



Rhode Island Department of Revenue

Division of Taxation

ADV 2020-54
SECURITY SUMMIT

ADVISORY FOR TAXPAYERS AND TAX PROFESSIONALS
DECEMBER 1, 2020

Online tax preparation products to offer multi-factor authentication

Feature will help taxpayers and tax preparers safeguard their information

PROVIDENCE — The Rhode Island Division of Taxation, the Internal Revenue Service, and other partners in the Security Summit announced today an improved feature that will be available on all 2021 online tax preparation products.



Designed to protect both taxpayers and tax professionals, multi-factor authentication means the returning user must enter two pieces of data to securely access an account or application. For example, taxpayers must enter their credentials (username and password) plus a numerical code sent as a text to their mobile phone.

The agreement to add the multi-factor authentication feature is just one publicly visible example of the ongoing collaboration by the IRS, state tax agencies and the tax industry, which work together as the Security Summit.

“Multi-factor authentication option is an easy, free way to really step up protection of your data whether you’re a taxpayer or a tax professional,” said Chuck Rettig, IRS Commissioner.

“This is an important step being taken by the tax software industry. This is just one example of the many actions taken by the Security Summit partners over the past five years that have dramatically improved our ability to combat identity thieves and to protect taxpayers,” said Rhode Island Tax Administrator Neena Savage, who oversees the Division of Taxation.

Standard feature

Some online products previously offered multi-factor authentication. However, for 2021 all providers agreed to make it a standard feature and all agreed that it would meet requirements set by the National Institute of Standards and Technology. (Multi-factor authentication may not be available on over-the-counter hard disk tax products.)

Because the multi-factor authentication option is voluntary, Security Summit partners urged both taxpayers and tax professionals to use it. Multi-factor authentication can reduce the likelihood of identity theft by making it difficult for thieves to get access to sensitive accounts.

Users should check the security section in their online tax product account to make the change. It may be labeled as two-factor authentication or two-step verification or similar names.

Use of multi-factor authentication is especially important for tax professionals who continue to be prime targets of identity thieves. Of the numerous data thefts reported to the IRS from tax professional offices this year, most could have been avoided had the practitioner used multi-factor authentication to protect tax software accounts.

Thieves use a variety of scams – but most commonly by a phishing email – to download malicious software, such as keystroke software. This malware will eventually enable them to steal all passwords from a tax pro. Once the thief has accessed the practitioner’s networks and tax software account, they will complete pending taxpayer returns, alter refund information and use the practitioner’s own e-filing and preparer numbers to file the fraudulent return – a dangerous combination.

However, with multi-factor authentication, it’s unlikely the thief will have stolen the practitioner’s cell phone — blocking the ability to receive the necessary security code to access the account. This protects the tax pro’s account information.

Multiple options

There are multiple options for multi-factor authentication. For example, taxpayers and tax practitioners can download an authentication app to their mobile device. These apps are readily available through Google Play or Apple’s App Store. Once properly configured, these apps will generate a temporary, single-use security code, which the user must enter into their tax software to complete authentication. Use a search engine for “Authentication apps” to learn more.

Other options include codes that may be sent to practitioner’s email or mobile phone via text, but those are not as secure as an authentication app.

While no product is foolproof, multi-factor authentication does dramatically reduce the likelihood that taxpayers or tax practitioners will become victims. Multi-factor authentication should be used wherever it is offered. For example, financial accounts, social media accounts, cloud storage accounts and popular email providers all offer multi-factor authentication options.

The Security Summit consists of the IRS, the Rhode Island Division of Taxation, other states’ tax agencies, and the tax community -- including tax preparation firms, software developers, tax professional organizations, and financial institutions. Partners in the Security Summit work together to combat identity theft and fight other scams to protect the nation’s taxpayers. To learn more about the Security Summit: <https://www.irs.gov/newsroom/security-summit>.
