PacificCPE

COURSE
60201A

Data Security Fundamentals for Tax Professionals

Client data is one of the most valuable—and vulnerable—assets in your practice. This course introduces the core principles of data security from the perspective of tax professionals and small business advisors. You'll explore why CPAs and tax preparers are prime targets for cybercriminals, what's at stake when a breach occurs, and how cybersecurity threats can affect both your clients and your firm. A solid starting point for anyone looking to strengthen their data protection practices.

CREDIT HOURS 2 | FIELD OF STUDY BUSINESS | EXAM QUESTIONS 10

Start Course ↓ | Final Exam Copy ↓

LEARNING ASSIGNMENTS AND OBJECTIVES

Assignment

- Study the full course materials included here.
- Complete the review questions after each chapter.
- Answer 10 final exam questions.
- Final exam is scored immediately, 70% or better passes.
- Certificate of completion is available in your account.
- Failed exams can be retaken free of charge.

Course Objectives

- Identify the topics focused on by the Security Summit.

Recall cybersecurity basics that can be employed to protect your business

-

Copyright Notice

© 2026 Pacific CPE, LP. All rights reserved.

The materials in this course — including the text, illustrations, exhibits, examples, exam questions, and review questions — are the copyrighted property of Pacific CPE, LP. No portion of this course may be reproduced, stored in a retrieval system, distributed, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise) without the prior written permission of Pacific CPE, LP, except for the personal, non-commercial use of the registered learner.

Pacific CPE, LP grants the registered learner a single-seat, non-transferable license to access this course for the purpose of completing the associated continuing professional education credit. Account credentials may not be shared. Group access requires a separate enterprise license.

This course is provided "as is" for educational purposes. While Pacific CPE, LP makes a reasonable effort to ensure the content is current and accurate, the materials should not be relied upon as a substitute for professional advice. Pacific CPE, LP disclaims all liability for any error, omission, or loss arising from the use of, or reliance on, the course content.

Questions about reproduction, licensing, or use of these materials should be directed to support@pacificcpe.com.

Publication Date: June 2026

TABLE OF CONTENTS

CHAPTER 01

Protect Your Clients; Protect Yourself 4

1.01 Identifying New Emerging Scams Targeting Tax Professionals. 7

1.02 Being Aware Of Phishing, Spear Phishing, Whaling, And The "Security Six". 8

1.03 Creating A Security Plan: Written Information Security Plan (Wisp) 10

1.04 Learning Tools To Help Protect Your Clients; Protect Yourself 12

1.05 Recognizing The Signs Of Identity Theft And Reporting Theft 15

Test Your Knowledge 17

CHAPTER 02

Cybersecurity: How It Impacts Tax Professionals And Small Businesses 21

2.01 Cybersecurity Basics 23

2.02 The Nist Cybersecurity Framework 25

2.03 Email Authentication 26

2.04 Secure Remote Access 28

2.05 Hiring A Web Host 29

2.06 Common Cyberattacks 30

Test Your Knowledge 38

Final Exam Copy 48

Glossary 42

Index .....

Chapter 1: PROTECT YOUR CLIENTS; PROTECT YOURSELF

Chapter Objective

After completing this chapter, you should be able to:

- Identify the topics focused on by the Security Summit.

Tax professionals operate in a high-trust, high-risk environment. They handle sensitive financial data, personal identifying information, and often act as intermediaries between clients and tax authorities. That combination makes them prime targets for fraud—and in some cases, unwitting participants in it. Protecting yourself and your practice isn't just about compliance; it's about preserving your reputation, your clients' trust, and your business.

Protecting client data is important, and **it is the law**. Federal Trade Commission regulations **require** professional tax preparers to create and enact security plans to protect client data.

One of the most important defenses is strong client verification. Fraudsters frequently pose as new clients with urgent requests, sometimes providing stolen or fabricated documents. It's essential to implement a consistent onboarding process: verify identities using government-issued ID, cross-check Social Security numbers where possible, and be cautious with clients who resist standard procedures or push for rushed filings. Urgency is a common tactic in fraud schemes.

Equally critical is safeguarding your digital environment. Tax professionals are frequent targets of phishing attacks, ransomware, and credential theft. Use multi-factor authentication on all accounts, especially tax preparation software, email, and cloud storage. Keep systems updated, encrypt sensitive files, and avoid using public Wi-Fi when accessing client data. Even a single compromised password can expose hundreds of records.

Another area of risk is client-provided information. While professionals rely on clients for accurate reporting, you are still responsible for identifying red flags. Be wary of suspiciously high deductions, inconsistent income records, or documents that appear altered. If something doesn't add up, ask questions and document your due diligence. Turning a blind eye can lead to penalties or legal consequences, even if the fraud originated with the client.

Internal controls also matter, particularly in larger firms. Limit access to sensitive data based on an individual's role and monitor employee activity for unusual behavior. Fraud doesn't always come from the outside—insider threats, whether intentional or accidental, can be just as damaging. Regular training on data security and ethical standards helps reduce these risks.

Communication practices should not be overlooked. Avoid sharing sensitive information via unsecured email channels. Use secure portals for document exchange and confirm any requests for changes to direct deposit or payment details through a secondary channel. Many fraud schemes rely on impersonation, such as fake emails that appear to come from clients or colleagues.

Finally, it is vitally important to stay informed. Fraud tactics evolve quickly, especially during tax season. Regulatory bodies and professional associations regularly issue alerts about emerging threats. Building time into your workflow to review these updates can make a significant difference.

You and every other tax professional in the United States – whether a member of a major accounting firm or an owner of a one-person storefront – are a potential target for highly sophisticated, well-funded, and technologically savvy criminals. However, you are not fighting this alone.

In March of 2015, the IRS convened an unprecedented coalition of state tax agencies and private-sector tax industry officials to begin a difficult task – fighting back against emerging criminal syndicates, based here and overseas, that were filing fraudulent returns for refunds. The resulting Security Summit consists of the IRS, state tax agencies, and the tax community, including tax preparation firms, software developers, payroll and tax financial product processors, tax professional organizations, and financial institutions.

Security Summit members are organized into six working groups, each tasked with addressing an area of need and each with a co-lead from the IRS, states, and industry.

- **Authentication Work Group:** Tasked with identifying ways to strengthen authentication practices, including new ways to validate taxpayers and return information.
- **Financial Services Work Group:** Tasked with examining ways to prevent criminals from potentially accessing tax-time financial products, deposit accounts, and prepaid debit cards.
- **Information Sharing Work Group:** Tasked with identifying **opportunities to improve the collective capabilities for detecting and** preventing Identity Theft tax refund fraud.
- **Strategic Threat Assessment and Response (STAR) Work Group:** Tasked with taking a holistic look at the entire tax ecosystem, identifying points of vulnerability (threats/risks), and developing a strategy to mitigate or prevent threats.
- **Communication and Tax Awareness Work Group:** Tasked with increasing awareness among individuals, businesses, and tax professionals on the need to protect sensitive tax and financial information.
- **Tax Professional Working Group:** Tasked with examining how new requirements will affect tax preparers who use professional software and how preparers can help prevent identity theft tax refund fraud.

Working in these teams, the Security Summit partners put into place a series of safeguards starting with the 2016 filing season. In the first two years, Summit safeguards resulted in a 57% decline in confirmed identity theft returns and a 65% decline in the number of taxpayers reporting themselves as victims.

However, because the work to counter evolving criminal tactics is ongoing, the Security Summit now generally convenes annually, introducing a "Protect Your Clients; Protect Yourself" campaign to remind tax professionals to stay alert against new and ongoing threats.

Now, in its tenth year, the Security Summit partners continue to work together to raise awareness about data theft in the tax professional community through their campaign.

> *"Reaching a ten-year milestone for the Security Summit is a testament to the collaboration of the IRS, state tax administrators, and all our industry partners in the tax ecosystem. Protecting taxpayers and the revenue system is of utmost importance, and state tax administrators will continue to be diligent in our quest to combat criminals, fraudsters, and all who attack the integrity of our systems and the people we serve."*
>
> – Sharonne Bonardi, Executive Director of The Federation of Tax Administrators (2025)

The key topics in the recent campaign highlight simple actions that tax professionals can take to better protect their clients and themselves from data theft. They include:

- **Identifying new emerging scams targeting tax professionals.** The Summit continues to see new scams targeting tax professionals in attempts to gain access to their systems. Learning to recognize these helps to protect taxpayers and professionals alike.
- **Being aware of phishing, spear phishing, whaling, and the "Security Six".** These may sound like fun summertime activities, but they are not; these are real cyber schemes that put sensitive information at risk. Tax professionals should be aware of different phishing terms and what the newest scams may look like, as well as the "Security Six" protections to combat these directed attacks.
- **Creating a security plan.** The Written Information Security Plan (WISP) was developed by and for tax and industry professionals to keep customer and business information safe and secure. Chapter 4, Chapter 2 of course 60202D of this course will detail how to create a WISP.
- **Learning tools to help Protect Your Clients; Protect Yourself.** This addresses Multi-factor Authentication, IP PINs, IRS Online Accounts, Tax Pro Accounts, and other resources to safeguard taxpayers' information.

- **Recognizing the signs of identity theft and reporting theft.** Many tax professionals who report data theft to the IRS also say they were unaware of the signs that a theft had already occurred. This outlines the many signs that tax pros should watch.

Let's examine each topic more closely.

IDENTIFYING NEW EMERGING SCAMS TARGETING TAX PROFESSIONALS.

Identity thieves are taking numerous approaches to steal sensitive information from tax professionals. This includes posing as new clients; using phishing emails to trick people into sharing Central Authorization File information, as well as elaborate schemes involving calling and texting. Tax professionals need to be on the look out to avoid falling prey to these attacks, which threaten not just their clients but their own businesses.

> *"Tax professionals face an increasingly complex threat landscape, with identity thieves using ever more sophisticated tactics to exploit both practitioners and the sensitive data they manage. The stakes are high – not just for individual firms, but for the taxpayers who rely on them. Staying vigilant, informed, and prepared is essential to defending taxpayer data and maintaining trust in the services these professionals provide."*
>
> - Taylor Rodier, Legislative Affairs Manager with Taxwell

Beware of the "new client" scheme.

In this form of spear phishing, fraudsters pretend to be real taxpayers seeking a tax professional's help with their taxes. In these fake "new client" schemes, the fraudster can send a malicious attachment or include a link to a site that the tax professional thinks they need to access to obtain the supposed new client's tax information. In reality, the site is collecting information from the tax professional, such as their email and password, or loading malware onto the tax professional's computer to gain access to their system. While not a fresh scam, the IRS continues to see activity, and it remains an ongoing threat that can be alluring to a tax professional or practice's employees seeking new business. Although this fake outreach may peak around tax season, this sort of scam remains a threat year-round.

Scams involving EFINs, PTINs, CAF numbers.

Another scam circulating on a large scale this year involves phishing attempts by scammers trying to obtain various identification numbers used by tax professionals, including their Electronic Filing Identification Number or EFIN; EFIN documents; their Preparer Tax Identification Number or PTIN; and their Centralized Authorized File or CAF number.

Obtaining these numbers helps a bad actor obtain information and file a fraudulent return that looks legitimate. Scammers are trying to get these sensitive identification numbers by sending emails or texts that appear to be from the IRS. The scammers tell tax professionals they need to

confirm this information by entering it into a form that was hosted on what appears to be a real IRS website, but in reality, it is a fake website designed to mimic the real thing.

For example, a fraudster with a compromised CAF number in hand can use it to obtain tax transcripts and other sensitive taxpayer personally identifiable information (PII) to commit identity theft refund fraud and other crimes. In many cases, the fraudster has not only obtained a practitioner's CAF number but also has the tax professional's sensitive personal information.

Watch and listen for phone, text, and correspondence schemes.

Tax professionals should be aware of another wave of scams hitting taxpayers, with identity thieves using phone calls and text messages to get social security numbers, birth dates, and banking information from victims. Several of these schemes are common and can target not just taxpayers, but tax professionals. These include:

- The so-called Zero Tax program, in which callers promise to wipe out tax debt for people who owe back taxes. The callers request people's social security numbers as part of their pitch, which they use for nefarious purposes. Tax professionals should watch out for clients reporting this scheme.
- Social media scams circulating inaccurate or misleading tax information that can involve creating common tax documents that are false, like a Form W-2, or claiming credits to which the taxpayer is not entitled to like the Fuel Tax Credit, Sick and Family Leave Credit, and household employment credits.
- Scammers reaching out by phone or text message to dupe people into handing over sensitive financial information in exchange for a false promise of IRS money for them.
- Artificial intelligence or AI scams used for false correspondence, with AI being used to create fake IRS letters that are mailed to victims.

BEING AWARE OF PHISHING, SPEAR PHISHING, WHALING, AND THE "SECURITY SIX".

The Security Summit partners continue to see a steady stream of e-mail and related attacks aimed at the nation's tax professional community. These are designed to steal sensitive tax and financial information from clients. The Summit partners warn tax professionals to be aware of evolving phishing scams and cloud-based schemes designed to steal such.

Phishing, spear phishing, clone phishing, and whaling

These are designed to trick the recipient into disclosing personal information such as passwords, bank account numbers, credit card numbers, or Social Security numbers. Tax professionals should be aware of different phishing terms and what the scams might look like.

- Phishing / Smishing: Phishing emails or SMS/texts (known as "smishing") attempt to trick the recipient into clicking a suspicious link, filling out information, or downloading a

malware file. Often, phishing attempts are sent to multiple email addresses at a business or agency, increasing the chance someone will fall for the scam.

- Spear phishing: This is a specific type of phishing scam that bypasses emailing large groups at an organization, but instead identifies potential victims and delivers a more realistic email known as a "lure." These types of scams can be trickier to identify since they don't occur in large numbers. They single out individuals, can be specialized, and make the email seem more legitimate.
- Clone phishing: A newer type of phishing scam that clones a real email message and resends it to the original recipient, pretending to be the original sender. The new message will have either an attachment that contains malware or a link that tries to steal information from the tax professional or recipient.
- Whaling: Whaling attacks are very similar to spear phishing, except these attacks are generally targeted at leaders or other executives with access to secure, large amounts of information at an organization or business. Whaling attacks can also target people in payroll offices, human resource personnel, and financial offices.
- New client scam: Tax pros have been particularly vulnerable to emails where the sender is posing as a potential client. Criminals use the "new client" scam to trick practitioners into opening email links or attachments that infect computer systems to steal existing client information.

Warning signs of scams

Regardless of the type of phishing attempt, tax professionals can protect themselves and their organization by being aware of these scams and looking for warning signs like:

- An unexpected email or text claiming to come from a known or trusted source, such as a colleague, bank, credit card company, cloud storage provider, tax software provider, or even the IRS and other government agencies.
- Receiving a duplicate email from what appears to be a known, trusted source that contains a new attachment or hyperlink.
- A message, often with an urgent tone, urging the receiver to open a link or attachment. These messages have a false narrative, like someone's password has expired or some other urgent action is needed.
- An email address, number, or link that is slightly misspelled or has a different domain name or URL (for example, irs**.com** versus irs.**gov**). A closer look at these email addresses – like hovering the cursor over the email address – can show slight variations on legitimate addresses.

Security Six adds up to more protection

As data thieves continue evolving tactics, these six essential steps are important in protecting sensitive taxpayer information. The "Security Six" protections offer a relatively simple but important starting point for tax professionals to protect their offices, computers, and data, as well as their clients.

These best practices include using anti-virus software, firewalls, multi-factor authentication, backup software or services, encrypted drives, and virtual private networks or VPNs. These six important security basics that form a critical defense against identity thieves and hackers include:

1. **Anti-virus software**: Scans computer files or memory for certain patterns that may indicate there's malicious software – also called malware – on the device. Anti-virus vendors find new issues and update malware daily. This is why it's important for users to install the latest updates of the software.
2. **Firewalls**: Provide protection against outside attackers. The firewall shields computers and networks from malicious or unnecessary web traffic. This helps prevent malicious software from accessing the user's system.
3. **Multi-factor authentication**: Adds an extra layer of protection beyond a password. Under new rules from the Federal Trade Commission, all tax professionals are required to use multi-factor authentication.
4. **Backup software or services**: Should be routinely used by tax professionals to back up critical files on their computers and hard drives to external sources. This is helpful not just to protect against a cyber-attack, but is also helpful in case of device failure or a natural disaster.
5. **Drive encryption**: Because tax professionals keep sensitive client data on their computers, users should consider drive encryption software. Drive encryption is also known as disk encryption. It transforms data on the computer into protected files that are unreadable to outsiders. This means only people who are authorized to access the data can do so.
6. **Virtual Private Network**: Because many tax firms' employees must occasionally connect to unknown networks or work from home, the office should establish an encrypted virtual private network (VPN). This allows for a more secure connection. A VPN provides a secure, encrypted tunnel to transmit data between a remote user over the internet and the company network.

CREATING A SECURITY PLAN: WRITTEN INFORMATION SECURITY PLAN (WISP)

There are many aspects to running a successful business in the tax preparation industry, including reviewing tax law changes, learning software updates, as well as managing and training staff. One often overlooked but critical component is creating a WISP.