Cybersecurity: What Every Practitioner Needs to Know!

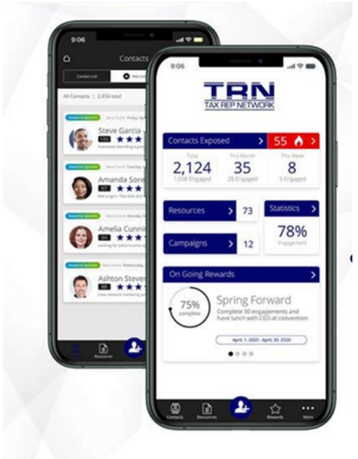
Joseph McCarthy, CPA, Internal Revenue Service
Eric Green, Esq, Green & Sklarz LLC
Dawn Brolin, CPA, CFE, Powerful Accounting LLC

TRN
TAX REP NETWORK

Eric Green, Esq.

- Managing partner in Green & Sklarz LLC, a boutique tax firm with offices in Connecticut and New York.
- Focus is civil and criminal taxpayer representation before the Department of Justice Tax Division, Internal Revenue Service and state Departments of Revenue Services.
- Eric is a contributing columnist for Bloomberg Tax and has served as a columnist for CCH's Journal of Practice & Procedure.
- Attorney Green is the past Chair of the Executive Committee of the Connecticut Bar Association's Tax Section.
- Eric is a Fellow of the American College of Tax Counsel ("ACTC").

Eric Green, Esq.



- Eric is the host of the weekly Tax Rep Network Podcast
- Eric is the founder of Tax Rep Network, an online community designed to help tax professionals build their IRS Representation Practice
- He is the author of the Accountant's Guides in IRS Representation
- Partnered with UConn and creator of the IRS Representation Certificate Program
- Creator of the Tax Rep App

The App

- Tax Preparation service line is ready!
- What it does
- Same App with the rep lines
- https://rapidfunnel.com/getting-started/tax-rep-network/

Housekeeping….

- 4 Attendance pop-up attendance checks
- Must do at least 3 of the 4 and be on for at least 50 minutes
- Look for a link for your certificate
- Issues? Email us at team@taxrepllc.com

TRN
TAX REP NETWORK

Poll

According to Deloitte, what percentage of cyber attacks start through email?

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)

TRN
TAX REP NETWORK

“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

TRN
TAX REP NETWORK

“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)

“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

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
- Use Publication 4557, Safeguarding Taxpayer Data, to help create plan
- Use Publication 5709 Creating a Written Information Security Plan for your tax and accounting practice

PTIN renewal check box

Data Security Responsibilities

- As a paid tax return preparer, I am aware of my legal obligation to have a data security plan and to provide data and system security protections for all taxpayer information. Check the box to confirm you are aware of this responsibility.

Step 3: Educate yourself on phishing scams

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

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 (cont.)

- 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

Put all the pieces together….

Liscio

Practice Protect

SmartVault

Step 4: Recognize the signs of client data theft

- Tax professionals should learn the signs of a possible data theft
- Data theft may result in fraudulent tax returns being filed in their clients' names
- Cybercriminals are tax savvy in their attempts to gain sensitive tax data

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 (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

Signs of client data theft (cont.)

- The number of returns filed with tax practitioner's Electronic Filing Identification Number (EFIN) exceeds number of clients;
- Tax professionals or clients responding to emails that practitioner did not send

Signs of client data theft (cont.)

- Network computers running slower than normal;
- Computer cursors moving or changing numbers without touching the keyboard;
- Network computers locking out tax practitioners.

Tax professionals monitor your accounts

- EFIN accounts
  - Too many returns filed with your EFIN
  - Contact e-Help Desk (866) 255-0654
- PTIN accounts
  - Too many returns filed
  - Complete Form 14157
- CAF accounts
  - Signs of identity theft
  - Contact Practitioner Priority Service

Monitor your EFIN

- To access “Returns Filed Per EFIN” information, follow these steps:
  - Go to e-Services
  - Access e-File Application
  - Search by name
  - Select “EFIN Status”

Monitor your PTIN

- To access “Returns Filed Per PTIN” information, follow these steps:
  - Log into your PTIN account
  - From the Main Menu, find “Additional Activities”
  - Under Additional Activities, select “Summary of Returns Filed.”

Monitor your CAF number

You can obtain a list of your POAs by:

- Filing a Freedom of Information Act (FOIA) request with the IRS.
- The filing is called a Centralized Authorization File (CAF) FOIA request letter.
- Type “CAF FOIA” in the search box at www.irs.gov for a sample FOIA letter.
- Register for an IRS Tax Pro Account and link the account to your CAF. Using the Tax pro account you can monitor all the 2848s and 8821s under your CAF number.

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 – Report immediately

Contact:

- IRS Stakeholder Liaison. Search “stakeholder liaisons” on IRS.gov
- Contact experts
  - Insurance company
  - Computer security experts
- Law enforcement

Data Compromise Action Items – Report immediately (cont.)

Contact state agencies:

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

Data Compromise Action Items – Report immediately (cont.)

Contact:

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

Review guidance at IRS.gov/identitytheft

Poll

Have you implemented a software solution for your cyber security?

Solutions We Use

SmartVault

Liscio

Practice Protect

Join us on August 2nd

https://taxrepllc.com/20240802-breach/

TRN
TAX REP NETWORK

Resources

- Publication 4557, Safeguarding Taxpayer Data
- Publication 5293, Data Security Resource Guide for Tax Professionals
- Small Business Information Security – The Fundamentals at NIST.gov
- Publication 5709 Creating a Written Information Security Plan for your tax and accounting practice

Resources (cont.)

IRS.gov websites:

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

Resources (cont.)

www.IRS.gov/subscribe

- E-news for tax professionals
- E-news for small businesses

Thank You!