

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

"Action Required: Your account has now been put on hold." The IRS has observed similar bogus emails that claim to be from a "tax preparation application provider."

Isaac M. O'Bannon • Feb. 20, 2022



With tax season in full swing, the Internal Revenue Service, state tax agencies and technology and service providers that serve the profession are warning tax professionals of new email scams that attempt to steal their tax software preparation credentials.

The Security Summit partners warned these scams serve as a reminder that [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

"Scams continue to evolve, and this one is especially sinister since it threatens tax professional's accounts," said IRS Commissioner Chuck Rettig. "Tax professionals must remain vigilant in identifying and staying clear of these IRS impersonation emails. A little extra care can protect the tax professionals and their clients."

Emails claiming "Your account has been put on hold" are scams

The IRS has observed similar bogus emails that claim to be from tax software providers. The scam email will send users to a website that shows the logos of several popular tax software preparation providers. Clicking on one of these logos requests tax preparer account credentials.

The IRS warns tax pros not to respond or take any of the steps outlined in the email. Similar emails include malicious links or attachments that are set up to [steal information](#) or to download malware onto the tax professional's computer.

In this case, if recipients enter their credentials into the pop up window, thieves can use this information to file fraudulent returns by using credentials that were provided by the tax professional.

An example of this type of bogus email states:

Your account has now been put on hold

ALL preparers are required to apply security feature to their Tax Pro account towards 2021 Tax Returns processing. You have failed to apply new update before expiry date You are restore and update your acc/ount immediately. Please Click Here to update your acc/ount now. Important Failure to update your account within the next 24hours will lead to you

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

Tax professionals who get a [scam email](#) should save the email as a file and then send it as an attachment to phishing@irs.gov. They should also notify the Treasury Inspector General for Tax Administration at www.tigta.gov to report the IRS impersonation scam. Both TIGTA and the [IRS Criminal Investigation division](#) are aware of this scam.

The IRS, state tax agencies and the nation's tax industry – working together in the Security Summit initiative – have taken numerous steps since 2015 to protect taxpayers, businesses and the tax system from identity thieves. Summit partners continue to warn people to watch out for common scams and schemes this tax season.

For additional information and help, tax professionals should review [Publication 4557, Safeguarding Taxpayer Data and Identity Theft Information for Tax Professionals](#).

Technology

CPA Practice Advisor is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.

© 2024 Firmworks, LLC. All rights reserved