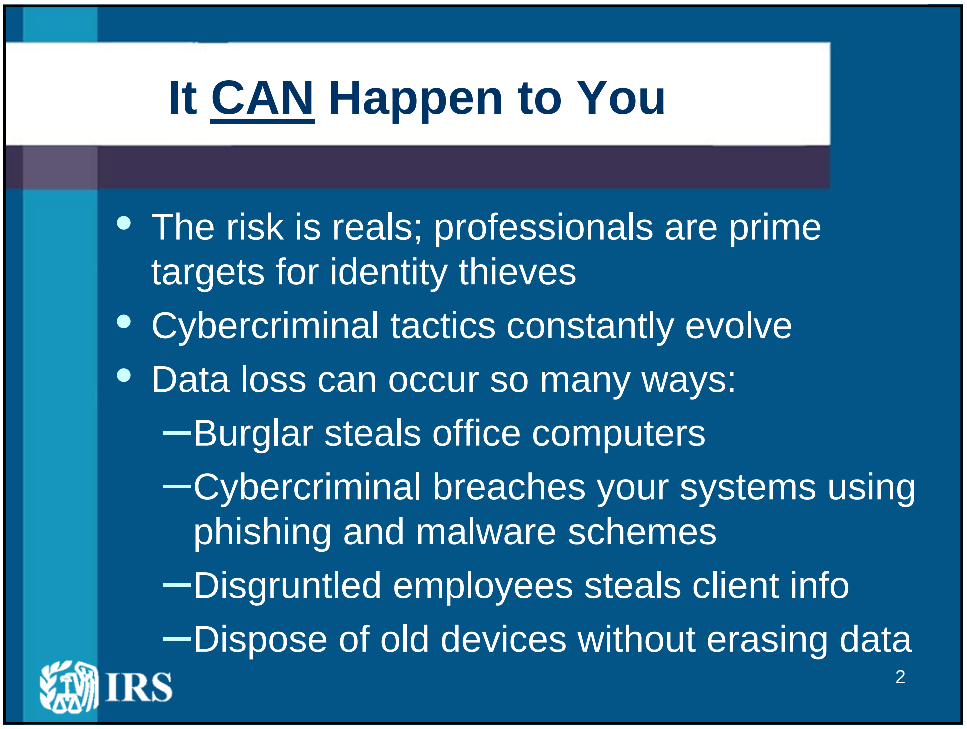


# Protect Your Clients, Protect Yourself: Avoiding a Professional Nightmare from Data Compromises

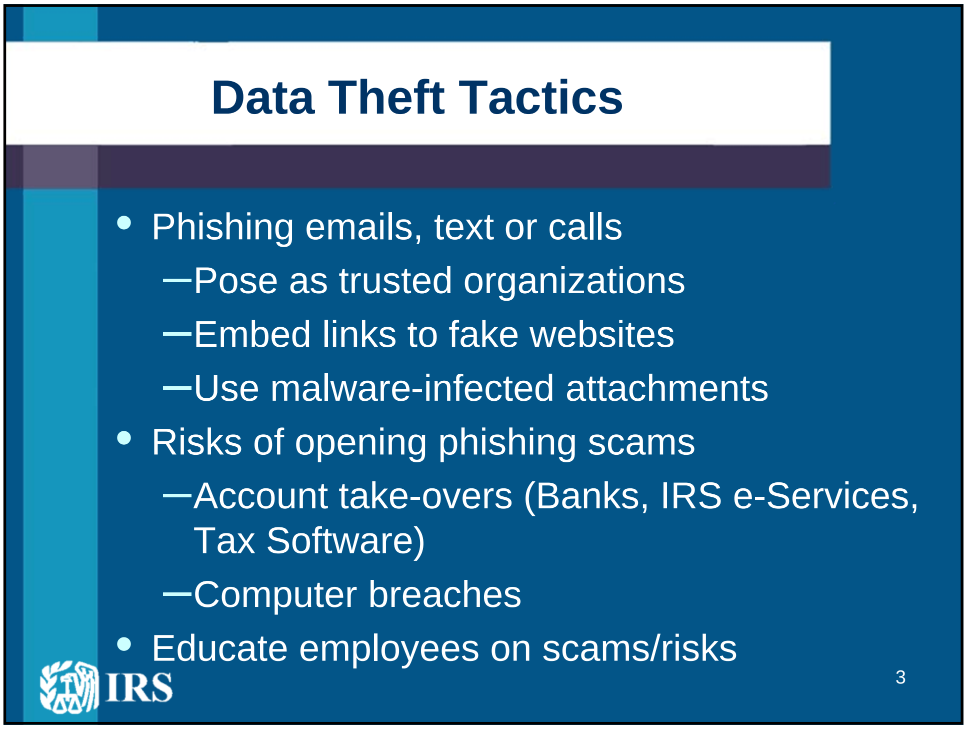
Richard Furlong, Jr.
Senior Stakeholder Liaison

Delaware Tax Institute
Widener University Delaware Law School
December 1, 2017



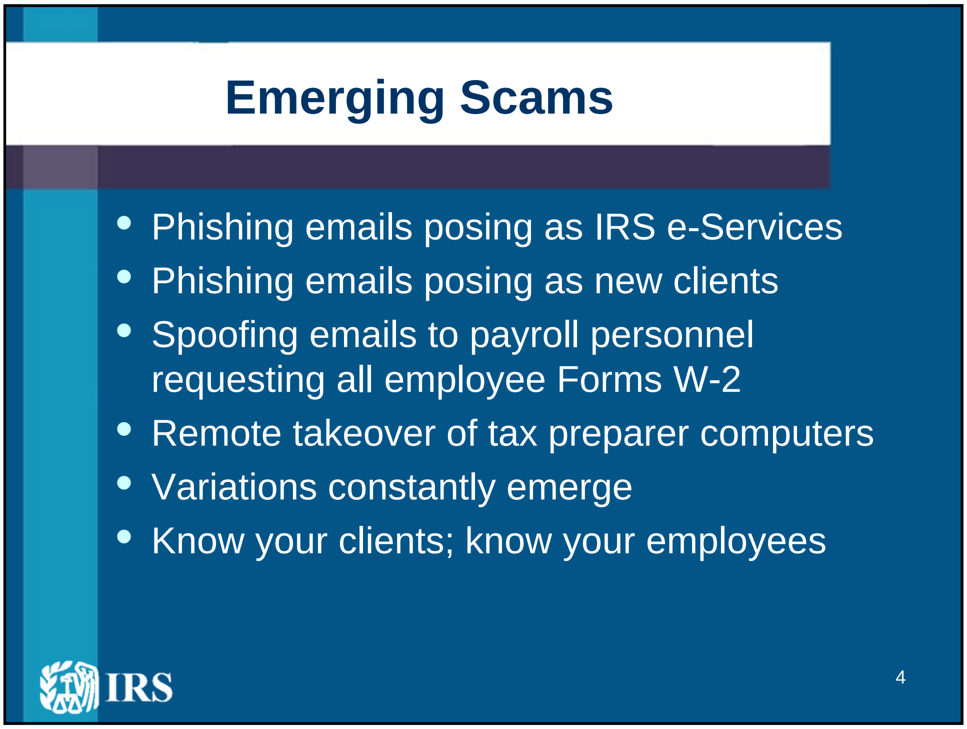
## It CAN Happen to You

- The risk is reals; professionals are prime targets for identity thieves
- Cybercriminal tactics constantly evolve
- Data loss can occur so many ways:
  - Burglar steals office computers
  - Cybercriminal breaches your systems using phishing and malware schemes
  - Disgruntled employees steals client info
  - Dispose of old devices without erasing data



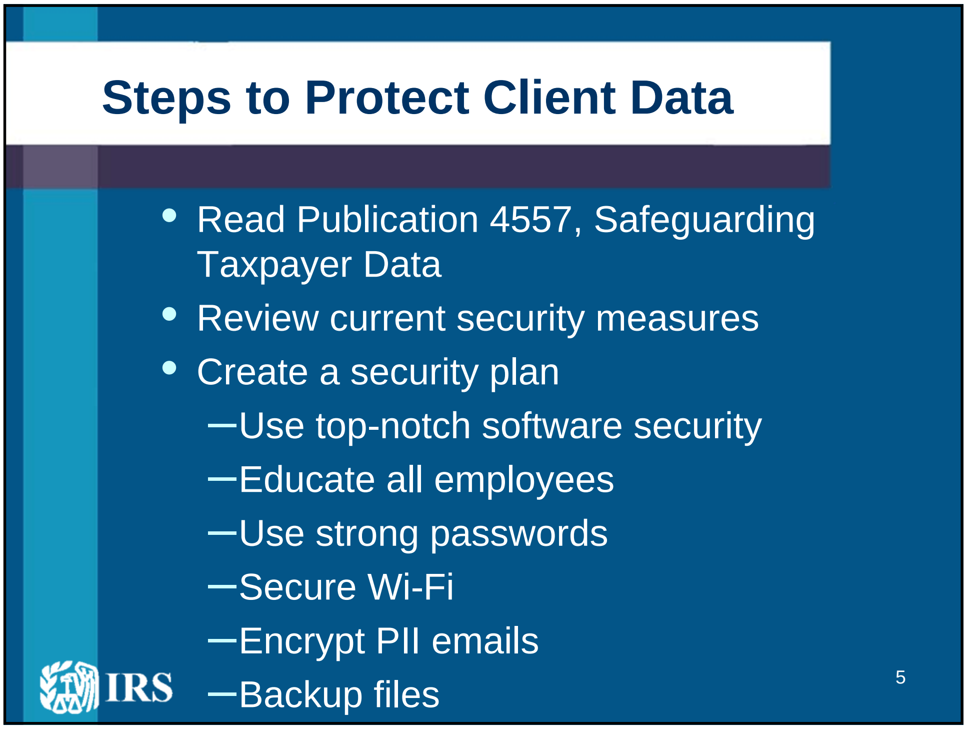
## Data Theft Tactics

- Phishing emails, text or calls
  - Pose as trusted organizations
  - Embed links to fake websites
  - Use malware-infected attachments
- Risks of opening phishing scams
  - Account take-overs (Banks, IRS e-Services, Tax Software)
  - Computer breaches
- Educate employees on scams/risks



## Emerging Scams

- Phishing emails posing as IRS e-Services
- Phishing emails posing as new clients
- Spoofing emails to payroll personnel requesting all employee Forms W-2
- Remote takeover of tax preparer computers
- Variations constantly emerge
- Know your clients; know your employees

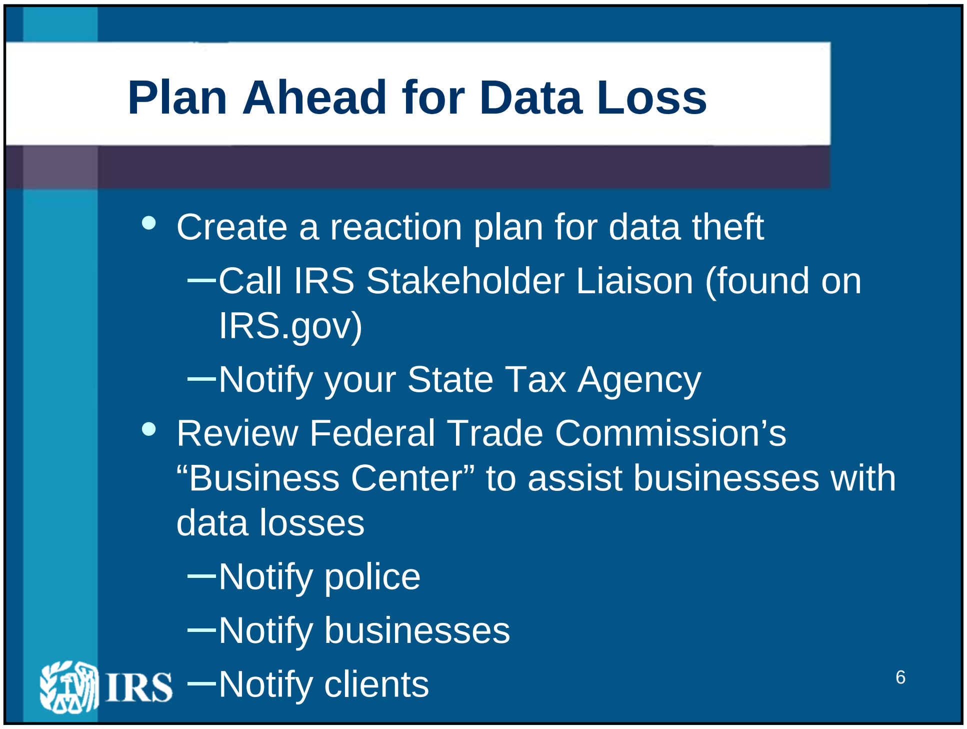


## Steps to Protect Client Data

- Read Publication 4557, Safeguarding Taxpayer Data
- Review current security measures
- Create a security plan
  - –Use top-notch software security
  - –Educate all employees
  - –Use strong passwords
  - –Secure Wi-Fi
  - –Encrypt PII emails
  - –Backup files

IRS

5



## Plan Ahead for Data Loss

- Create a reaction plan for data theft
  - –Call IRS Stakeholder Liaison (found on IRS.gov)
  - –Notify your State Tax Agency
- Review Federal Trade Commission’s “Business Center” to assist businesses with data losses
  - –Notify police
  - –Notify businesses
  - –Notify clients

IRS

6

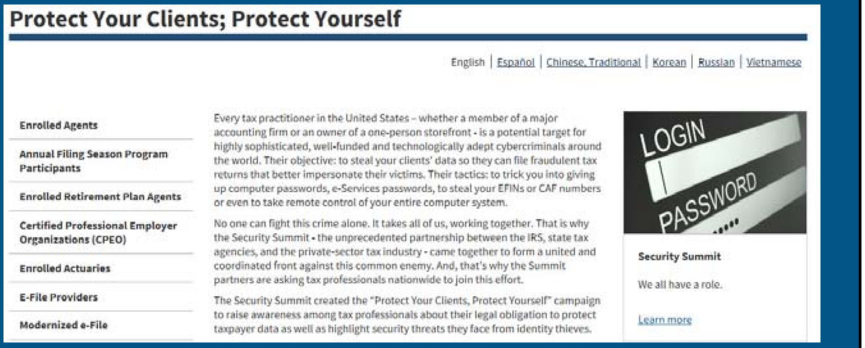
## Help Educate Clients

- IRS, state tax administrators and tax industry working together to increase public awareness about security protections online and at home.
- Review Publication 4524, Security Awareness for Taxpayers
- Consider printing and sharing this one-page guide with your clients

IRS

7

## Search on IRS.gov: “Protect Your Clients; Protect Yourself”



### Protect Your Clients; Protect Yourself

English | Español | Chinese, Traditional | Korean | Russian | Vietnamese

- Enrolled Agents
- Annual Filing Season Program Participants
- Enrolled Retirement Plan Agents
- Certified Professional Employer Organizations (CPEO)
- Enrolled Actuaries
- E-File Providers
- Modernized e-File

Every tax practitioner in the United States – whether a member of a major accounting firm or an owner of a one-person storefront - is a potential target for highly sophisticated, well-funded and technologically adept cybercriminals around the world. Their objective: to steal your clients' data so they can file fraudulent tax returns that better impersonate their victims. Their tactics: to trick you into giving up computer passwords, e-Services passwords, to steal your EFINs or CAF numbers or even to take remote control of your entire computer system.

No one can fight this crime alone. It takes all of us, working together. That is why the Security Summit - the unprecedented partnership between the IRS, state tax agencies, and the private-sector tax industry - came together to form a united and coordinated front against this common enemy. And, that's why the Summit partners are asking tax professionals nationwide to join this effort.

The Security Summit created the "Protect Your Clients, Protect Yourself" campaign to raise awareness among tax professionals about their legal obligation to protect taxpayer data as well as highlight security threats they face from identity thieves.

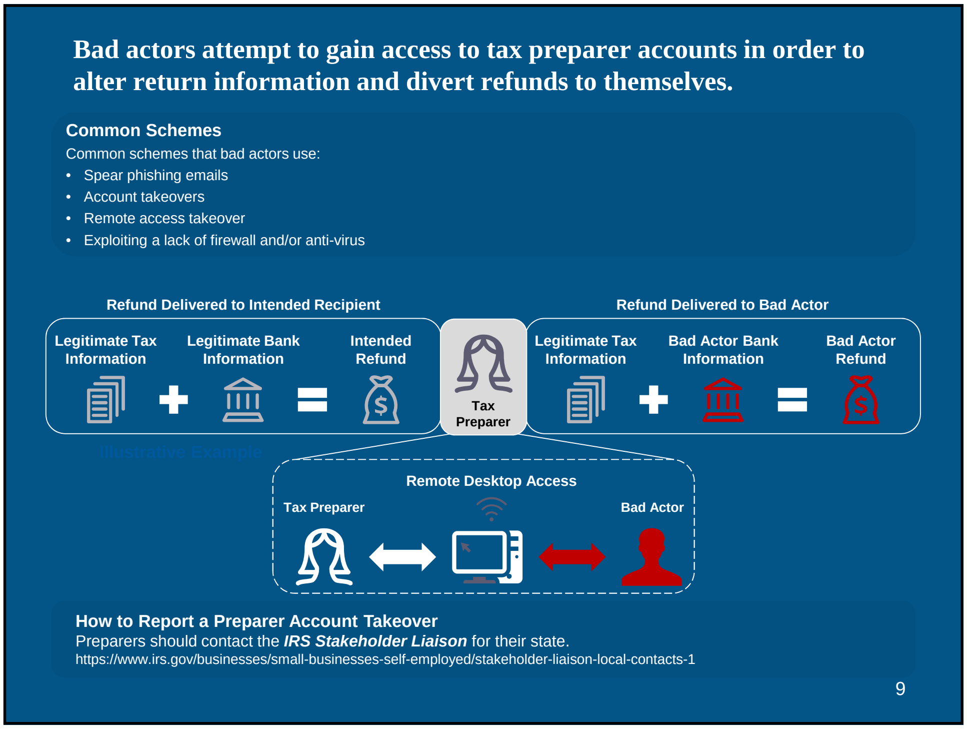
**Security Summit**

We all have a role.

Learn more

IRS

8



**Bad actors attempt to gain access to tax preparer accounts in order to alter return information and divert refunds to themselves.**

**Common Schemes**

Common schemes that bad actors use:

- Spear phishing emails
- Account takeovers
- Remote access takeover
- Exploiting a lack of firewall and/or anti-virus

**Refund Delivered to Intended Recipient**

Legitimate Tax Information + Legitimate Bank Information = Intended Refund

Tax Preparer

**Refund Delivered to Bad Actor**

Legitimate Tax Information + Bad Actor Bank Information = Bad Actor Refund

Illustrative Example

**Remote Desktop Access**

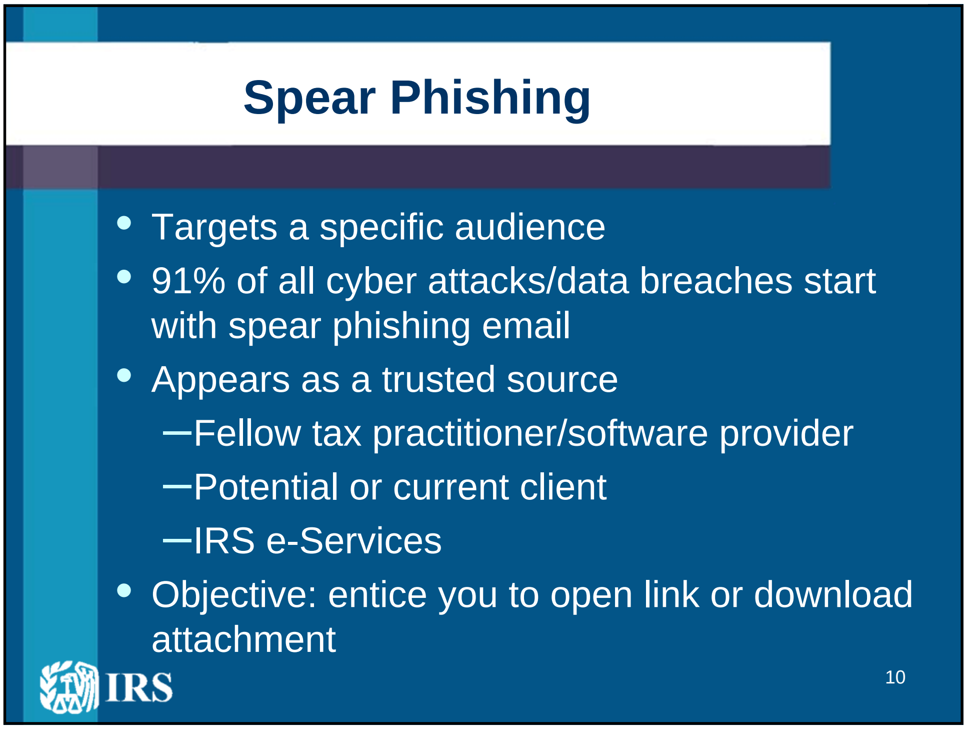
Tax Preparer ⟷ ⟷ Bad Actor

**How to Report a Preparer Account Takeover**

Preparers should contact the ***IRS Stakeholder Liaison*** for their state.

https://www.irs.gov/businesses/small-businesses-self-employed/stakeholder-liaison-local-contacts-1

9



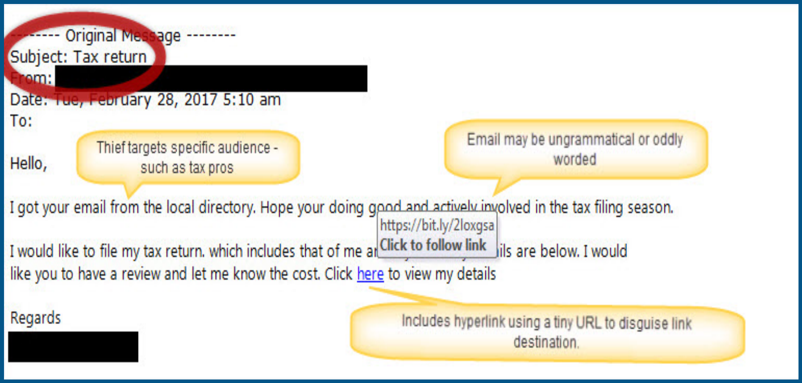
# Spear Phishing

- Targets a specific audience
- 91% of all cyber attacks/data breaches start with spear phishing email
- Appears as a trusted source
  - Fellow tax practitioner/software provider
  - Potential or current client
  - IRS e-Services
- Objective: entice you to open link or download attachment

IRS

10

# Spear Phishing



-------- Original Message --------
Subject: Tax return
From: [redacted]
Date: Tue, February 28, 2017 5:10 am
To:

Hello,

I got your email from the local directory. Hope your doing good and actively involved in the tax filing season.

I would like to file my tax return. which includes that of me an ils are below. I would like you to have a review and let me know the cost. Click here to view my details

https://bit.ly/2loxgsa
Click to follow link

Regards
[redacted]

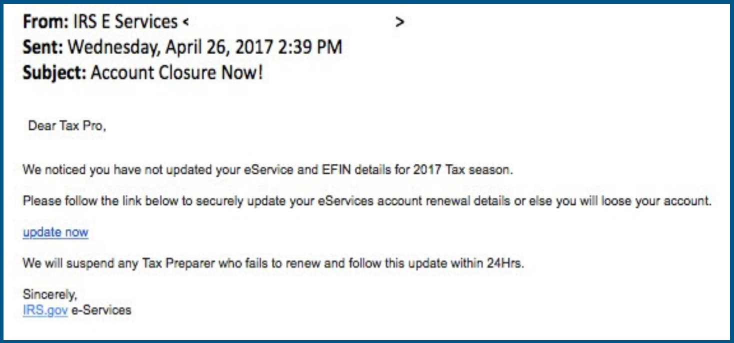
Thief targets specific audience - such as tax pros

Email may be ungrammatical or oddly worded

Includes hyperlink using a tiny URL to disguise link destination.

# Account Takeover

Often starts with a spear phishing email like this:



**From:** IRS E Services < >
**Sent:** Wednesday, April 26, 2017 2:39 PM
**Subject:** Account Closure Now!

Dear Tax Pro,

We noticed you have not updated your eService and EFIN details for 2017 Tax season.

Please follow the link below to securely update your eServices account renewal details or else you will loose your account.

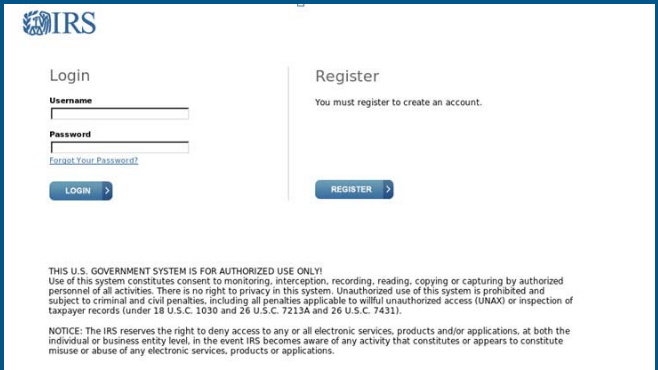
update now

We will suspend any Tax Preparer who fails to renew and follow this update within 24Hrs.

Sincerely,
IRS.gov e-Services

## Account Takeover

Fake e-Services site copies real one



You must register to create an account.

THIS U.S. GOVERNMENT SYSTEM IS FOR AUTHORIZED USE ONLY!
Use of this system constitutes consent to monitoring, interception, recording, reading, copying or capturing by authorized personnel of all activities. There is no right to privacy in this system. Unauthorized use of this system is prohibited and subject to criminal and civil penalties, including all penalties applicable to willful unauthorized access (UNAX) or inspection of taxpayer records (under 18 U.S.C. 1030 and 26 U.S.C. 7213A and 26 U.S.C. 7431).

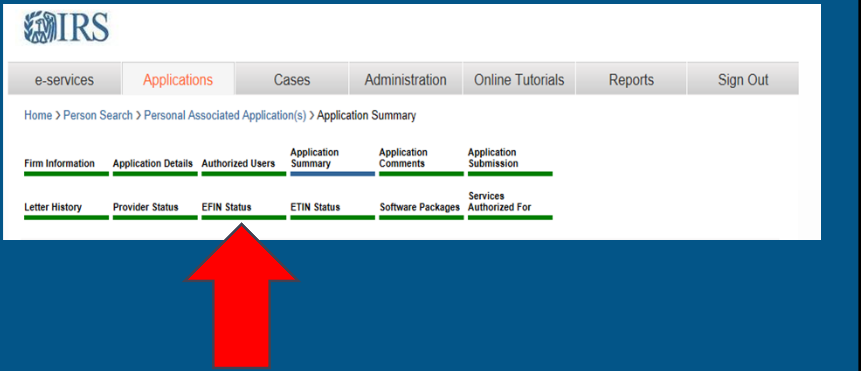
NOTICE: The IRS reserves the right to deny access to any or all electronic services, products and/or applications, at both the individual or business entity level, in the event IRS becomes aware of any activity that constitutes or appears to constitute misuse or abuse of any electronic services, products or applications.

## Protect your EFIN

- IRS reviewing improvements to EFIN safeguards
  - Stepped up efforts to expel EFIN abusers;
  - Increased on-site visits as part of monitoring process
- EFIN holders should review return numbers during filing season
  - e-Services Account updated weekly
  - Excessive numbers can be reported to e-Help Desk (866-255-0654)

# Account Takeover

Monitor your EFIN: Check EFIN Status Weekly during filing season

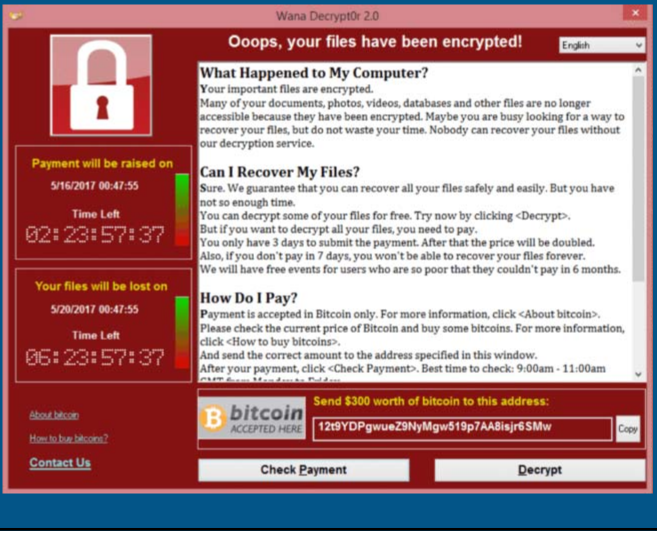


# Account Takeover

Maintain your EFIN: Keep it current

- Update within 30 days of any personnel, address or telephone changes
- EFIN is not transferable
- EFIN application required for each office location where e-File transmissions occur

# Ransomware



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

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

**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?**

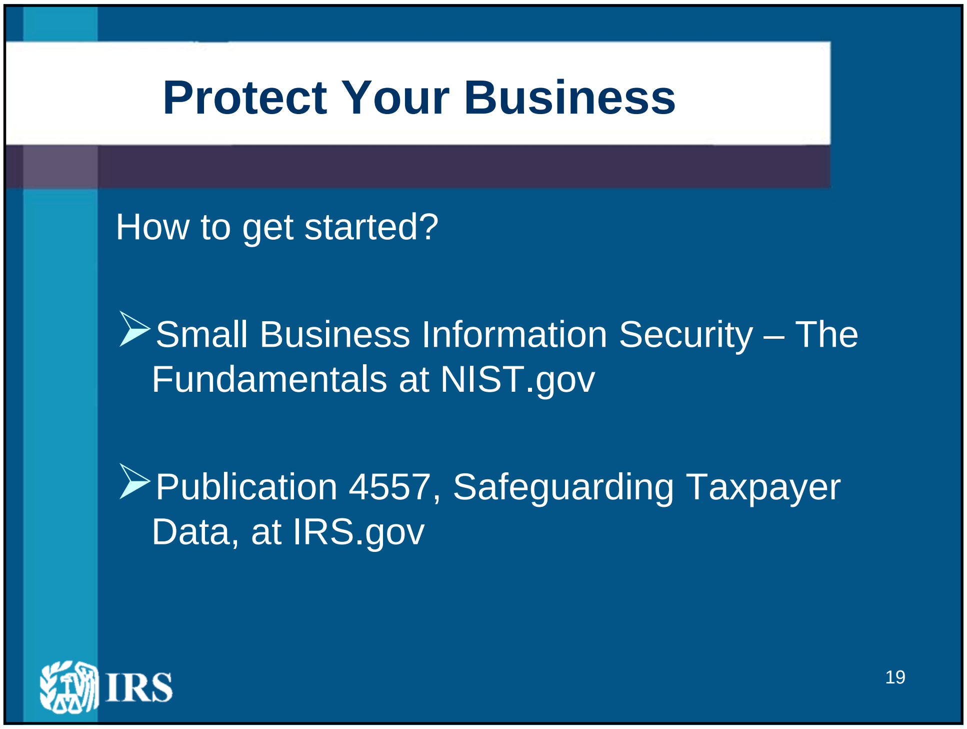
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the 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:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

# Remote Access Attack



## Protect Your Business

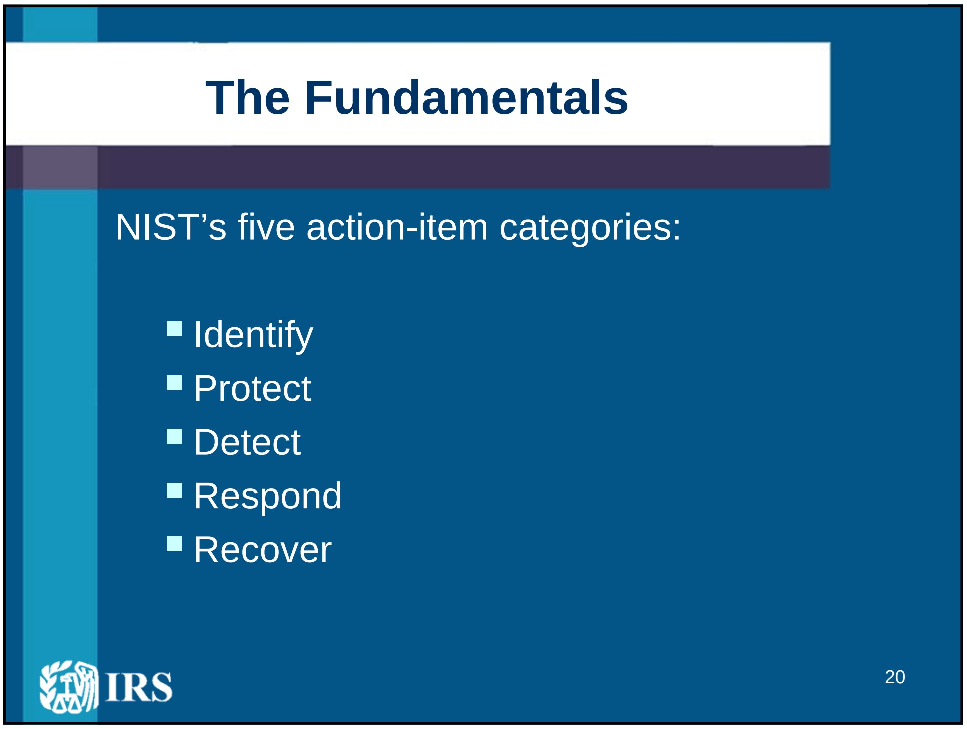
How to get started?

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

- Publication 4557, Safeguarding Taxpayer Data, at IRS.gov

IRS

19



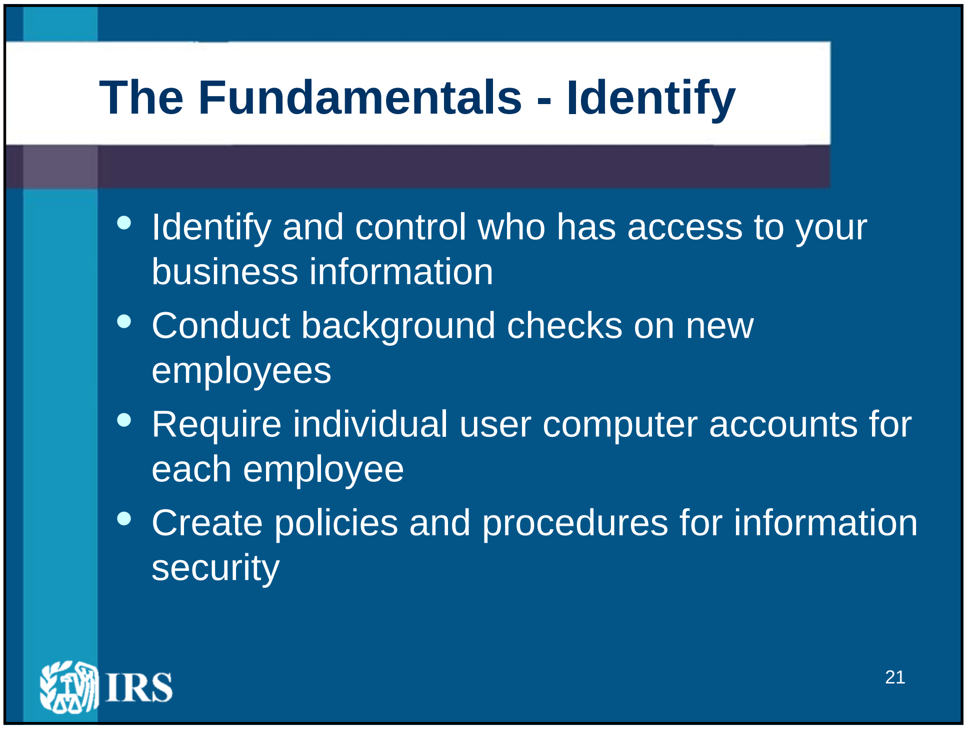
## The Fundamentals

NIST’s five action-item categories:

- Identify
- Protect
- Detect
- Respond
- Recover

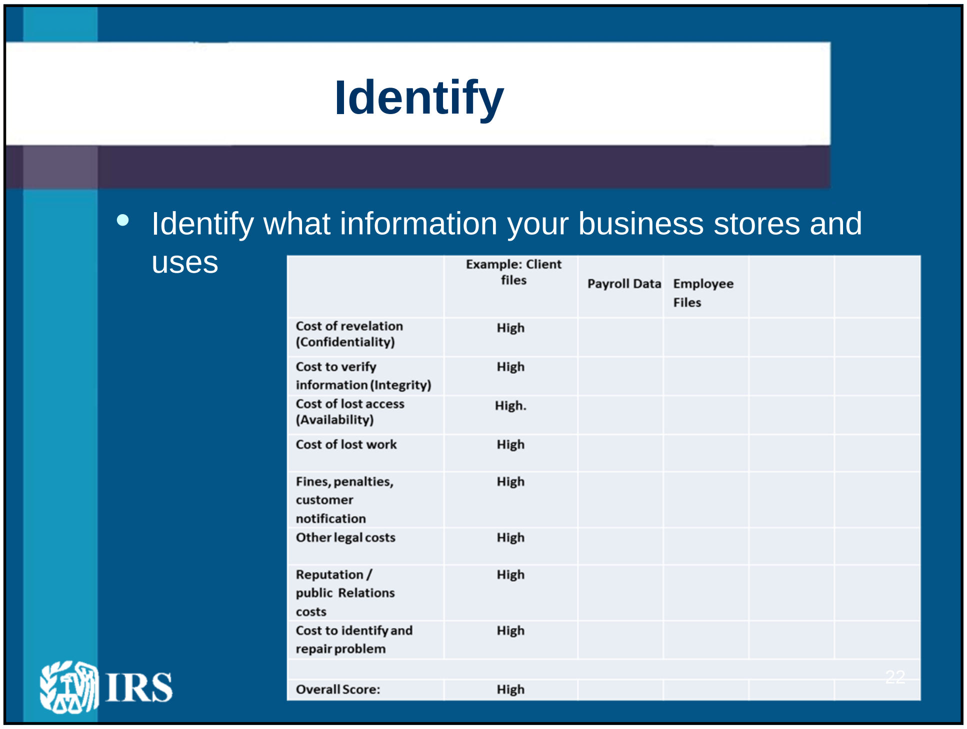
IRS

20



## The Fundamentals - Identify

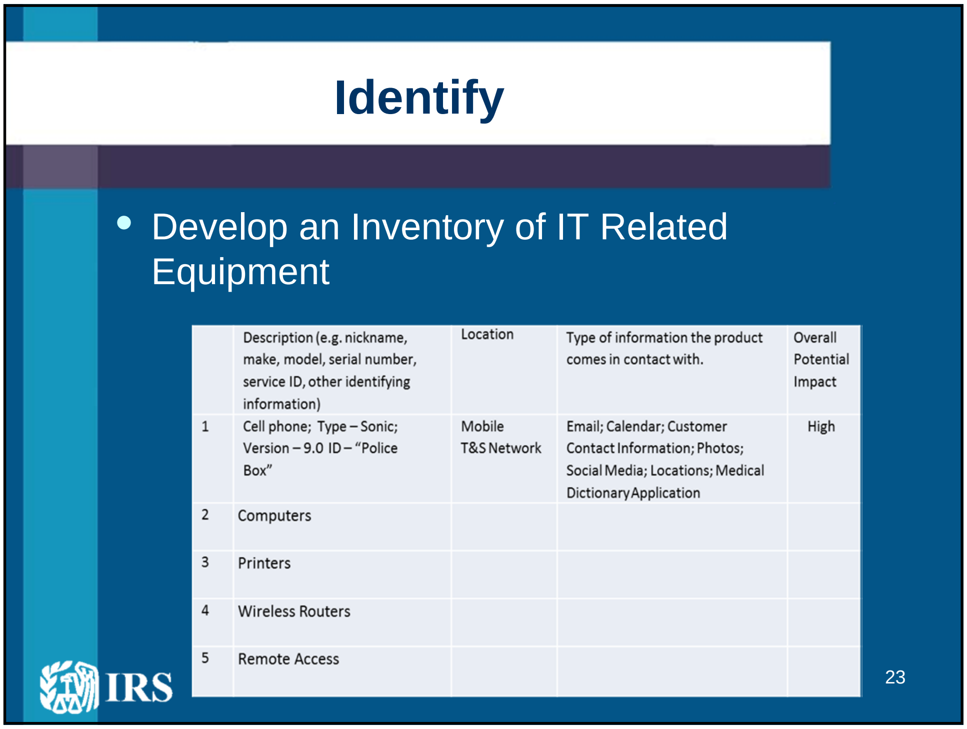
- Identify and control who has access to your business information
- Conduct background checks on new employees
- Require individual user computer accounts for each employee
- Create policies and procedures for information security



## Identify

- Identify what information your business stores and uses

| | Example: Client files | Payroll Data | Employee Files | | |
|---|---|---|---|---|---|
| Cost of revelation (Confidentiality) | High | | | | |
| Cost to verify information (Integrity) | High | | | | |
| Cost of lost access (Availability) | High. | | | | |
| Cost of lost work | High | | | | |
| Fines, penalties, customer notification | High | | | | |
| Other legal costs | High | | | | |
| Reputation / public Relations costs | High | | | | |
| Cost to identify and repair problem | High | | | | |
| | | | | | |
| Overall Score: | High | | | | |



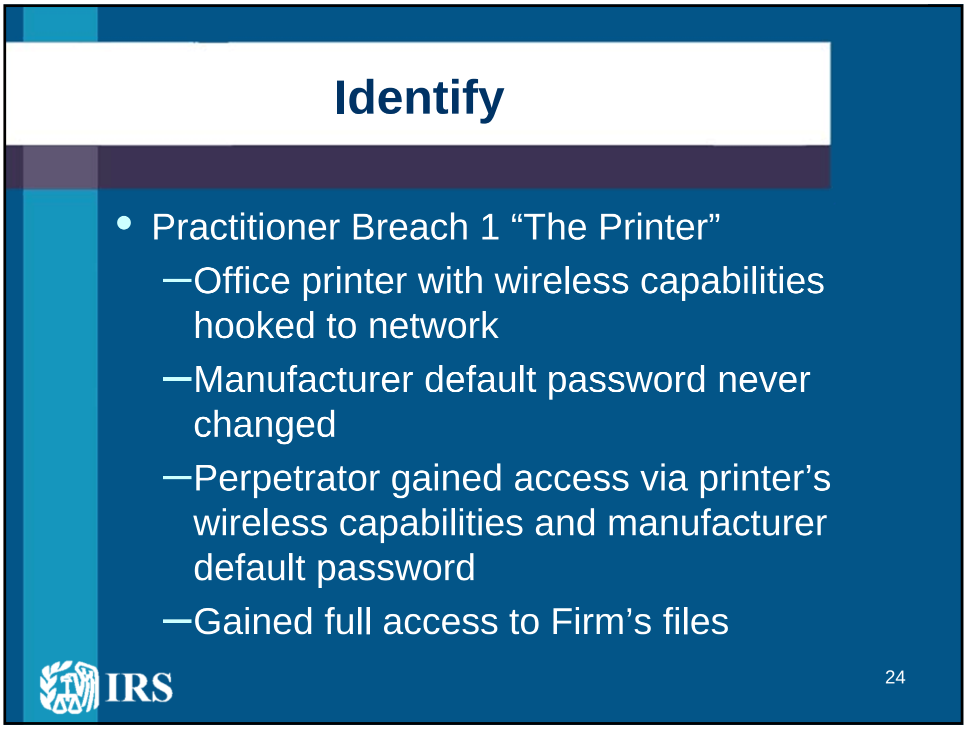
## Identify

- Develop an Inventory of IT Related Equipment

| | Description (e.g. nickname, make, model, serial number, service ID, other identifying information) | Location | Type of information the product comes in contact with. | Overall Potential Impact |
|---|---|---|---|---|
| 1 | Cell phone; Type – Sonic; Version – 9.0 ID – "Police Box" | Mobile T&S Network | Email; Calendar; Customer Contact Information; Photos; Social Media; Locations; Medical Dictionary Application | High |
| 2 | Computers | | | |
| 3 | Printers | | | |
| 4 | Wireless Routers | | | |
| 5 | Remote Access | | | |

IRS

23

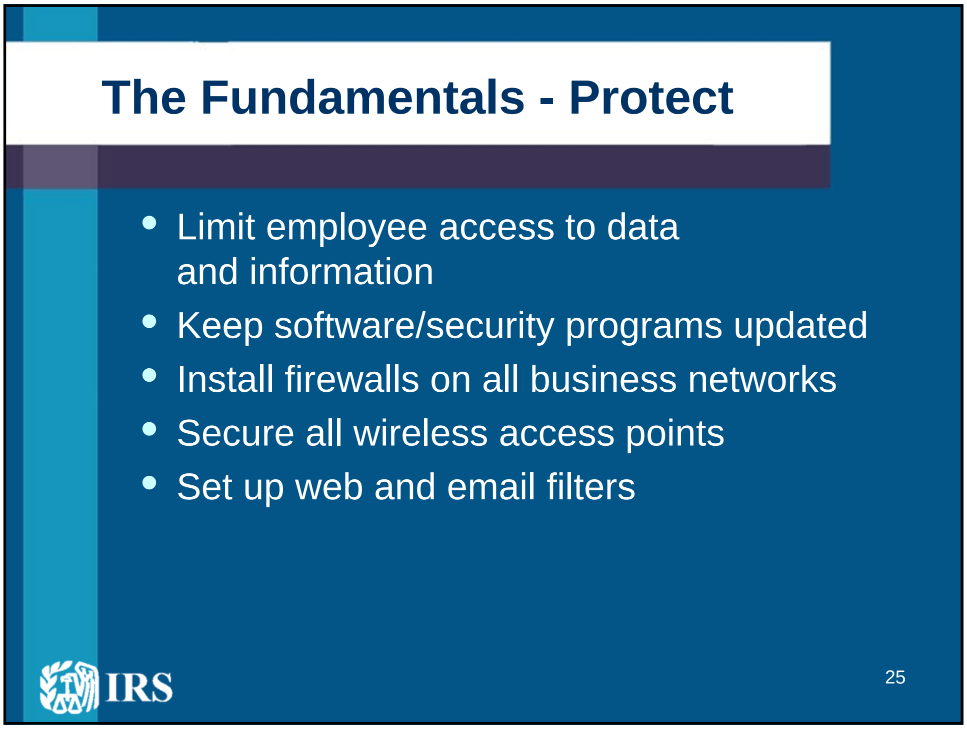


## Identify

- Practitioner Breach 1 "The Printer"
  - Office printer with wireless capabilities hooked to network
  - Manufacturer default password never changed
  - Perpetrator gained access via printer's wireless capabilities and manufacturer default password
  - Gained full access to Firm's files

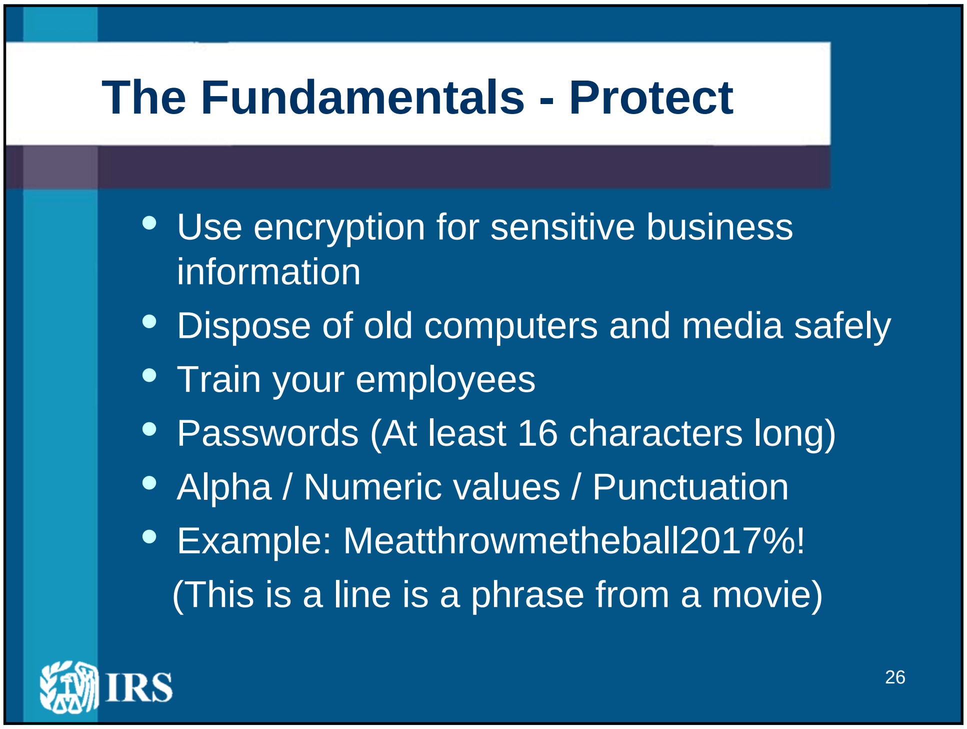
IRS

24



## The Fundamentals - Protect

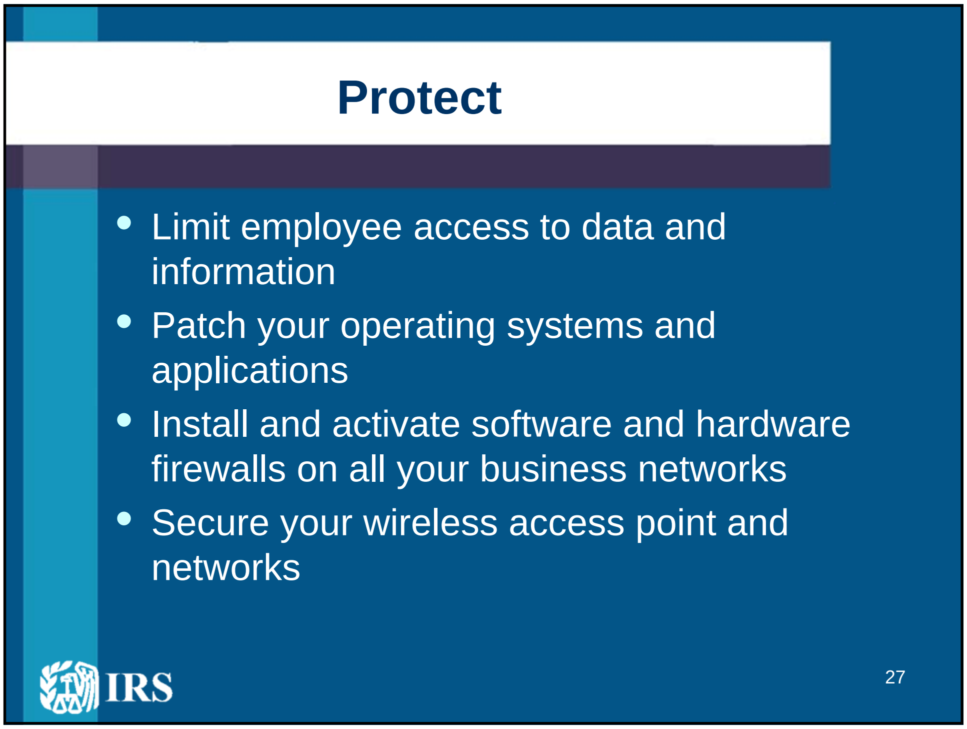
- Limit employee access to data and information
- Keep software/security programs updated
- Install firewalls on all business networks
- Secure all wireless access points
- Set up web and email filters



## The Fundamentals - Protect

- Use encryption for sensitive business information
- Dispose of old computers and media safely
- Train your employees
- Passwords (At least 16 characters long)
- Alpha / Numeric values / Punctuation
- Example: Meatthrowmetheball2017%!

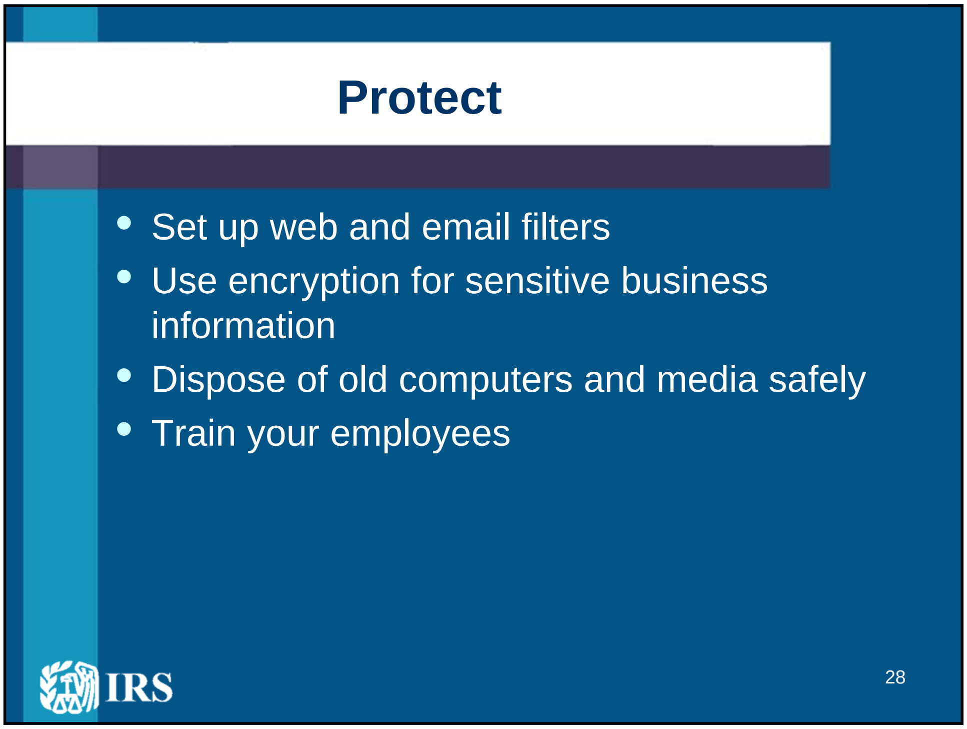
(This is a line is a phrase from a movie)



## Protect

- Limit employee access to data and information
- Patch your operating systems and applications
- Install and activate software and hardware firewalls on all your business networks
- Secure your wireless access point and networks

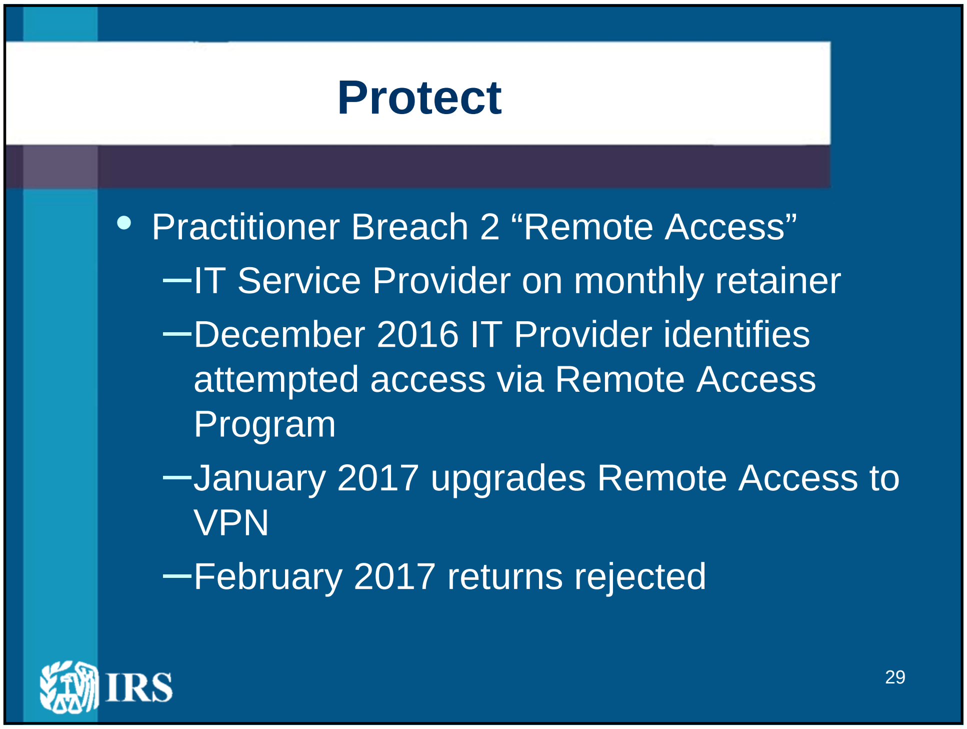
IRS



## Protect

- Set up web and email filters
- Use encryption for sensitive business information
- Dispose of old computers and media safely
- Train your employees

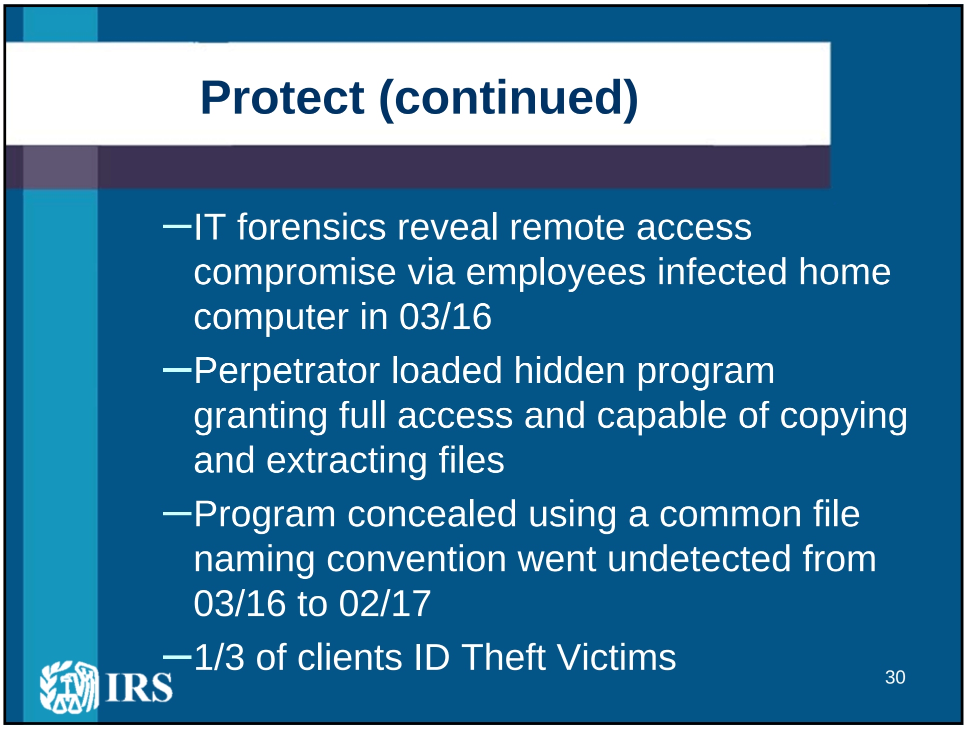
IRS



## Protect

- Practitioner Breach 2 “Remote Access”
  - —IT Service Provider on monthly retainer
  - —December 2016 IT Provider identifies attempted access via Remote Access Program
  - —January 2017 upgrades Remote Access to VPN
  - —February 2017 returns rejected

IRS

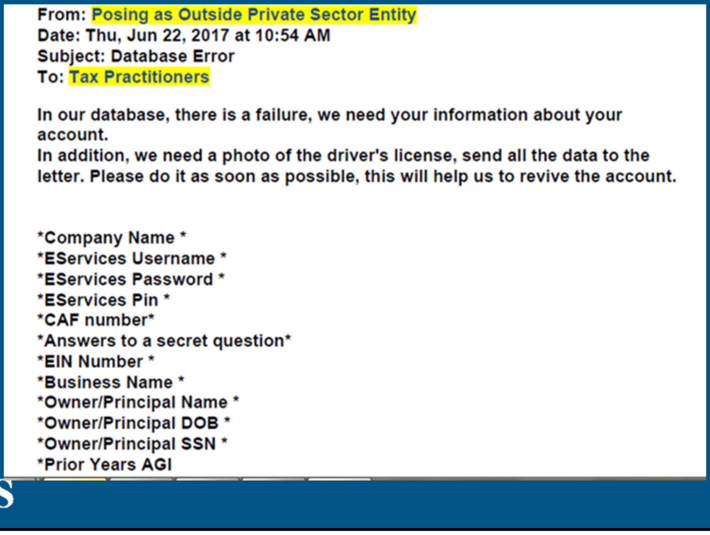


## Protect (continued)

- —IT forensics reveal remote access compromise via employees infected home computer in 03/16
- —Perpetrator loaded hidden program granting full access and capable of copying and extracting files
- —Program concealed using a common file naming convention went undetected from 03/16 to 02/17
- —1/3 of clients ID Theft Victims

IRS

# Protect (Phishing Emails)

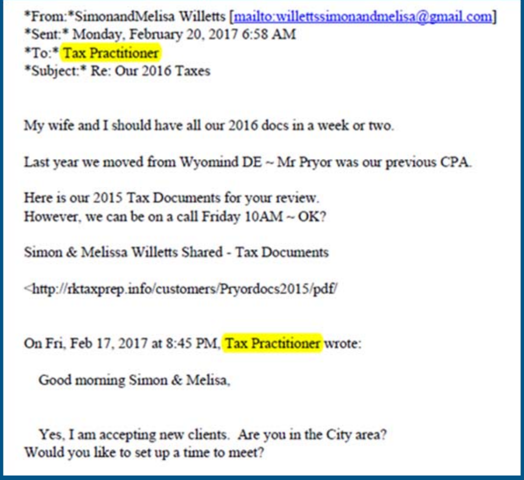


**From:** Posing as Outside Private Sector Entity
**Date:** Thu, Jun 22, 2017 at 10:54 AM
**Subject:** Database Error
**To:** Tax Practitioners

In our database, there is a failure, we need your information about your account.
In addition, we need a photo of the driver's license, send all the data to the letter. Please do it as soon as possible, this will help us to revive the account.

*Company Name *
*EServices Username *
*EServices Password *
*EServices Pin *
*CAF number*
*Answers to a secret question*
*EIN Number *
*Business Name *
*Owner/Principal Name *
*Owner/Principal DOB *
*Owner/Principal SSN *
*Prior Years AGI

# Phishing E-mail (Continued)



*From:*SimonandMelisa Willetts [mailto:willettssimonandmelisa@gmail.com]
*Sent:* Monday, February 20, 2017 6:58 AM
*To:* Tax Practitioner
*Subject:* Re: Our 2016 Taxes

My wife and I should have all our 2016 docs in a week or two.

Last year we moved from Wyomind DE ~ Mr Pryor was our previous CPA.

Here is our 2015 Tax Documents for your review.
However, we can be on a call Friday 10AM ~ OK?

Simon & Melissa Willetts Shared - Tax Documents

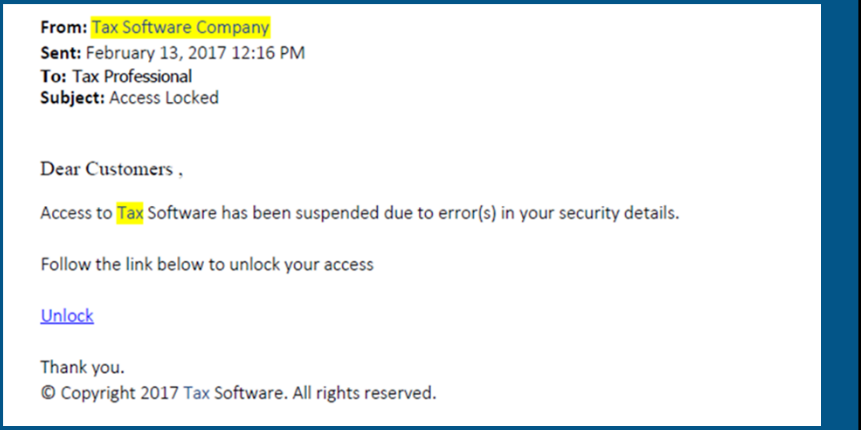
<http://rktaxprep.info/customers/Pryordocs2015/pdf/

On Fri, Feb 17, 2017 at 8:45 PM, Tax Practitioner wrote:

Good morning Simon & Melisa,

Yes, I am accepting new clients. Are you in the City area?
Would you like to set up a time to meet?

## Phishing E-mail (Continued)



**From:** Tax Software Company
**Sent:** February 13, 2017 12:16 PM
**To:** Tax Professional
**Subject:** Access Locked

Dear Customers ,

Access to Tax Software has been suspended due to error(s) in your security details.

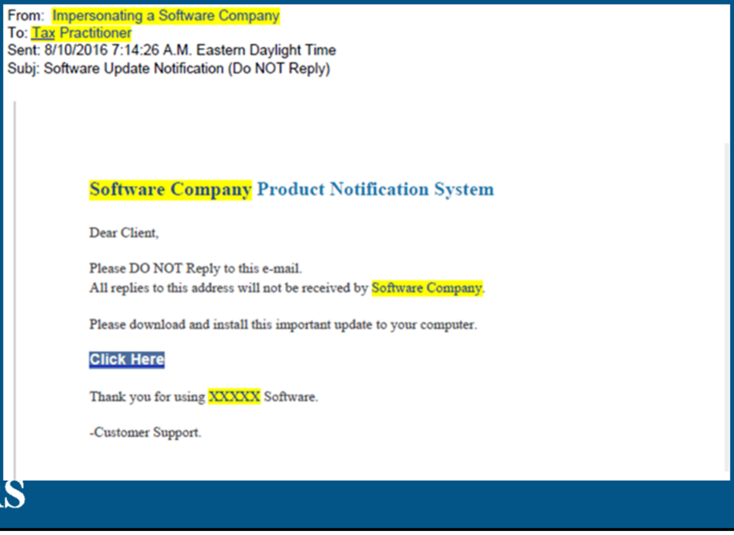
Follow the link below to unlock your access

Unlock

Thank you.
© Copyright 2017 Tax Software. All rights reserved.

33

## Phishing E-mail (Continued)



From: Impersonating a Software Company
To: Tax Practitioner
Sent: 8/10/2016 7:14:26 A.M. Eastern Daylight Time
Subj: Software Update Notification (Do NOT Reply)

**Software Company Product Notification System**

Dear Client,

Please DO NOT Reply to this e-mail.
All replies to this address will not be received by Software Company.

Please download and install this important update to your computer.

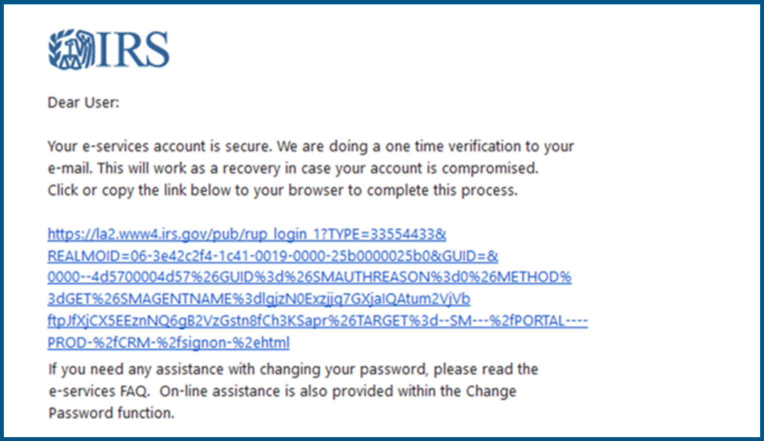
Click Here

Thank you for using XXXXX Software.

-Customer Support.

34

# Phishing E-mail (Continued)



IRS

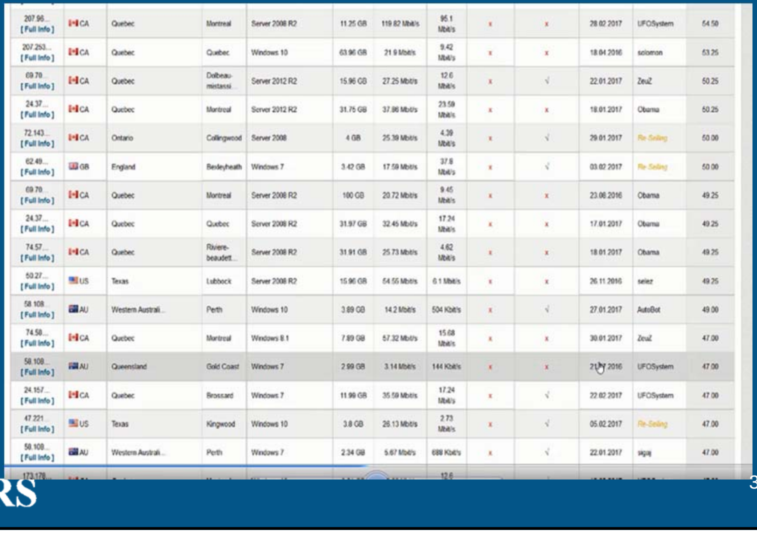
Dear User:

Your e-services account is secure. We are doing a one time verification to your e-mail. This will work as a recovery in case your account is compromised. Click or copy the link below to your browser to complete this process.

https://la2.www4.irs.gov/pub/rup_login_1?TYPE=33554433&REALMOID=06-3e42c2f4-1c41-0019-0000-25b0000025b0&GUID=&0000--4d5700004d57%26GUID%3d%26SMAUTHREASON%3d0%26METHOD%3dGET%26SMAGENTNAME%3dlgjzN0Exzjjq7GXjalQAtum2VjVbftpJfXjCX5EEznNQ6gB2VzGstn8fCh3KSapr%26TARGET%3d--SM---%2fPORTAL----PROD-%2fCRM-%2fsignon-%2ehtml

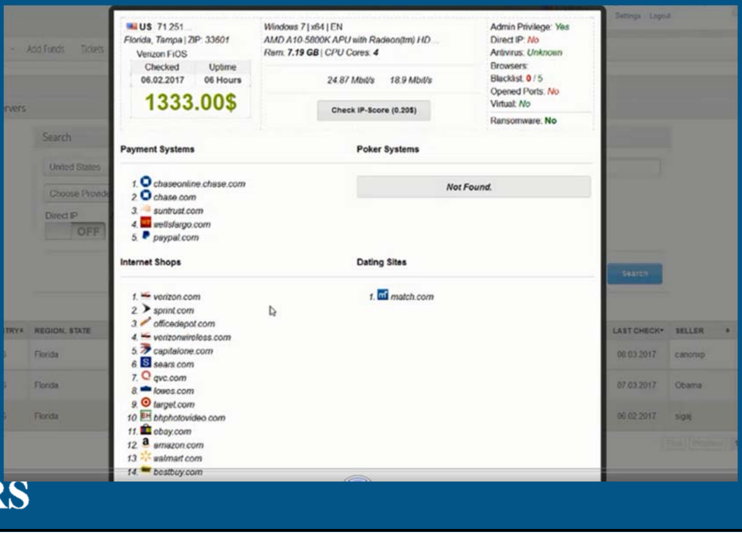
If you need any assistance with changing your password, please read the e-services FAQ.  On-line assistance is also provided within the Change Password function.

# Protect



| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 207.96...<br>[ Full Info ] | CA | Quebec | Montreal | Server 2008 R2 | 11.25 GB | 119.82 Mbit/s | 95.1 Mbit/s | x | x | 28.02.2017 | UFOSystem | 54.50 |
| 207.253...<br>[ Full Info ] | CA | Quebec | Quebec | Windows 10 | 63.96 GB | 21.9 Mbit/s | 9.42 Mbit/s | x | x | 18.04.2016 | solomon | 53.25 |
| 69.70...<br>[ Full Info ] | CA | Quebec | Dolbeau-mistassi... | Server 2012 R2 | 15.96 GB | 27.25 Mbit/s | 12.6 Mbit/s | x | √ | 22.01.2017 | ZeuZ | 50.25 |
| 24.37...<br>[ Full Info ] | CA | Quebec | Montreal | Server 2012 R2 | 31.75 GB | 37.86 Mbit/s | 23.59 Mbit/s | x | x | 18.01.2017 | Obama | 50.25 |
| 72.143...<br>[ Full Info ] | CA | Ontario | Collingwood | Server 2008 | 4 GB | 25.39 Mbit/s | 4.39 Mbit/s | x | √ | 29.01.2017 | Re-Selling | 50.00 |
| 62.49...<br>[ Full Info ] | GB | England | Bexleyheath | Windows 7 | 3.42 GB | 17.59 Mbit/s | 37.8 Mbit/s | x | √ | 03.02.2017 | Re-Selling | 50.00 |
| 69.70...<br>[ Full Info ] | CA | Quebec | Montreal | Server 2008 R2 | 100 GB | 20.72 Mbit/s | 9.45 Mbit/s | x | x | 23.08.2016 | Obama | 49.25 |
| 24.37...<br>[ Full Info ] | CA | Quebec | Quebec | Server 2008 R2 | 31.97 GB | 32.45 Mbit/s | 17.24 Mbit/s | x | x | 17.01.2017 | Obama | 49.25 |
| 74.57...<br>[ Full Info ] | CA | Quebec | Riviere-beaudett... | Server 2008 R2 | 31.91 GB | 25.73 Mbit/s | 4.62 Mbit/s | x | x | 18.01.2017 | Obama | 49.25 |
| 50.27...<br>[ Full Info ] | US | Texas | Lubbock | Server 2008 R2 | 15.96 GB | 54.55 Mbit/s | 6.1 Mbit/s | x | x | 26.11.2016 | selez | 49.25 |
| 58.108...<br>[ Full Info ] | AU | Western Australi... | Perth | Windows 10 | 3.89 GB | 14.2 Mbit/s | 504 Kbit/s | x | √ | 27.01.2017 | AutoBot | 49.00 |
| 74.58...<br>[ Full Info ] | CA | Quebec | Montreal | Windows 8.1 | 7.89 GB | 57.32 Mbit/s | 15.68 Mbit/s | x | x | 30.01.2017 | ZeuZ | 47.00 |
| 58.108...<br>[ Full Info ] | AU | Queensland | Gold Coast | Windows 7 | 2.99 GB | 3.14 Mbit/s | 144 Kbit/s | x | x | 21.[illegible] 2016 | UFOSystem | 47.00 |
| 24.157...<br>[ Full Info ] | CA | Quebec | Brossard | Windows 7 | 11.99 GB | 35.59 Mbit/s | 17.24 Mbit/s | x | √ | 22.02.2017 | UFOSystem | 47.00 |
| 47.221...<br>[ Full Info ] | US | Texas | Kingwood | Windows 10 | 3.8 GB | 26.13 Mbit/s | 2.73 Mbit/s | x | √ | 05.02.2017 | Re-Selling | 47.00 |
| 58.108...<br>[ Full Info ] | AU | Western Australi... | Perth | Windows 7 | 2.34 GB | 5.67 Mbit/s | 688 Kbit/s | x | √ | 22.01.2017 | sigaj | 47.00 |
| 173.178... | | | | | | | 12.6 | | | | | |

## Protect



US 71.251...
Florida, Tampa | ZIP: 33601
Verizon FiOS

| Checked | Uptime |
|---|---|
| 06.02.2017 | 06 Hours |

1333.00$

Windows 7 | x64 | EN
AMD A10-5800K APU with Radeon(tm) HD ...
Ram: 7.19 GB | CPU Cores: 4

24.87 Mbit/s 18.9 Mbit/s

Check IP-Score (0.20$)

Admin Privilege: Yes
Direct IP: No
Antivirus: Unknown
Browsers:
Blacklist: 0 / 5
Opened Ports: No
Virtual: No
Ransomware: No

**Payment Systems**

1. chaseonline.chase.com
2. chase.com
3. suntrust.com
4. wellsfargo.com
5. paypal.com

**Poker Systems**

Not Found.

**Internet Shops**

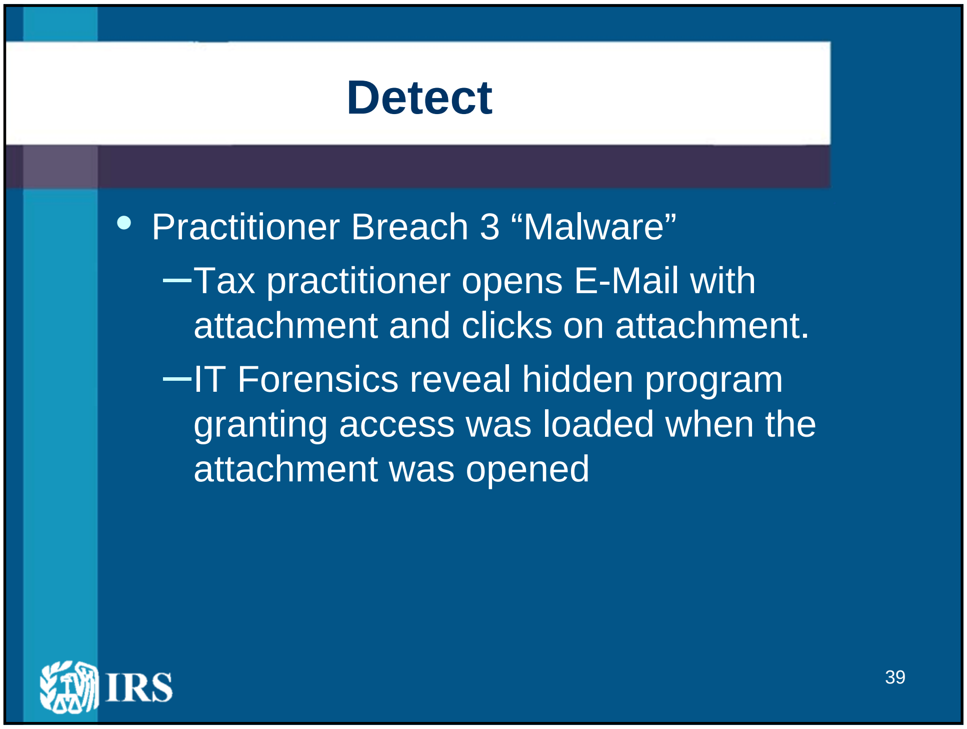
1. verizon.com
2. sprint.com
3. officedepot.com
4. verizonwireless.com
5. capitalone.com
6. sears.com
7. qvc.com
8. lowes.com
9. target.com
10. bhphotovideo.com
11. ebay.com
12. amazon.com
13. walmart.com
14. bestbuy.com

**Dating Sites**

1. match.com

## The Fundamentals - Detect

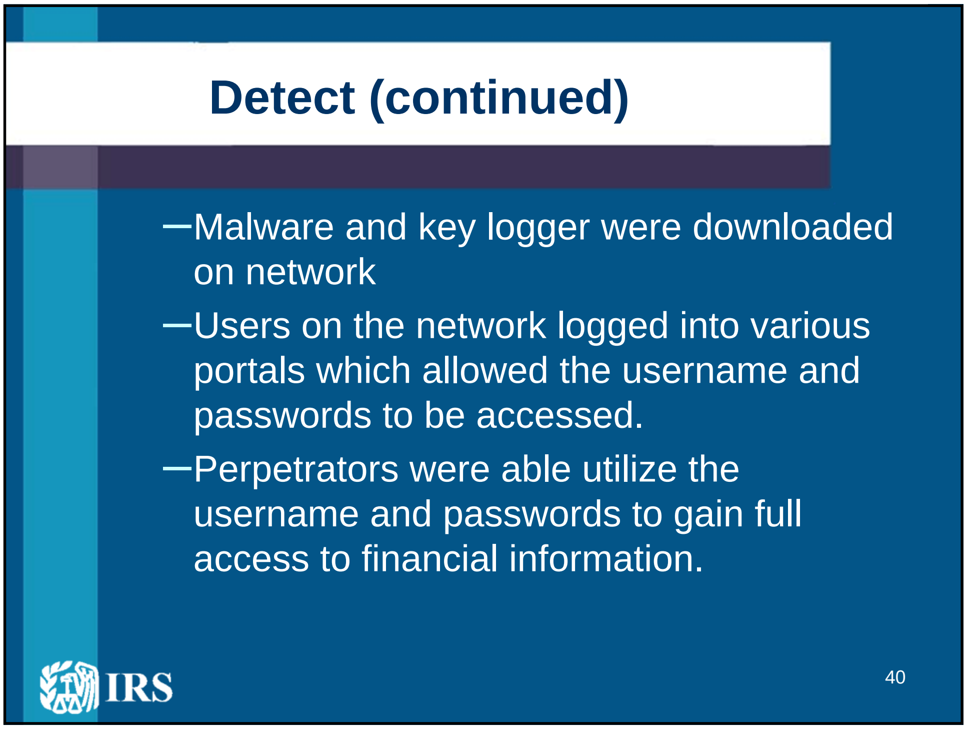
- Install and update anti-virus, spyware and other malware programs
- Maintain and monitor logs



## Detect

- Practitioner Breach 3 “Malware”
  - Tax practitioner opens E-Mail with attachment and clicks on attachment.
  - IT Forensics reveal hidden program granting access was loaded when the attachment was opened

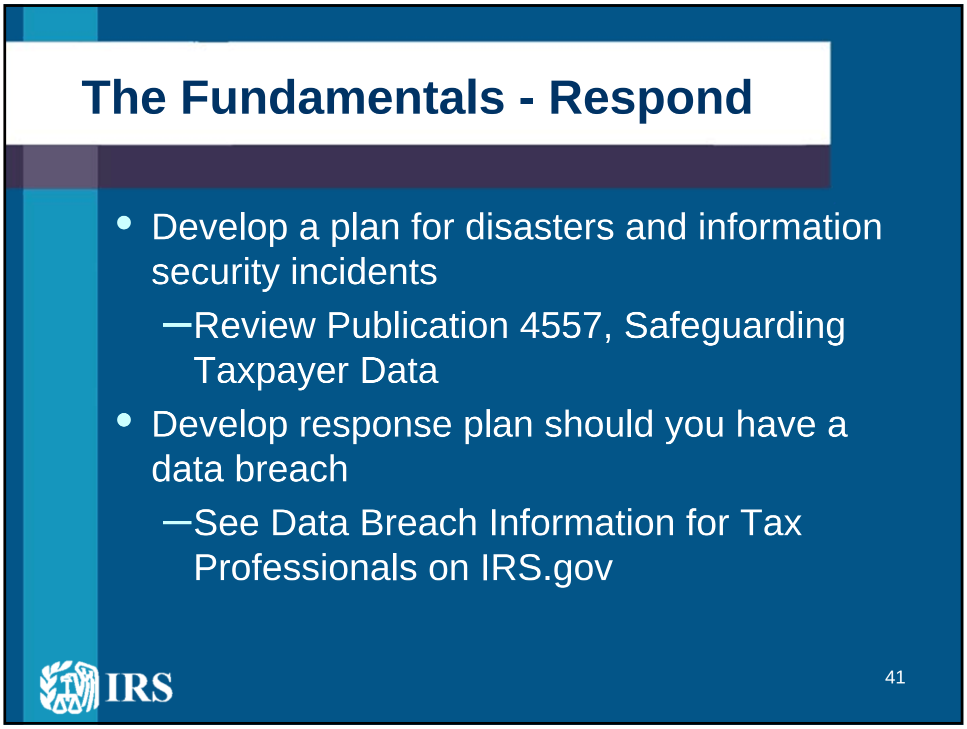
39



## Detect (continued)

- Malware and key logger were downloaded on network
- Users on the network logged into various portals which allowed the username and passwords to be accessed.
- Perpetrators were able utilize the username and passwords to gain full access to financial information.

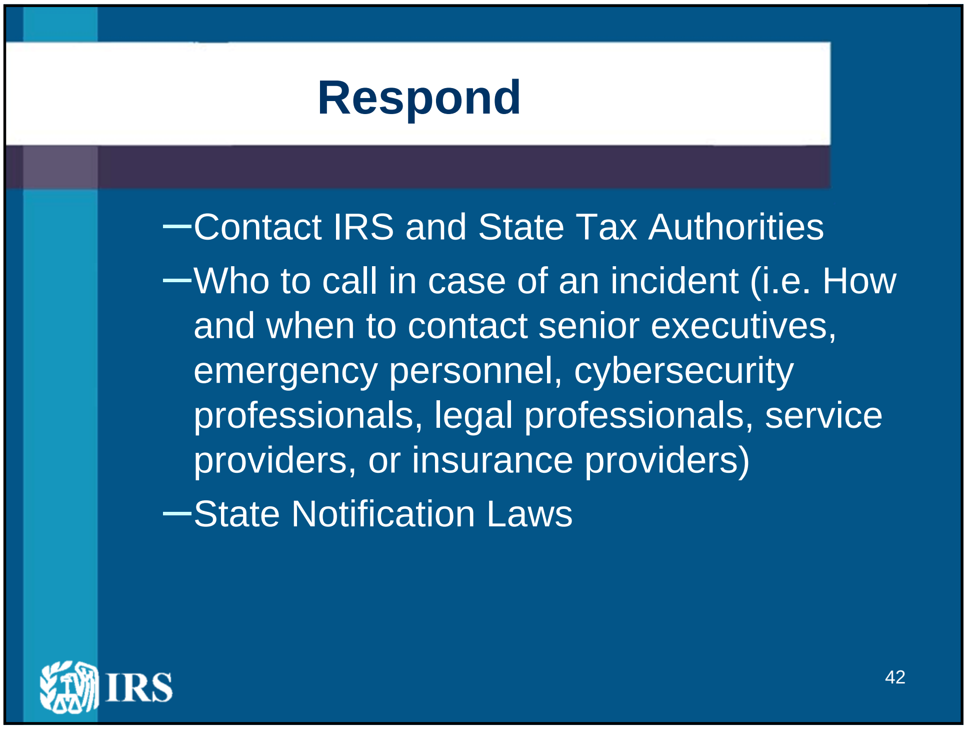
40



## The Fundamentals - Respond

- Develop a plan for disasters and information security incidents
  - Review Publication 4557, Safeguarding Taxpayer Data
- Develop response plan should you have a data breach
  - See Data Breach Information for Tax Professionals on IRS.gov

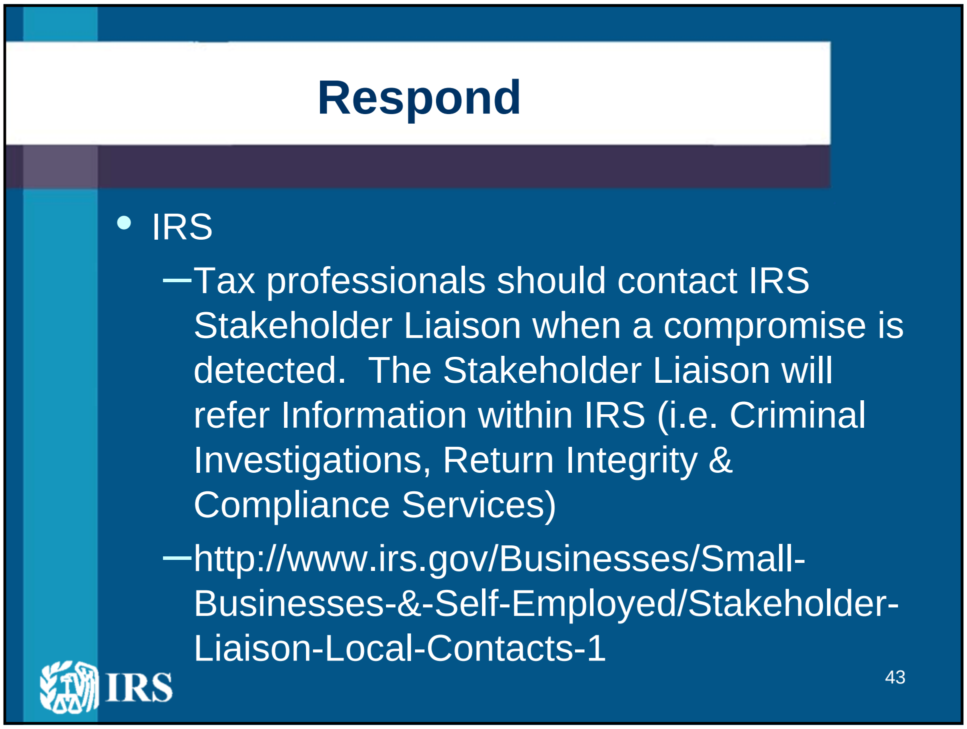
IRS



## Respond

- Contact IRS and State Tax Authorities
- Who to call in case of an incident (i.e. How and when to contact senior executives, emergency personnel, cybersecurity professionals, legal professionals, service providers, or insurance providers)
- State Notification Laws

IRS

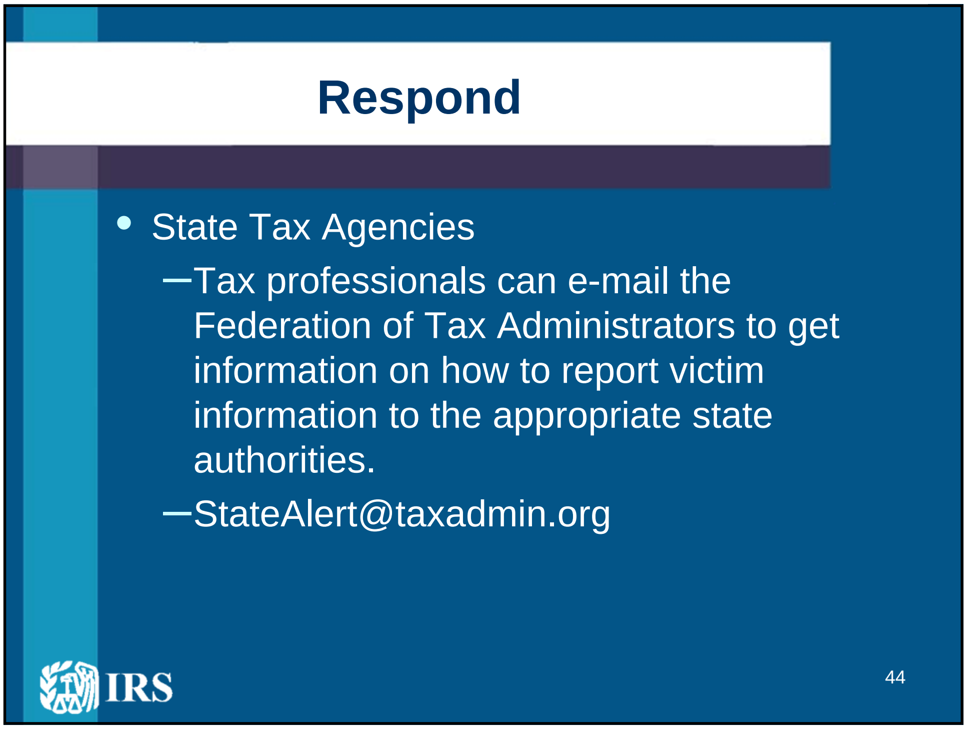


## Respond

- IRS
  - Tax professionals should contact IRS Stakeholder Liaison when a compromise is detected.  The Stakeholder Liaison will refer Information within IRS (i.e. Criminal Investigations, Return Integrity & Compliance Services)
  - http://www.irs.gov/Businesses/Small-Businesses-&-Self-Employed/Stakeholder-Liaison-Local-Contacts-1

IRS

43

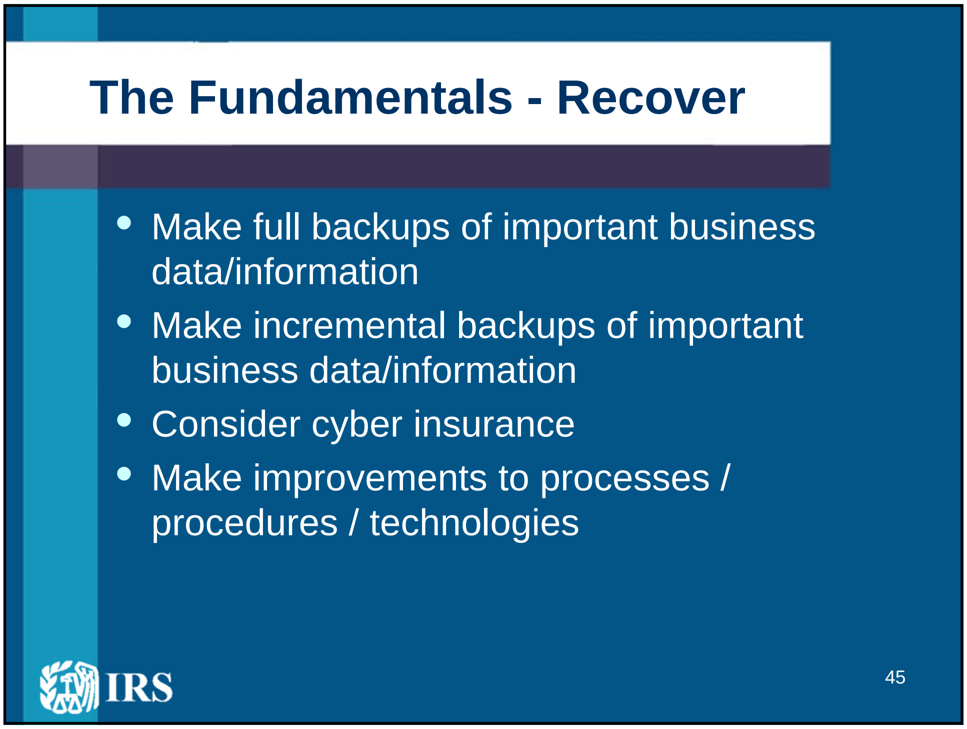


## Respond

- State Tax Agencies
  - Tax professionals can e-mail the Federation of Tax Administrators to get information on how to report victim information to the appropriate state authorities.
  - StateAlert@taxadmin.org

IRS

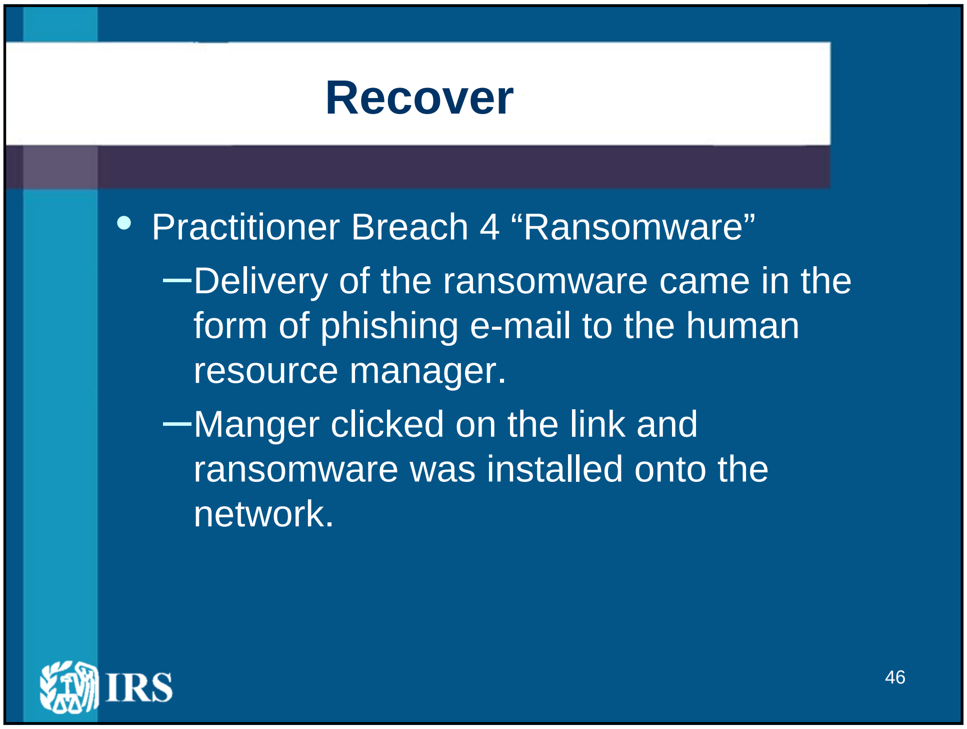
44



## The Fundamentals - Recover

- Make full backups of important business data/information
- Make incremental backups of important business data/information
- Consider cyber insurance
- Make improvements to processes / procedures / technologies

45



## Recover

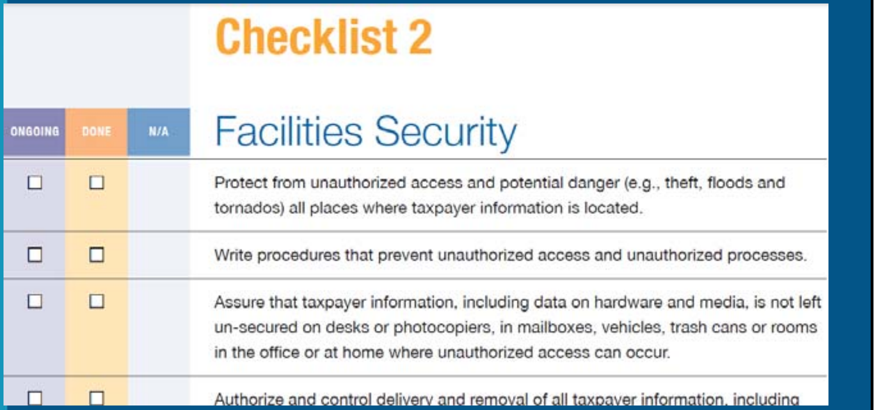
- Practitioner Breach 4 “Ransomware”
  - Delivery of the ransomware came in the form of phishing e-mail to the human resource manager.
  - Manger clicked on the link and ransomware was installed onto the network.

46

## Recover

- Ransomware shutdown the system and demanded payment of $1,500 in Bitcoins.
- Perpetrators threatened to sell the PII on the dark web.
- Tax practitioner paid $1,500 and had IT specialist remove and restore the data using backup tapes

## IRS Publication 4557

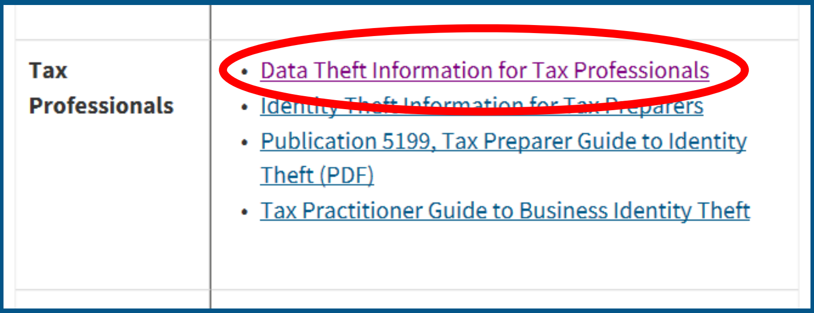


### Checklist 2

| ONGOING | DONE | N/A | Facilities Security |
|---|---|---|---|
| □ | □ |  | Protect from unauthorized access and potential danger (e.g., theft, floods and tornados) all places where taxpayer information is located. |
| □ | □ |  | Write procedures that prevent unauthorized access and unauthorized processes. |
| □ | □ |  | Assure that taxpayer information, including data on hardware and media, is not left un-secured on desks or photocopiers, in mailboxes, vehicles, trash cans or rooms in the office or at home where unauthorized access can occur. |
| □ | □ |  | Authorize and control delivery and removal of all taxpayer information, including |

## Data Theft? Here’s what to do

www.irs.gov/identitytheft



| | |
|---|---|
| **Tax Professionals** | • Data Theft Information for Tax Professionals<br>• Identity Theft Information for Tax Preparers<br>• Publication 5199, Tax Preparer Guide to Identity Theft (PDF)<br>• Tax Practitioner Guide to Business Identity Theft |

IRS

49

## Data Theft? Here’s what to do

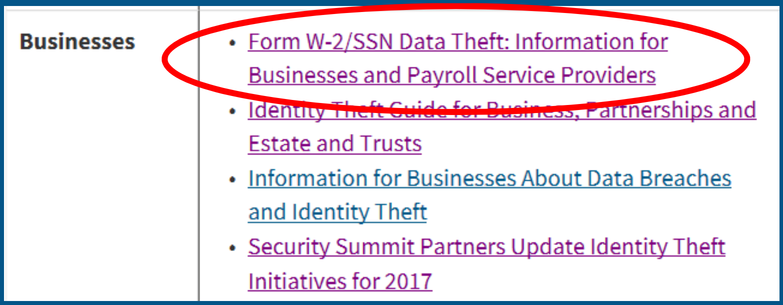
- Contact the IRS and law enforcement
  - IRS Stakeholder Liaisons
- Contact states in which you prepare state returns
  - StateAlert@taxadmin.org
- Contact experts
  - Cyber and insurance agency
- Contact clients and other services
  - See FTC suggestions

IRS

50

## Protect Your Clients

- Warn employers of W-2 scam
- Information at www.irs.gov/identitytheft



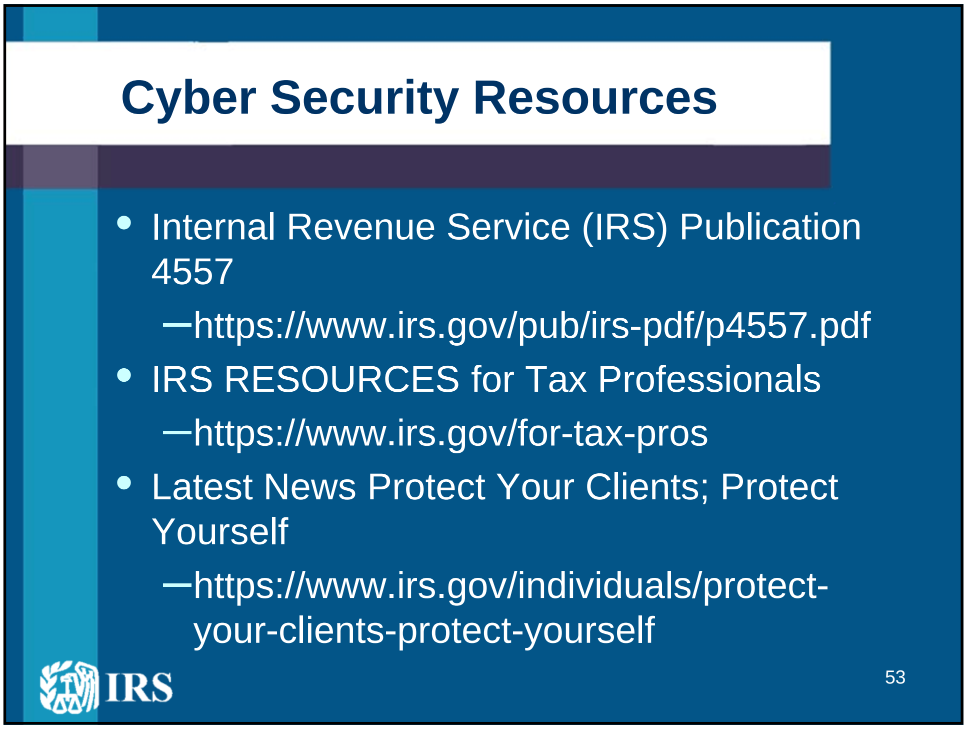
| Businesses | • Form W-2/SSN Data Theft: Information for Businesses and Payroll Service Providers<br>• Identity Theft Guide for Business, Partnerships and Estate and Trusts<br>• Information for Businesses About Data Breaches and Identity Theft<br>• Security Summit Partners Update Identity Theft Initiatives for 2017 |
|---|---|

IRS

## Protect Your Clients

- Complete trusted customer information fields for individual returns
  - –Example: Driver’s license number
  - –Example: Authentication document
- Complete trusted customer information fields for business returns
  - –Example: Name and SSN of person signing return

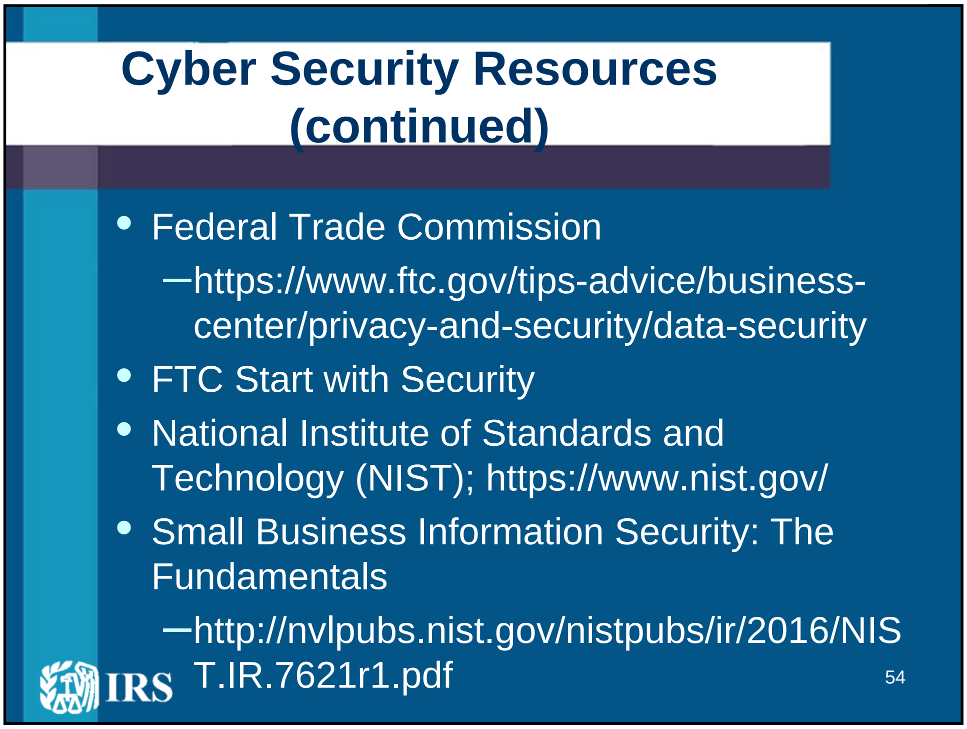
IRS



## Cyber Security Resources

- Internal Revenue Service (IRS) Publication 4557
  - https://www.irs.gov/pub/irs-pdf/p4557.pdf
- IRS RESOURCES for Tax Professionals
  - https://www.irs.gov/for-tax-pros
- Latest News Protect Your Clients; Protect Yourself
  - https://www.irs.gov/individuals/protect-your-clients-protect-yourself

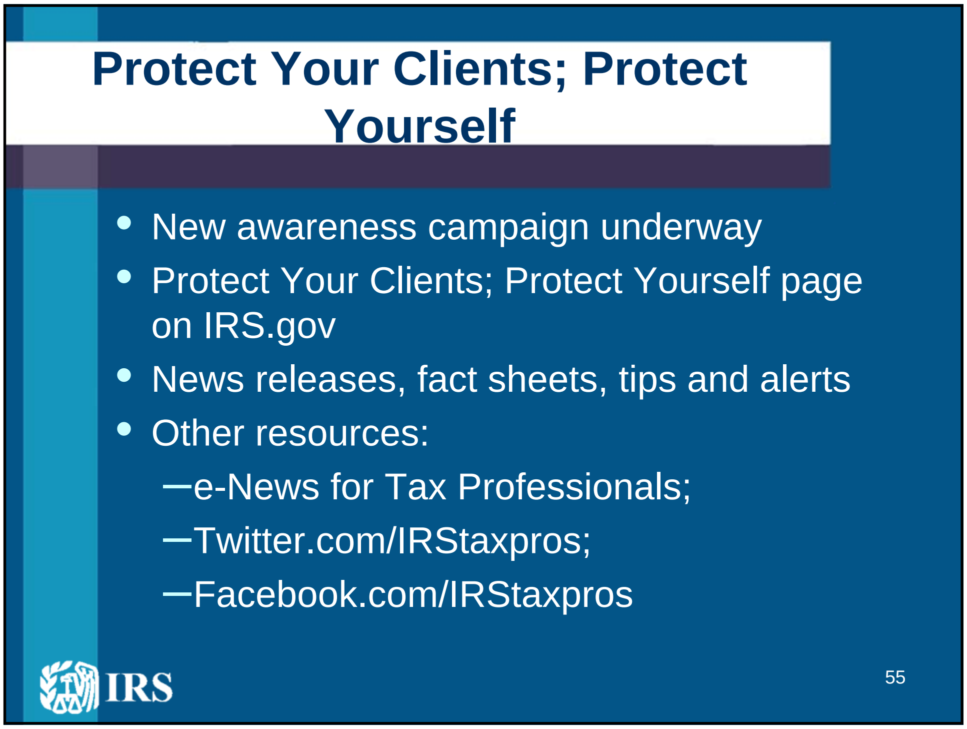
53



## Cyber Security Resources (continued)

- Federal Trade Commission
  - https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security
- FTC Start with Security
- National Institute of Standards and Technology (NIST); https://www.nist.gov/
- Small Business Information Security: The Fundamentals
  - http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf

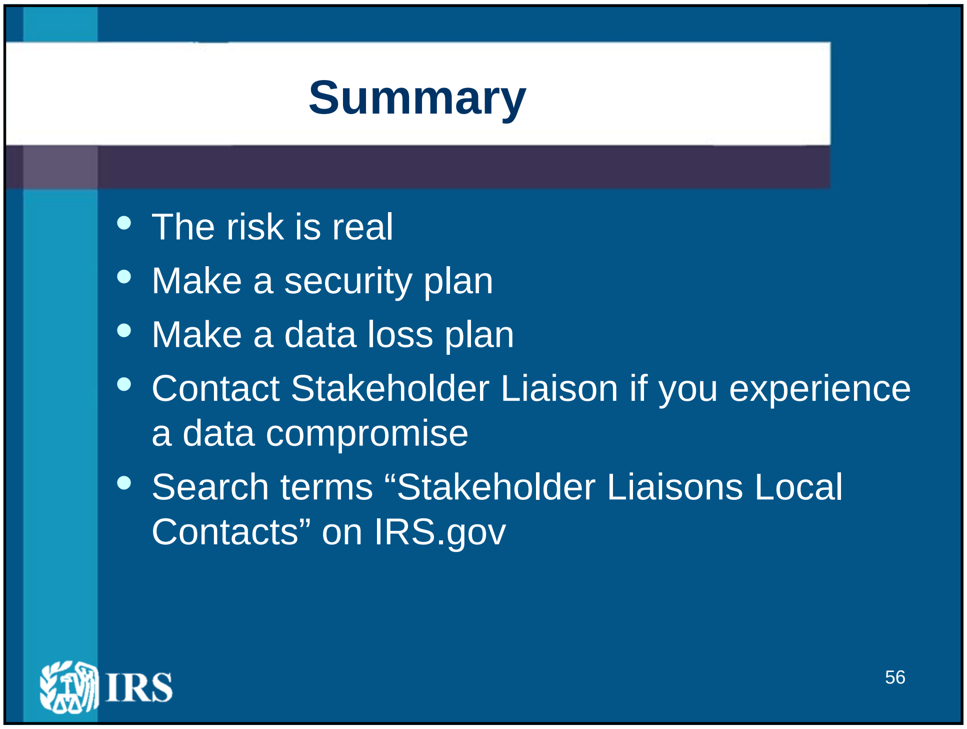
54



## Protect Your Clients; Protect Yourself

- New awareness campaign underway
- Protect Your Clients; Protect Yourself page on IRS.gov
- News releases, fact sheets, tips and alerts
- Other resources:
  - e-News for Tax Professionals;
  - Twitter.com/IRStaxpros;
  - Facebook.com/IRStaxpros

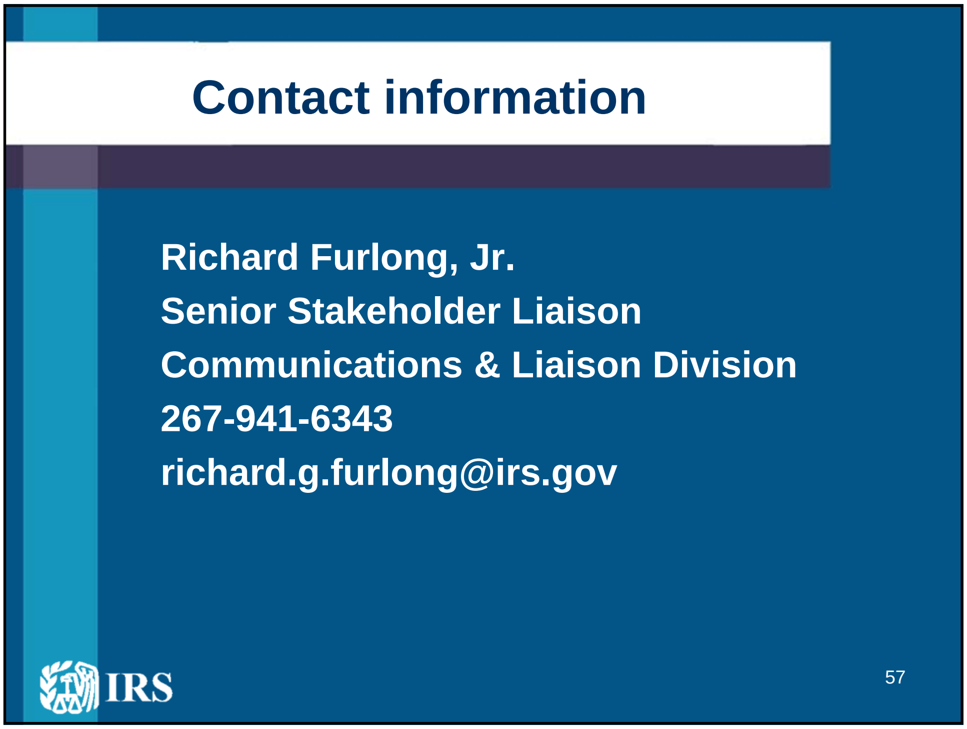
IRS



## Summary

- The risk is real
- Make a security plan
- Make a data loss plan
- Contact Stakeholder Liaison if you experience a data compromise
- Search terms “Stakeholder Liaisons Local Contacts” on IRS.gov

IRS



## Contact information

Richard Furlong, Jr.
Senior Stakeholder Liaison
Communications & Liaison Division
267-941-6343
richard.g.furlong@irs.gov

IRS