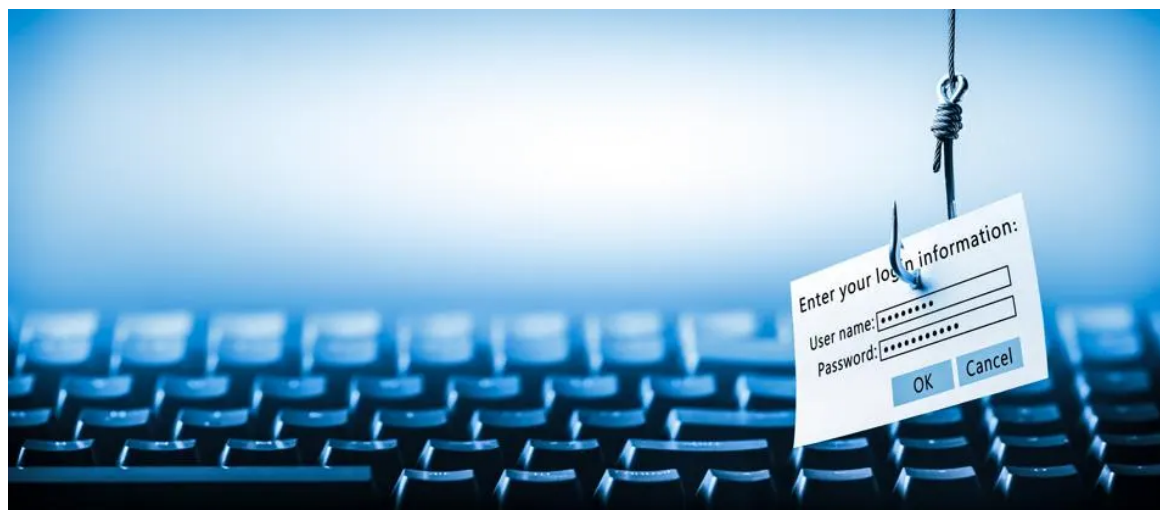


FORBES &gt; MONEY &gt; TAXES

# Phishing Scams Are Targeting You And Your Tax Preparer

**Amber Gray-Fenner** Contributor ⓘ*I cover individual tax issues and IRS developments.*[Follow](#)

Jan 24, 2024, 12:25pm EST



Increasingly sophisticated scammers are targeting taxpayers and tax return preparers. GETTY

At least one “potential new client” phishing scam arrives in my inbox every day asking me to “take a look at the attached W2 and last year’s tax return.” Typically, these e-mails arrive with other e-mails that purport to be from my various software vendors that are asking me to update my credentials or password by clicking a link. I don’t click the link. Neither should you.

Phishing scams were number two on the IRS’ annual [Dirty Dozen](#) list

of tax scams for 2023 (right behind fraudulent ERC claims). Brad Messner, EA and owner of [Financial Guardians, LLC](#) (a firm that specializes in cybersecurity for tax professionals), recently noted that in addition to the usual types of phishing scams there has been a “massive increase” in people sending out phishing e-mails that look like e-signature requests.

I received one such request last week. The request asked me to answer various knowledge-based authentication questions, provide a PIN, and enter a password in order to provide an electronic signature on a document. It looked legitimate. It had what appeared to be a person’s name and an authentic-looking e-mail address as the sender. I also had recently told someone that I was happy to do e-signatures on some documents. It was only after I paused to think that I realized I had given that office a different e-mail address and that this particular e-mail was a fake.

According to Messner, the Department of Defense is expecting a significant increase in e-signature-related phishing attacks moving forward. Messner also noted he was shocked that it took scammers this long to start getting aggressive with this type of attack “because the world converted to e-signatures in 2020 and it is now 2024.” Nevertheless, he expressed appreciation for the delay.

Messner offered the following tips for taxpayers:

- Be skeptical about e-mails you aren’t expecting even if they look like they are from your tax professional.
- Be aware of services you use that use a generic e-mail to send

messages (*e.g.*, donotreply@domain.com). These services are at higher risk for being used to run a phishing scam because scammers find them attractive targets (those generic e-mail addresses are easy to spoof).

- Check your service provider's online portal rather than clicking a link in an e-mail from donotreply@myfinancialinstitution.com even if you are expecting that service provider to have online documents for you. It's always best when you receive an e-mail from a service provider to log on independently via your web browser rather than clicking a link.
- Do not click on buttons or links in unexpected e-mails. Don't even open unexpected e-mails. Delete them immediately and block the sender.
- Be sure you have phishing scanning configured for your e-mail. Messner says most paid security suites have e-mail security, but many free e-mail options do not offer built-in security (you may have to purchase it or upgrade to a paid version of the e-mail service). If you are using e-mail in your business, both Google GOOG +0.1% Workspace and MSOffice 365 have built-in security. Nevertheless, Messner notes "It's always good to verify what you have and review your settings periodically."

---

MORE FROM [FORBES ADVISOR](#)

## Best Tax Software Of 2022

## Best Tax Software For The Self-Employed Of 2022

### Income Tax Calculator: Estimate Your Taxes

---

“These phishing attackers are starting to use generative AI to create e-mails that are both personalized and removing the typical triggers we see that flag them as phishing attacks (*e.g.*, spelling and grammar errors).” The attacks aren’t just about tax returns or banking information either. They are often disguised to look like they are about updating your healthcare insurance or 401(k) information or have something to do with your mortgage or FASFA.

---

**Investing Digest: Know what's moving the financial markets and what smart money is buying with Forbes Investing Digest.**

Sign Up

By signing up, you accept and agree to our [Terms of Service](#) (including the class action waiver and arbitration provisions), and [Privacy Statement](#).

---

Messner also reminds taxpayers that their tax return professionals are a tasty target for phishing scammers “because of the valuable information they have access to and store.” When hiring a tax professional “Ask them what their security policy is. You're typically going to get a blank stare.” This even though all paid practitioners are required by the IRS to have a Written Information Security Plan (or WISP).

He goes on to say that you don’t necessarily want your tax professional to be highly specific about their security plan because that could mean they are willing to provide that information to a

malicious actor. “You want just enough information to be confident that they are taking security seriously.” Messner recommends avoiding tax professionals who ask you to e-mail sensitive content or materials. It’s simply not a best practice even when using secure e-mail providers, having strong security settings, and using password-protected attachments.

Another potential security red flag for taxpayers looking for a tax professional is if the taxpro agrees to engage you as a client with little due diligence or insight into your operation. Messner says “Taking on any client without review is a red flag because they [the practitioner] might miss a bad actor because they aren’t vetting clients properly.” That could put your information is at risk.

Sometimes quick client onboarding can mean that the “ tax practitioner” is just going to take your information and disappear. Messner mentioned a case in Mississippi where a “tax preparer” didn’t prepare the client returns at all, “They just collected info and vanished.”

Stay safe out there!

*Follow me on [Twitter](#) or [LinkedIn](#).*



**Amber Gray-Fenner**

Follow

I own Tax Therapy, LLC, in Albuquerque, New Mexico. I am an Enrolled Agent and non-attorney practitioner admitted to the bar of the U.S. Tax Court. I...

**Read More**

[Editorial Standards](#)

[Print](#)


[Reprints & Permissions](#)

ADVERTISEMENT

---

## Join Our Conversation

---

Commenting on this article  
has ended  [Log in](#)

---

Powered  
by



[Terms](#) | [Privacy](#) | [Feedback](#)