Prep Systems

The Internal Revenue Service, state tax agencies and the tax industry have announced an improved feature that will be available on all 2021 online tax preparation products.

Dec. 04, 2020

The Internal Revenue Service, state tax agencies and the tax industry have announced 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

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 Summit partners over the past five years that have dramatically improved our ability to combat identity thieves and to protect taxpayers."

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, 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-

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 fool-proof, 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 IRS, state tax agencies, the private sector tax industry, including tax professionals, work in partnership as the Security Summit to help protect taxpayers from identity theft and refund fraud. This is the second in a week-long series of tips to raise awareness about identity theft. See IRS.gov/securitysummit for more details.

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.