Welcome

Tax Security 2.0 – A Tax Pro's Security Checklist

D ate: 11/16/2023

Topics

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)

"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

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

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

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 – 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.

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

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**

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.**