Protect Your Clients; Protect Yourself

Data Security Resource Guide for Tax Professionals

The Data Security Resource Guide for Tax Professionals is intended to provide a basic understanding of minimal steps to protect client data. All tax professionals are encouraged to work with cybersecurity professionals to ensure secure systems. Protecting taxpayer data from theft and disclosure is your responsibility.

Get Started

The Security Summit – the partnership between the Internal Revenue Service, state tax agencies and the tax industry – reminds all tax professionals that everyone has a role in protecting taxpayer data.

The Financial Services Modernization Act of 1999, also known as Gramm-Leach-Bliley Act, requires certain entities – including tax return preparers – to create and maintain a security plan for the protection of client data.

Here are two publications to help you get started:

- **IRS Publication 4557, Safeguarding Taxpayer Data**
  This publication provides an overview of tax professionals' obligations to protect taxpayer information and provides a step-by-step checklist for how to create and maintain a security plan for your digital network and office.
- **NIST's Small Business Information Security – The Fundamentals**
  The National Institute of Standards and Technology (NIST) is a branch of the U.S. Commerce Department. It sets the information security framework for federal agencies. It also produced this document to provide small businesses with an overview of those steps to security data. Its focus is on five principles: identify, protect, detect, respond and recover.

Don't forget **Publication 1345**, Handbook for Authorized IRS e-File Providers, which outlines your responsibility as an Electronic Return Originator, including in the area of e-File security and privacy.

What Can You Do?

- Learn to recognize phishing emails, especially those pretending to be from the IRS, e-Services, a tax software provider or cloud storage provider. Never open a link or any attachment from a suspicious email. Remember: The IRS never initiates initial email contact with tax pros about returns, refunds or requests for sensitive financial or password information.
- Create a data security plan using IRS **Publication 4557**, Safeguarding Taxpayer Data, and **Small Business Information Security – The Fundamentals**, by the National Institute of Standards and Technology.
- Review internal controls:
  - Install anti-malware/anti-virus security software on all devices (laptops, desktops, routers, tablets and phones) and keep software set to automatically update.

- Use strong and unique passwords of 8 or more mixed characters, password protect all wireless devices, use a phrase or words that are easily remembered and change passwords periodically.
- Encrypt all sensitive files/emails and use strong password protections.
- Back up sensitive data to a safe and secure external source not connected fulltime to a network.
- Make a final review of return information – especially direct deposit info - prior to e-filing.
- Wipe clean or destroy old computer hard drives and printers that contain sensitive data.
- Limit access to taxpayer data to individuals who need to know.
- Check IRS e-Services account weekly for number of returns filed with EFIN.

- Report any data thefts or losses to the appropriate IRS Stakeholder Liaison.
- Stay connected to the IRS through subscriptions to e-News for Tax Professionals, QuickAlerts and Social Media.

Learn the Signs of Data Theft

You or your firm may be a victim and not even know it. Here are some common clues to data theft:

- Client e-filed returns begin to reject because returns with their Social Security numbers were already filed;
- 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;
- Clients receive tax transcripts that they did not request;
- Clients who created an IRS online account receive an IRS notice that their account was accessed or IRS emails stating their account has been disabled; or, clients receive an IRS notice that an IRS online account was created in their names;
- 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;
- Network computers running slower than normal;
- Computer cursors moving or changing numbers without touching the keyboard;
- Network computers locking out tax practitioners.

Stay Vigilant

Stay ahead of the thieves by taking certain actions daily or weekly to ensure your clients and your business remain safe:

- Track your daily e-File acknowledgements. If there are more acknowledgements than returns you know you filed, dig deeper.

- Track your weekly EFIN usage. The number of returns filed with your Electronic Filing Identification Number (EFIN) is posted weekly. Go to your e-Services account, access your e-file application and check "EFIN Status." If the numbers are off, contact the e-Help desk. Keep your EFIN application up-to-date with all phone, address or personnel changes.
- If you are a 'Circular 230 practitioner' or an 'annual filing season program participant' and you file 50 or more returns a year, you can check your PTIN account for a weekly report of returns filed with your Preparer Tax Identification Number (PTIN.) Access your PTIN account and select "View Returns Filed Per PTIN." File Form 14157, Complaint: Tax Return Preparer, to report excessive using your PTIN or misuse of PTIN.
- If you have a Centralized Authorization File (CAF) Number, make sure you keep your authorizations up to date. Remove authorizations for taxpayers who are no longer your clients. See **Publication 947**, Practice Before the IRS and Power of Attorney.
- Create your IRS online accounts using the two-factor Secure Access authentication, which helps prevent account takeovers. See **IRS.gov/secureaccess** to review necessary steps.

Data Lost or Stolen? Report It Quickly

Contact the IRS and law enforcement:

- **Internal Revenue Service**, report client data theft to your local Stakeholder Liaison.
- **Federal Bureau of Investigation**, your local office (if directed.)
- **Secret Service**, your local office (if directed.)
- Local police – To file a police report on the data breach.

Contact states in which you prepare state returns:

- Email the Federation of Tax Administrators at **StateAlert@taxadmin.org** to get information on how to report victim information to the states.
- **State Attorneys General** for each state in which you prepare returns. Most states require that the attorney general be notified of data breaches.

Contact experts:

- Security expert – to determine the cause and scope of the breach, to stop the breach and to prevent further breaches from occurring.
- Insurance company – to report the breach and to check if your insurance policy covers data breach mitigation expenses.

For a complete checklist, see **Data Theft Information for Tax Professionals**.

Stay Connected

The IRS attempts to alert tax professionals as quickly as possible when it learns of a new scam, which are especially common during the filing season. Sign up so you can stay up to date with the latest alerts and tax administration issues:

- e-News for Tax Professionals – A weekly digest of important tax news geared for tax practitioners
- QuickAlerts – An urgent messaging system regarding e-File for tax professionals who have e-Services accounts.
- IRS social media – The IRS uses several social media outlets to connect with tax pros and with taxpayers. You can follow us at:
  - Twitter.com/IRStaxpros.
  - Twitter.com/IRSnews.
  - Facebook.com/IRStaxpros.

IRS Security Bookmarks:

- Identity Protection: Prevention, Detection and Victim Assistance – Main identity theft page
- Data Theft Information for Tax Professionals – How to report client data loss to the IRS
- Protect Your Clients; Protect Yourself – Awareness campaign and scam alerts for tax pros
- Taxes. Security. Together. – Awareness campaign for taxpayers
- Identity Theft Information for Tax Professionals – An overview
- Report Phishing and Online Scams – How to report IRS-related scams
- How IRS Identity Theft Victim Assistance Works – What clients can expect
- Maintain, Monitor and Protect Your EFIN – Protect your IRS-issued identification numbers
- Secure Access – How to authenticate your identity to access IRS online tools
- Security Summit – Track safeguards enacted by IRS, states and industry
- Newsroom – Stay in the know by subscribing to IRS News Releases
- Stakeholder Liaisons Local Contact – find your local contact to report data losses