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 real; 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

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
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

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

**How to Report a Preparer Account Takeover**

Preparers should contact the IRS Stakeholder Liaison for their state.


---

**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
Spear Phishing

Original Message

Subject: Tax return

Date: Fri, February 24, 2017 5:10 am
To:

Hello,

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

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

Regards,

[Email body]

- Original message may be ungrammatical or oddly worded.
-Thief targets specific audience - such as tax pros.
- 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 eServices and EFIN details for 2017 Tax season.

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

[Link]

We will suspend any Tax Preparer who fails to renew and follow this update within 30 days.

Sincerely,
IRS e-Services
Account Takeover

Fake e-Services site copies real one

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)

Protect your EFIN
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

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

The Fundamentals

NIST’s five action-item categories:

- Identify
- Protect
- Detect
- Respond
- Recover
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

<table>
<thead>
<tr>
<th>Example: Client files</th>
<th>Payroll Data</th>
<th>Employee Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost of revelation (Confidentiality)</td>
<td>High</td>
<td></td>
</tr>
<tr>
<td>Cost to verify information (Integrity)</td>
<td>High</td>
<td></td>
</tr>
<tr>
<td>Cost of lost access (Availability)</td>
<td>High</td>
<td></td>
</tr>
<tr>
<td>Cost of lost work</td>
<td>High</td>
<td></td>
</tr>
<tr>
<td>Fines, penalties, customer notification</td>
<td>High</td>
<td></td>
</tr>
<tr>
<td>Other legal costs</td>
<td>High</td>
<td></td>
</tr>
<tr>
<td>Reputational / public relations costs</td>
<td>High</td>
<td></td>
</tr>
<tr>
<td>Cost to identify and repair problem</td>
<td>High</td>
<td></td>
</tr>
</tbody>
</table>

Overall Score: High
Identify

• Develop an Inventory of IT Related Equipment

<table>
<thead>
<tr>
<th>Description (e.g. nickname, make, model, serial number, service ID, other identifying information)</th>
<th>Location</th>
<th>Type of information the product comes in contact with.</th>
<th>Overall Potential Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Cell phone: Type = Sonic; Version = 9.0; ID = “Police Box”</td>
<td>Mobile T&amp;B Network</td>
<td>Email; Calendar; Customer Contact Information; Photos; Social Media; Locations; Medical Dictionary/Application</td>
<td>High</td>
</tr>
<tr>
<td>2 Computers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 Printers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 Wireless Routers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 Remote Access</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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
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

Protect

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

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
Protect (Phishing Emails)

From: Fake 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:* Simon & Melissa Willetts [mailto:willetts@simonandmelissa@gmail.com]
*Sent:* Monday, February 20, 2017 6:56 AM
*To:* Tax Practitioners
*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 Wyoming 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 - Tax Documents

*http://drxtaxprep.com/customers/Pryor/docs2015/pdf*

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

Good morning Simon & Melissa,

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.

Phishing E-mail (Continued)

From: Impersonating a Software Company
To: Tax Practitioner
Sent: 8/10/2016 7:14:26 A.M. Eastern Daylight Time
Subject: 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.
Phishing E-mail (Continued)

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://fa2.wwv4.irs.gov/pub/hs_userlogin_1?TYPE=333544338

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Address</th>
<th>Phone</th>
<th>Email</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>John Smith</td>
<td>123 Main St.</td>
<td>555-1234</td>
<td><a href="mailto:john@email.com">john@email.com</a></td>
<td>Active</td>
</tr>
<tr>
<td>Jane Doe</td>
<td>456 Oak Ave.</td>
<td>555-5678</td>
<td><a href="mailto:jane@email.com">jane@email.com</a></td>
<td>Active</td>
</tr>
<tr>
<td>Alex Johnson</td>
<td>789 Pine Rd.</td>
<td>555-9876</td>
<td><a href="mailto:alex@email.com">alex@email.com</a></td>
<td>Active</td>
</tr>
<tr>
<td>Michael Lee</td>
<td>101 Maple Ln.</td>
<td>555-2345</td>
<td><a href="mailto:michael@email.com">michael@email.com</a></td>
<td>Active</td>
</tr>
</tbody>
</table>

11/27/2017
Protect

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

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.
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

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
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)

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
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

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.
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

Facilities Security

- Protect from unauthorized access and potential danger (e.g., theft, floods and tornadoes) all places where taxpayer information is located.
- Write procedures that prevent unauthorized access and unauthorized processes.
- Ensure 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

<table>
<thead>
<tr>
<th>Tax Professionals</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Data Theft Information for Tax Professionals</td>
</tr>
<tr>
<td>• Identity Theft Information for Tax Preparers</td>
</tr>
<tr>
<td>• Publication 5199, Tax Preparer Guide to Identity Theft (PDF)</td>
</tr>
<tr>
<td>• Tax Practitioner Guide to Business Identity Theft</td>
</tr>
</tbody>
</table>

• 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
Protect Your Clients

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

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

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
Cyber Security Resources

- Internal Revenue Service (IRS) Publication 4557
- IRS RESOURCES for Tax Professionals
- Latest News Protect Your Clients; Protect Yourself

Cyber Security Resources (continued)

- Federal Trade Commission
- FTC Start with Security
- National Institute of Standards and Technology (NIST); https://www.nist.gov/
- Small Business Information Security: The Fundamentals
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

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
Contact information

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