

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

clients looking for tax help.

Jason Bramwell • Jan. 09, 2024



With the [2024 filing season right around the corner](#), the IRS is alerting tax professionals about a new round of email schemes in which cybercriminals pose as potential clients looking for tax help.

Previously, the IRS has seen a surge in these “new client” scams during tax season where identity thieves target accounting and tax preparation firms with fake emails. In these scams, fraudsters pretend to be actual taxpayers seeking help with

their taxes and use emails to try to obtain sensitive information or gain access to tax

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

The objective of the new client email scam is to steal sensitive personal information that will allow fraudsters to prepare authentic-looking tax returns to collect a refund—or use it to commit other types of fraud.

The IRS provided an example of what the current new client scam looks like:

Subject: 2024 Tax Submission

Hello,

My name is (name can vary), I am searching for another CPA to help handle my taxes.

Is it safe to say that you are accepting new clients for the 2024 tax season? Do you additionally assist with IRS representation?

I figured I may have an issue with last year's return. (Click) [HERE TO VIEW MY CREDENTIAL](#) [Link to a phishing web address]

Upon your approval, we can arrange a physical or virtual meeting to discuss my situation and also provide my tax documents amongst others.

Kindly prompt how you plan to push ahead.

Best Regards,

(Name varies)

New client scammers often try a direct approach by sending an email asking the tax professional to help them with their taxes where the phishing email contains a

malicious link or attachment, or the scammer might take a more cautious approach

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

In one of the latest examples seen by the IRS, the new client scam features several red flags that should raise questions about the legitimacy of the email. This includes awkwardly phrased sentences and odd word usage. However, with access to a stolen email account, scammers can find a legitimate email from a previous victim's email account between the victim and their tax preparer. This email might have no grammatical or spelling mistakes and could reference what seems to be legitimate tax issues, which is then repurposed as part of the new client phishing scam. The subject line will often reference the current tax season and the underlying message will amount to the sender needing someone to "help prepare their taxes."

In some cases, new client phishing emails may appear to come from a legitimate sender or organization—perhaps even a friend or colleague—because their friend or colleague had their email account credentials stolen. The IRS recommends that tax professionals set up two-factor or multifactor authentication with their email provider to reduce the risk of having their email account compromised.

Posing as a trusted organization or friend remains a common way to target individuals and tax preparers for a variety of scams, according to the IRS. Individuals should verify the identity of the sender by using another communication method, such as calling a number they independently know to be accurate, not the number provided in the email or text.

Last year, the IRS received hundreds of reports at phishing@irs.gov of the new client scam. The new client scam made up roughly two-thirds of the 400 reports of business email compromise or business email spoofing complaints that the IRS received.

Given the mass production of these messages by cybercriminals, the number of actual spearphishing emails sent to tax professionals associated with these campaigns

likely runs into the thousands with the goal to reach tens of thousands of preparers

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

© 2024 Firmworks, LLC. All rights reserved