Russell, R., & Russell, R. (2025). Small Business Tax Data Protection in the Artificial Intelligence Era — A WISP Away. *Small Business Institute Journal*, *21*(2), 24–32.
https://doi.org/10.53703/001c.147324

Articles

Small Business Tax Data Protection in the Artificial Intelligence Era — A WISP Away

Richard Russell Jr., JD, MPA, CPA[1], Richard Russell Sr., JD, MBA, CPA[2]

[1] Accounting, Metropolitan State University of Denver, [2] Accounting, Jackson State University

Keywords: Artificial Intelligence, Taxation, Accounting, Identity Theft, Data Protection

https://doi.org/10.53703/001c.147324

Small Business Institute Journal

Vol. 21, Issue 2, 2025

Generative AI, large language models (LLMs), advanced image recognition, AI agents, Chatbot GPT, DeepSeek and . . .TaxBot GPT? These are Artificial Intelligence (AI) technologies that are available to the public, including tax firms that prepare tax returns with sensitive business and client data. Businesses, especially small businesses, should choose their tax practitioners carefully as AI-based tax services become more common-placed. AI has the potential to greatly improve the availability, costs, and quality of tax services for small businesses (Federico & Thompson, 2023; Hussin, Bukhari, Hashim, Bahari, & Mohd, 2024). However, are there are potential privacy and data risks associated with tax firms or their staff using AI technologies? This paper highlights important points that small business might consider when selecting a tax firm that uses AI technologies.

Introduction

Generative AI, large language models (LLMs), advanced image recognition, AI agents, Chatbot GPT, DeepSeek and . . .TaxBot GPT? These are among the limitless Artificial Intelligence (AI) options that are available to the public, including small businesses and their tax advisors that prepare tax returns with sensitive business and client data. Businesses, especially small businesses, should take active steps to protect their tax data as AI-based services become more common-placed — often included with email, search engines, word processing software, pdf software, messaging apps, and even industry specific software such as professional grade software for tax advisers. AI has the potential to greatly improve the availability, costs, and quality of tax services for small businesses (Federico & Thompson, 2023; Mat Hussin et al., 2024). AI can also help non-tech savvy individuals write code and computer programs, overcome language barriers, or manage data. Artificial intelligence programs can even act as AI agents — directly performing tasks on behalf of a user with the user's permission. Thus, AI has gone from simply grammar checking emails to actively managing users' email inboxes, with the ability to autonomously log into a user's account and respond to all of the users' emails without any direction.

Small businesses and their tax advisers should be prepared for the data and privacy risks associated with the rapidly increasing capabilities of AI technologies. The security of tax data is an important consideration as tax returns and related documents are a figurative goldmine of personal information for identity thieves and other nefarious groups that may also utilize AI. Furthermore, the services provided by your tax advisor often include much more than simply preparing tax returns and thus can involve sensitive data that small businesses may not have contemplated beforehand. Sensitive tax data potentially includes the information of the business, and payees such as employees and contractors (Treasury Inspector General, 2017). Further, this information can include sensitive business plans or even closely held business secrets such as patented formulas, software, or other inventions. Businesses with leaked data can face disclosure requirements, reputational damage, loss of business secrets/patents, or legal liability from breaches of data (26 United States Code [U.S.C.] § 41, n.d.; Nield et al., 2020; Vaaler & Greenwood, 2023). Data breaches may even affect cyber insurance premiums and loan terms from banks (Chen et al., 2023; Huang & Wang, 2021; Talesh, 2018).

Purchasing anti-virus software and hoping for the best is no longer enough to protect sensitive data, especially tax data which is notorious for being targeted by bad actors. Avoiding deepfakes and new security risks presented by AI will require small businesses to understand the services that are provided by their tax advisors. Failure to understand a tax advisors role or services outside of preparing returns makes businesses more susceptible to AI related security threats. Equally important will be establishing proper communication channels and becoming familiar with your tax advisor's key personnel. This is because AI's ability to create realistic videos, photos, reproduce voices, and even make phone or voice calls will rapidly improve over the next decade (Kahn, 2025). Thus, small businesses, their tax advisers, and their employees are not the only ones utilizing AI. These advanced capabilities can also be used by bad actors for their own nefarious purposes. It is imperative that small businesses take active steps to protect their tax data

by ensuring that communications, document requests, and the individuals initiating these communications are genuine. It is also important that small businesses predetermine their tax advisor's contacts, communication methods, and data transmission methods.

This paper recommends specific steps that small businesses can take to protect their tax data. First, the paper provides a background of tax advisors, the sensitive data necessary for their services, and why it is important to understand which specific services you have requested. This paper also provides a background of traditional threats to tax data and broader security threats associated with AI's advanced capabilities. The paper then analyzes how AI's advanced capabilities exacerbate current threats to sensitive tax data as well as communications between client and tax advisor. The paper also recommends seven active steps that small businesses can take to protect their tax data. This includes discussing the tax advisor's data security playbook, also known as a Written Information Security Plan (WISP), to identify specific key contacts, establish communication channels, and to assess whether the tax advisor has training for employees regarding AI. Lastly, the conclusion section provides a brief perspective on the importance of proactively protecting tax data from being harvested now and stored for future decryption with advanced technologies.

Background

Why Is Understanding My Tax Advisor's Role Important?

Understanding the role and nature of your tax advisor is critical to protect your tax data from AI related fraud or theft. Tax advisors often garner a high degree of trust from clients and small businesses. Data thieves often misuse this trust to gain access to private or proprietary information. A common scenario involves data thieves posing as a tax advisor in order to fish for information or lull an unsuspecting employee into opening a virus ladened file. Therefore, it is imperative that small businesses familiarize themselves with their tax advisor, the information tax advisors are likely to request, and how that information is going to be requested. These points seem simple; however, AI is expected to make the task of distinguishing between genuine and faux communications increasingly difficult (Kahn, 2025).

Thus, documenting the answers to these simple questions will become increasingly important. Who does a business expect to hear from regarding tax matters? How often does the business normally hear from this individual? What time of year or day do we normally expect to hear from this person? What type of communication do I expect to receive (phone, email, text message)? What information is being requested and in what context? Is this information request genuine? The answers to these questions will change depending on the specific practitioner and the specific tax advisory service used by the small business.

Traditional tax services can be grouped into three broad advisory areas: tax compliance, tax controversy, and tax consulting (AICPA, 2024). They can involve various types of sensitive information ranging from biographical, financial, and proprietary information depending on the nature and scope of the specific services. These services may also have seasonal deadlines that provide predictability about when communications should be expected. Businesses might also verify the identity of the sender of a communication with information on their tax firm's website or through a trusted contact for those specific services.

Tax compliance services involve filing tax returns or informational returns which report "closed transactions" and other financial data of the taxpayer (AICPA 2024; Sawyers & Gill, 2021). "Closed transactions" are based on events that have already occurred (Sawyers & Gill, 2021). Items needed to report closed transactions can include tax data such as prior tax returns, social security numbers, digital signatures, and addresses (Treasury Inspector General, 2017). Closed transactions are notable because documents and other information would tend to involve digital and paper records of a company's past transactions and financial position. Tax compliance services are often on a predictable schedule of payments as well as quarterly and annual filings based on the business' fiscal year.

Tax controversy services involve representing a taxpayer during audits, hearings, or challenges to IRS assessments, and can include data for any tax return at issue (AICPA, 2024). Tax controversy services also involve closed transactions and associated tax return information. These services are notable because tax audits and litigation include multiple tax years and potentially much more tax data. Further, these engagements often include trusted contacts that routinely request confidential information from their clients during a controversy. Tax controversy services are in many ways richer with detailed information than tax compliance services. In many cases, these services involve a tax return, related documents, workpapers, as well as possible detailed testimony and affidavits.

Consulting services, on the other hand, include "open transactions" (Sawyers & Gill, 2021). Open transactions are proposed future transactions (AICPA 2024; Sawyers & Gill, 2021). Open transactions generally have the maximum possible impact of reducing a client's future tax exposure (Sawyers & Gill, 2021). This is because proposed transactions can be tailored to meet the rules of a tax benefit before the close of the tax year (Sawyers & Gill, 2021). Tax consulting communications can be rich with sensitive information too. These transactions are notable because they involve possible tax outcomes of a company's confidential strategies, services, suppliers or products. For example, communications regarding a startup's research credit might be particularly sensitive due to proprietary concerns regarding a secret patent, formula, or process.

What Are Traditional Data Threats to My Tax Information?

Many traditional threats to tax data are based on forgetfulness, a mistake of fact, a misunderstanding, and/or misplaced trust. These threats include: 1) unintentional disclosure, 2) phishing scams, 3) unauthorized access, 4)

tax refund theft, and 5) theft of proprietary information (IRS Dirty Dozen Scams, 2025). Note that data theft events might combine one or more aspects of these threats. Small businesses might also experience tax data threats differently depending on the nature of the business, the size of the business, the tax services used, and the data practices of the tax firm.

Unintentional disclosure is often an overlooked threat to tax data. Unintentional disclosures occur in tax compliance, controversy, or consulting engagements. This might involve an owner or custodian of sensitive data unwittingly sending, sharing, or publicizing private data. This includes lapses in physical asset policies such as leaving facilities unlocked or leaving sensitive documents at a large airport or courthouse. Additionally, this might involve storing sensitive data on a computer that does not have a lock screen, password, or two-factor authentication (generally requiring a password and a phone/email contact to confirm that an authentic user is the person logging into a system).

"Phishing" scams are a traditional threat that have become more sophisticated over time. These scams generally involve an email or other communication intended to elicit information from the victim through false pretenses. The goal of a phishing scam is to gain the users trust just long enough for the user to disclose information or provide access to a sensitive database without examining the communication further. For example, a taxpayer might receive an email, purportedly from the IRS, stating that the taxpayer owes penalties/back taxes in a scam to obtain credit card information, social security numbers, or other data. Another example would be a tax firm receiving an email from a "new client" with virus laden files attached. More recent examples include text messages claiming that a taxpayer's IRS account has been put on hold. An individual might even receive text messages or emails claiming to be from colleagues or a tax professional (IRS Dirty Dozen Scams, 2025).

Unauthorized access is also a traditional threat to tax data. This involves bad actors gaining physical or digital access to sensitive information without proper authorization and with ill intentions. Examples can include keystroke logging malware to steal passwords or break encryptions. Bad actors might also gain physical access to documents through burglary. Further, bad actors may send emails that lull a user into clicking on a link or file that is used to spread malware and/or steal information. Note that new client scams also lead to unauthorized access as well, through the spread of malware and malicious code that provide access to bad actors (IRS Dirty Dozen Scams, 2025).

A particularly aggressive form of data theft is Tax Refund Theft. This involves e-filing an unauthorized tax return of an individual or business. In addition, the unauthorized individual generally claims fraudulent tax benefits to increase the size of the refund. The identity thief then has the refund routed to their own bank account (Collins, 2024a, 2024b; LexisNexis, 2015).

Victims are often unaware of tax refund theft until the financial damage is done. A first indication is usually a notice from the IRS regarding irregularities associated with the victim's tax return (Collins, 2024b). The taxpayer might notice that thieves have claimed tax benefits that the victim was not qualified to claim. Fraudulently claimed benefits can include child tax credits, earned income credits, and other tax benefits (Collins, 2024b). The taxpayer must immediately sign an affidavit to begin identity theft procedures to avoid penalties (Collins, 2024b). Otherwise, the taxpayer may experience harsh legal consequences if they are unable to complete this process (Collins, 2024b). This lengthy process can sometimes take up to two years (Collins, 2024b).

Theft or disclosure of proprietary information is another risk for taxpayers. As previously noted, tax benefits can involve sensitive information surrounding products, processes and formulas (26 United States Code [U.S.C.] § 41, n.d.). Further, tax planning communications can disclose sensitive information surrounding mergers, acquisitions, and other future actions that business stakeholders would like to remain private. The development of AI poses a significant challenge for data privacy (Kahn, 2025). Thus, selecting a tax firm that safeguards tax data is more important than ever.

How Does Artificial Intelligence Impact Data Security Overall?

Purchasing anti-virus software is no longer enough to protect sensitive data; users will need to take a proactive role in data security. Advanced features of AI complicate data protection and present inherent risks for small businesses. Accounting and tax professionals have echoed these concerns. A large number of professional firms in accounting, law, and tax expect AI to significantly impact data security, privacy, and confidentiality according to a Thomson Reuters' whitepaper (Thomson Reuters Institute, 2024). The whitepaper surveyed accounting, legal and tax professionals and found that 68% of respondents expected AI to negatively affect data security (Thomson Reuters Institute, 2024). The same whitepaper found that 62% of respondents were concerned with AI's impact on privacy and security (Thomson Reuters Institute, 2024). Other researchers have uncovered similar sentiments as well (Lehner et al., 2022).

These professional concerns about AI are well founded. AI complicates data security, privacy, and confidentiality by "lowering the barriers to entry" for data thieves including: the public availability of AI searches, creation of realistic media, coding ability, and language translation features (Kahn, 2025). Moreover, AI's core competencies can be enhanced by using AI agents. As previously noted, AI agents can act independently while controlling the user's computer, software applications, email inbox, or data bases with the user's permission. Access can be granted for digital services such as: Google Drive, Drop Box, SharePoint, Outlook, Microsoft Teams, GitHub, Google Calendar, Outlook Calendar, and other web based services (Babo, Nakibly, & Uziel, 2025). These features are all impressive. However, a tax advisor, small business owner, employee, or AI Agent can be duped into granting access by a human or digital imposter posing as a boss, colleague, client, or authorized user. This is arguably the greatest security challenge posed by AI.

The public availability of AI searches presents challenges for companies that do not have proper AI training for employees. Research indicates that many employees using AI at work without proper training do not understand that the information entered into AI software could be publicly available (Claburn, 2025). Meaning that information entered could be searchable via search engines such as Google (Claburn, 2025). Many employees can readily use unvetted AI software at work without permission, training, or forethought from their employers. For instance, A recent report by LayerX, a data security firm, indicates that 45% of enterprise employees use some form of generative AI (Eshed, 2025). Yet, 77% of those users report copying and pasting information into AI prompts (Eshed, 2025). It is even more alarming that 22% of these instances involve personally identifiable information (PII) or involve payment card industry numbers (Eshed, 2025). Further, half of file uploads into AI search prompts include sensitive data (Eshed, 2025). Thus, a major threat of AI is not theft, but rather employees carelessly depositing sensitive information into the public sphere.

Deepfakes are another security challenge presented by AI. The production of realistic communications is often referred to as a "deepfake" — creating or reproducing documents, pictures, websites, video footage, and even voices (Kahn, 2025). The danger of deepfakes is not only that they appear genuine, but also that deepfakes can be created with increasing volume, speed, and quality that can be customized for a specific the target. For example, an employee receives a phone or video call from an entity that they believe is their boss or colleague. Thus, AI is expected to create a "trust bomb" — a challenge to the business community's perception of security and privacy that interferes with ordinary operations (Kahn, 2025).

Coding is another AI ability that poses a threat to data security. "Vibe coding" is the use of artificial intelligence software to code by using written natural language prompts (Google Cloud, 2025; Karpathy, 2025; Willison, 2025). Vibe coding lowers barriers to entry for bad actors — decreasing the skill, number of people, and financial costs necessary to create and spread malware (Google Cloud, 2025; Willison, 2025). Thus, bad actors no longer need years of coding experience, a computer science degree, coding ability, or familiarity with programming languages such as python or C++.

AI's language translation abilities are not limited to computer programing languages but also includes the ability to translate natural languages. This lowers the barriers to entry for potential data thieves who do not speak the language of their target. In the past, an email littered with typos and grammatical errors was a strong indicator that the email was not authored by your colleague or boss. However, this luxury no longer exists in the AI era. Users need much greater due diligence to determine whether a communication is genuine (Kahn, 2025).

AI agents are arguably the greatest threat to data security. Users may request AI agents to perform unfamiliar, complex, and time-consuming tasks (Kahn, 2025). The user could follow the AI's instructions and complete the task themselves; however, in some cases this is not practical or necessary. An AI agent can directly accomplish the task with permission. However, it is critical to ask whose permission does an AI agent need to take over a computer, application, cloud computing accounts or databases?

Prompt injection is a vulnerability of AI agents. Prompt injection is the hi-jacking of another user's AI agent (Babo et al., 2025). This is accomplished by using a prompt that is hidden or undetectable to human eyes, such as "white-on-white" text or a small text size. Generally, AI agents will address commands directed towards the agent. Agents may have difficulty distinguishing the appropriate users' commands from nefarious individual's commands. Data thieves could conceivably use their own AI agents to overcome security measures; however, research indicates that covertly hi-jacking a user's agent may pose a far greater data security threat (Babo et al., 2025).

Researchers at Radware, a data security firm, recently performed an experimental data attack called ShadowLeak. The experiment involved hi-jacking ChatGPT's Deep Research AI agent to exfiltrate data directly from OpenAI's cloud server environment (Babo et al., 2025). The experiment involved providing an AI agent genuine user access to a Gmail account with the instructions to read, sort and generate a report of emails in the account (Babo et al., 2025). Researchers were able to hi-jack the AI agent by injecting hidden prompts into an email sent to the experimental Gmail account (Babo et al., 2025). The prompts were hidden by formatting the text with a white color and by using extremely small fonts, as mentioned above. The researchers successfully hi-jacked the agent into exfiltrating information from OpenAI's cloud servers with the hidden prompts (Babo et al., 2025). While OpenAI has claimed to fix this vulnerability, the experiment highlights the vulnerabilities of AI platforms (Babo et al., 2025). This experiment has also been reproduced successfully with other AI platforms as well (Pathade, 2025).

Analysis

What Challenges Will AI Present for Tax Data Security of Small Businesses?

AI will likely increase the effectiveness and likelihood of unintended disclosure, unauthorized access attempts, phishing scams, and tax return refund theft. Burglary and sophisticated malware are no longer necessary to pose a substantial threat to tax data. Theives are likely to find indirect ways to exploit vulnerabilities such as deepfakes or prompt injection. Moreover, research indicates that many employees have been unwittingly posting sensitive information online via AI searches.

Unintended disclosure by small business employees and tax advisors will be more problematic due to the public availability of AI searches. As noted previously, employees are likely to upload sensitive information into AI searches, especially if they have not received AI training. (Eshed, 2025). This presents a major security challenge for small businesses and their advisors because tax documents are particularly sensitive. Pasting a tax document into an AI

search prompt is also tempting for a tax professionals because it can yield quick results when trying to meet a tight tax deadline. Furthermore, small businesses and their tax advisors may not have the funds to build their own AI systems. Thus, small businesses and their tax advisors may be particularly susceptible to unintended public disclosure of sensitive documents or information.

Tax-based phishing scams and tax refund scams will be more frequent, capable, and realistic. Targeted small businesses may receive emails purportedly from their tax advisors with injected prompts along with the traditional suspicious links and malware. In some cases, scam emails might even use the specific name, logos, and insignia of the tax advisor.

Taxpayers may also experience an increase in the complexity of tax refund theft schemes as a result of AI deepfakes. Generally, tax refund thefts are carried out by individuals posing as genuine tax professionals (Collins, 2024a, 2024a). Deepfakes will make it increasingly difficult for small businesses to distinguish their tax advisor from scammers. Trust indicators used for verification may be compromised or easily reproduced by AI. Trust indicators would include websites and documents designed to temporarily suspend critical thinking of the victim due to trust (Kahn, 2025). However, AI can create additional layers of complexity such as realistic voice or video calls as well (Kahn, 2025).

These enhanced tax scams will present new and unique security challenges for small businesses and their tax advisors. Specifically, these developments will increase the difficulty in discerning between genuine and fake communications. As previously noted, it is no longer enough for small businesses to take a passive approach to data security. Small businesses and their tax advisors will need to be proactive in protecting their data and communications. These actions are not complicated but are powerful steps towards protecting data involving communication, verification, and review.

Recommendations

What Steps Can Small Businesses Take to Protect Their Tax Data?

Steps that small businesses can take to protect their tax data in the AI era include: 1) discussing data privacy with their tax advisor; 2) verifying data security contacts; 3) determining specific tax team contacts; 4) verifying the appropriate transfer and storage methods for tax data; 5) verifying that their tax advisor's employees receive AI training; 6) verifying access provided to AI agents; and 7) reviewing the above steps annually.

What Should Small Businesses Discuss with Tax Advisors?

Data security conversations allow small businesses to determine the level of preparedness of their tax advisors, especially in regards to AI. This discussion might involve the following questions: what is your tax advisor's plan in the event of a data breach? Who will contact the small business in case of a data breach? Does the tax advisor use AI or AI agents in conjunction with sensitive information? Does the firm have policies to prevent individual employees from using nonapproved AI programs with sensitive client data? Does the tax advisor have training on the appropriate use of AI for their employees? Note that tax advisors are generally required to contemplate basic data security issues, but to date, not AI (IRS, Publication 5708, 2024; 16 C.F.R. § 314.3(a)). Specifically, firms are required by law to have a Written Information Security (WISP) plan that outlines the firm's policies regarding basic data security (IRS, Publication 5708, 2024; 16 C.F.R. § 314.3(a)).

The Gramm-Leach-Bliley Act requires financial institutions to protect confidential client data (Gramm-Leach-Bliley Act, § 501 - 510). The Federal Trade Commission's (FTC) regulations on the subject consider tax firms to be financial firms (16 C.F.R. § 314.2(e)(2)(H)). Further, the IRS has created the Data Security Summit, a panel of FTC, tax, and data security professionals to help tax firms with these issues (IRS, Publication 5708, 2024a). The IRS Security Summit provides guidance for tax firms to create WISPs (IRS, Publication 5708, 2024; 16 C.F.R. § 314.3(a)). The data security summit and WISP requirements have led to a 57% reduction of identity theft related tax returns after the first two years of the Security Summit, (IRS, About the Security Summit, 2024c). The IRS has stated that this was also accompanied by a 65% reduction in taxpayers reporting tax identity theft related incidents (IRS, About the Security Summit, 2024c).

A WISP is a data security playbook that details a tax firm's data protection policies. This plan will generally detail key personnel, data protection methods, and possible responses to data breaches (IRS, Publication 5708, 2024a). The typical WISP details a tax firm's key data security personnel, trainings for employees, and policies (IRS, Publication 5708, 2024a). A tax advisor is generally free to share their WISP with clients upon request. However, the current WISP requirements do not directly address AI (IRS, Publication 5708, 2024b). Therefore, small businesses should verify AI-related questions with their tax advisor.

What Data Security Contacts Should I Verify?

The WISP will identify a tax advisor's Data Security Coordinator (DSC) and Public Information Officer (PIO). (IRS, Publication 5708, 2024). The DSC and PIO should be intimately familiar with a tax advisors data security policies and procedures (16 C.F.R. § 314.4; IRS, Publication 5708, 2024). The DSC's role will involve internal data security, while the PIO's role generally involves external communications. These roles might be combined into one position or assigned to a third party at a small or solo tax firm (IRS, Publication 5708, 2024b; Love, 2021). Also, the size of the firm will presumably affect the resources available to the individual that oversees data security at the tax firm.

The DSC's responsibility is to oversee the firm's data security. This includes vetting and selecting third party service providers, which presumably includes possible AI based services for the firm. Further, the DSC should know whether their are policies limiting employees use of exter-

nal AI systems — especially regarding the uploads of sensitive client data. This individual is also responsible for ensuring all recurring security trainings are completed by firm owners, managers, employees, and independent contractors. Further, the DSC must annually review the security measures, policies, and protocols of the firm and report findings to firm leadership (IRS, Publication 5708, 2024b).

The PIO is another important contact because they are responsible for communications with various stakeholders in the event of major data breaches. This includes releases to the news media, communications to law enforcement, and client communications. This individual would also communicate with the tax firm's associations, neighboring businesses, and trade associations. A PIO will likely be the first to report a data breach to a small business client (IRS, Publication 5708, 2024b)..

Why Should Small Business Verify Tax Team Contacts with Their Advisor?

Small business should verify tax team contacts to protect against deepfakes. Confirming the identity of your tax team contacts is particularly important. Not every member of your tax advisors firm will contact you to request information. A small business receiving a realistic information request purportedly from an inappropriate or non-existent tax team member is more likely to be noticed. Furthermore, a small business can confirm with tax team members about what types of information are likely to be requested.

A small business should also confirm the method of contact for information requests to ensure the request is coming from a familiar phone number, email, or video call account. Small businesses can also designate employees within their own enterprises to receive tax information. A designated tax-matters partner or employee is more likely to be familiar with their advisors tax team and methods used for information requests (26 CFR § 301.6231(a)(7)-1).

Why Verify Information Transfer and Storage Methods for Tax Data?

Verifying transfer and storage methods can prevent small businesses from attempting to send information via unsecured methods. Tax professionals generally discouraged clients from sending unsecured tax data via email, even before AI became commonplace. Tax advisors typically ask clients to password protect sensitive files before sending them via email (IRS, 2024b; IRS, Office of Chief Counsel, 2020). In some cases advisors may also use special software or communication encryption methods as well (IRS, 2024b; IRS, Office of Chief Counsel, 2020). Documenting how information is stored and transferred will arguably help businesses to avoid prompt injection attacks. Furthermore, a deepfake information request that discusses an unfamiliar method of transfer or storage is more likely to be noticed by small businesses.

Why Is Verifying AI-Specific Training for Tax Advisors Important?

Advisors with AI specific training requirements might be less likely to upload tax documents into AI systems inappropriately (Eshed, 2025). Further, the current WISP rules are silent on AI specific trainings or policies for employees of tax firms (IRS, Publication 5708, 2024b, IRS, About the Security Summit, 2024c). Therefore, it is up to small businesses to confirm whether their tax advisor's owners, employees, and third party contracts have training and policies surrounding the appropriate use of AI.

Why Scrutinize Your Tax Advisors Usage of AI Agents?

AI agents present another layer of informational security risk for small businesses and their tax firms (Kahn, 2025). A tax advisor that utilizes AI agents may need to scrub emails for hidden prompts in order to protect against prompt injection attempts. Tax data is fully compromised once a prompt injection attempt is successful (Babo et al., 2025). Inboxes and other databases can contain numerous undetected prompts (Babo et al., 2025). One successful prompt injection attempt is enough to compromise an entire database of sensitive information (Babo et al., 2025).

Why Review These Steps Annually?

AI is improving quickly and being implemented by enterprises rapidly. Moreover, Artificial general intelligence (AGI) is not yet available as of this writing, but is expected to be achieved quickly (Kahn, 2025). AGI will be exponentially more effective than currently available AI software (Kahn, 2025). Thus, AI safeguards, trainings, and policies that are currently appropriate could be completely ineffective in the next year (or even the next month). Therefore, small businesses and their advisors must remain vigilant to ensure their data stays secure, private, and safe.

Conclusion

Protecting tax data in the AI era starts and ends with communication. AI is expected to bring many new capabilities for tax firms to serve more clients and to provide quality tax services quickly. However, many of these advanced AI capabilities will also be available to identity thieves and other nefarious groups, willing to mine valuable tax data. This puts employees, contractors and potentially, customers, at risk.

Fortunately, small businesses can protect their tax data by finding the right people and asking the right questions. Specifically, starting a conversation with a tax advisor about their WISP is an excellent way to assess a tax advisors data security playbook and to start a conversion on data security and AI. Further, businesses should take actives steps to protect their data now as anti-virus software and encryption technology will not be enough. Small businesses should take these proactive data steps now. New developments such as AGI and advanced decryption techniques are

just on the horizon (NIST, 2025). As a cautionary note, data theives are likely to store stolen information now, and decrypt it later (NIST, 2025).

Submitted: March 24, 2025 MST. Accepted: November 13, 2025 MST. Published: November 24, 2025 MST.

References

16 C.F.R. § 314.2(e)(2)(H).

16 C.F.R. § 314.3(a).

26 United States Code [U.S.C.] § 41.

American Institute of Certified Public Accountants (AICPA). (2024). *Statement on Standards for Tax Services (SSTS) No. 4: Standards for Members Providing Tax Representation Services 4.11*. https://www.aicpa-cima.com/resources/download/revised-statements-on-standards-for-tax-services-no-1-4-1-1-2024

Babo, Z., Nakibly, G., & Uziel, M. (2025, September 18). *Radware uncovers first zero-click, server-side vulnerability in ChatGPT*. Radware. https://www.radware.com/blog/threat-intelligence/shadowleak/

Chen, J., Henry, E., & Jiang, X. (2023). Is Cybersecurity Risk Factor Disclosure Informative? Evidence from Disclosures Following a Data Breach. *J Bus Ethics*, *187*, 199–224. https://doi.org/10.1007/s10551-022-05107-z

Claburn, T. (2025, October 7). *Employees regularly paste company secrets into ChatGPT: Microsoft Copilot, not so much*. The Register. https://www.theregister.com/2025/10/07/gen_ai_shadow_it_secrets/

Collins, E. M. (2024a). *National Taxpayer Advocate 2023 Annual Report to Congress*. Taxpayer Advocate Service. https://www.taxpayeradvocate.irs.gov/reports/2023-annual-report-to-congress/

Collins, E. M. (2024b, June 6). *Identity Theft Victims Are Waiting Nearly Two Years to Receive Their Tax Refunds*. Taxpayer Advocate Service. https://www.taxpayeradvocate.irs.gov/news/nta-blog/identity-theft-victims-are-waiting-nearly-two-years-to-receive-their-tax-refunds/2024/06/

Eshed, O. (2025). *LayerX Enterprise AI and SaaS Data Security Report 2025: Real-world insights into enterprise AI and SaaS usage, blindspots, governance gaps, and data leakage channels*. LayerX.

Federico, C., & Thompson, T. (2023). Amusing Inventions Not to Be Thrown Away: ChatGPT and the Future of Tax. *Journal of Tax Practice and Procedure*, *25*(2), 21. https://link-gale-com.aurarialibrary.idm.oclc.org/apps/doc/A759394139/AONE?u=auraria_main&sid=bookmark-AONE&xid=044ef8e6

Google Cloud. (2025). *What is vibe coding?* https://cloud.google.com/discover/what-is-vibe-coding

Huang, H. H., & Wang, C. (2021). Do Banks Price Firms' Data Breaches? *The Accounting Review*, *96*(3), 261–286. https://doi.org/10.2308/TAR-2018-0643

Internal Revenue Service. (2024a). *Publication 4557. Safeguarding Taxpayer Data: A Guide for Your Business* (No. Rev. 6-2024). https://www.irs.gov/pub/irs-pdf/p4557.pdf

Internal Revenue Service. (2024b). *Publication 5708. Creating a Written Information Security Plan for your Tax & Accounting Practice* (Rev. 8-2024). https://drive.google.com/drive/u/0/folders/1bGeCvOZnLnbL18PJ4cliBt-GDWFY749B

Internal Revenue Service. (2024c, November). *About the Security Summit*. https://www.irs.gov/pub/newsroom/about_the_security_summit.pdf

Internal Revenue Service. (2025, February 27). *Dirty Dozen tax scams for 2025: IRS warns taxpayers to watch out for dangerous threats (IR-2025-26)*. https://www.irs.gov/newsroom/

Internal Revenue Service, Office of Chief Counsel. (2020). *Notice CC-2020-007*. U.S. Department of the Treasury. https://www.irs.gov/pub/irs-ccdm/cc-2020-007.pdf

Kahn, J. (2025). *Mastering AI: A Survival Guide to Our Superpowered Future*. Simon & Schuster.

Karpathy, A. (2025, February). *There's a new kind of coding I call "vibe coding," where you fully give in to the vibes…* [Post]. X. https://x.com/

Lehner, O. M., Ittonen, K., Silvola, H., & Strëm, E. (2022). Artificial Intelligence Based Decision-making in Accounting and Auditing: Ethical Challenges and Normative Thinking. *Accounting, Auditing & Accountability Journal*, *35*(9), 109–135. https://doi.org/10.1108/AAAJ-09-2020-4934

LexisNexis. (2015). *The Rise in State Income Tax Refund Identity Fraud: The True Challenges and New Ways to Combat it*. https://risk.lexisnexis.com/insights-resources/white-paper/the-rise-in-state-income-tax-refund-identity-fraud

Love, H. C., & Valenti, S. P. (2021). Taking back control with quality management. *The Tax Adviser*, *52*(11). https://link-gale-com.aurarialibrary.idm.oclc.org/apps/doc/A698138467/AONE?u=auraria_main&sid=summon&xid=6d047759

Mat Hussin, N. A. K., Mohd Bukhari, N. A. N., Nor Hashim, N. H. A., Shaipul Bahari, S. N. A., & Mohd Ali, M. (2024). The Impact of Artificial Intelligence on the Accounting Profession: A Concept Paper. *Business Management and Strategy*, *15*(1), 34–50. https://doi.org/10.5296/bms.v15i1.21620

National Institute of Standards and Technology (NIST). (2025). *What is post-quantum cryptography?* NIST. https://www.nist.gov/cybersecurity/what-post-quantum-cryptography

Nield, J., Scanlan, J., & Roehrer, E. (2020). Exploring Consumer Information-Security Awareness and Preparedness of Data-Breach Events. *Library Trends*, *68*(4), 611–635. https://doi.org/10.1353/lib.2020.0014

Pathade, C. (2025). Red Teaming the Mind of the Machine: A systematic evaluation of prompt injection and jailbreak vulnerabilities in LLMs. In *arXiv*. https://arxiv.org/abs/2505.04806

Sawyers, R., & Gill, S. (2021). *Federal Tax Research* (12th ed.). Cengage.

Talesh, S. A. (2018). Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Businesses. *Law & Social Inquiry*, *43*(2), 417–440. https://doi.org/10.1111/lsi.12303

Thomson Reuters Institute. (2024). *Generative AI in Professional Services: Perceptions, Usage & Impact on the Future of Work*. https://www.thomsonreuters.com/en/reports/2024-generative-ai-in-professional-services

Treasury Inspector General for Tax Administration. (2017). *The Number of Employment-Related Identity Theft Victims Is Significantly Greater Than Identified* (Nos. 2017-40–031). https://www.tigta.gov/sites/default/files/reports/2024-11/201740031fr.pdf

Vaaler, P. M., & Greenwood, B. (2023). Do US State Breach Notification Laws Decrease Firm Data Breaches? *Review of Law & Economics*, *19*(3), 263–316. https://doi.org/10.1515/rle-2023-0038

Willison, S. (2025, March 19). *Not all AI-assisted programming is "vibe coding."* https://simonwillison.net/2025/Mar/19/vibe-coding/