IRS News Release

Internal Revenue Service
Media Relations Office
Washington, D.C.

Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

Security Summit partners urge tax pros to use multi-factor authentication; critical step to boost protection against data theft

IR-2021-155, July 20, 2021

WASHINGTON – With security incidents on the rise, the Internal Revenue Service, state tax agencies and the tax industry urged tax professionals and taxpayers to use a special feature – multi-factor authentication – available on tax software products to help protect against identity and data theft.

The Security Summit partners today kicked off the annual 2021 “Protect Your Clients; Protect Yourself” summer campaign aimed at tax professionals. This year’s theme is “Boost Security Immunity: Fighting Against Identity Theft” to urge tax professionals to step up their efforts to protect client data amid the pandemic and its aftermath.

Multi-factor authentication, also known as two-factor authentication, provides more security. It allows the tax professional or taxpayer to use another feature such as a security code sent to a mobile device, a pin number or a fingerprint in addition to the username and password. A thief may steal usernames and passwords but cannot access accounts without the additional multifactor feature.

“The Security Summit has made great strides to protect the tax community, but we need the help of everyone in the tax professional community,” said IRS Commissioner Chuck Rettig. “Using the multi-factor authentication feature available on tax preparation products is one of the easiest and cheapest security measures any tax pro can take. It’s offered for free by the tax software providers. As people continue to get vaccines, we urge tax professionals as well as taxpayers to boost their security immunity and help in the battle against identity theft.”

This marks the sixth year of the tax professional campaign, part of a wider effort by the Security Summit coalition of the IRS, state tax agencies and the nation’s tax community to strengthen protections against identity and data theft threatening the tax system. This is the first in a series of weekly news releases running through Aug. 17.

Through June 30, 2021, there have been 222 data theft reports this year from tax professionals to the IRS, outpacing the rate of 211 in 2020 and 124 in 2019. Each individual report may involve hundreds to thousands of taxpayers. Client information stolen from tax professionals’ offices is used to create fraudulent tax returns that are difficult to detect because the identity thief is using real financial data.

Based on reports to the IRS in 2020, many tax professionals whose client data was stolen failed to use multifactor authentication, and the feature could have prevented some of the thefts. Tax professionals also should use multi-factor authentication features anywhere it is offered, such as commercial email products and cloud storage providers.

Multi-factor authentication is just one of several security steps tax professionals – and taxpayers – should use to protect sensitive data. Other steps include:

- Use anti-virus software and set it for automatic updates. Anti-virus software scans existing files and drives on computers - and mobile phones – to protect from malware.
- Use a firewall to shield digital devices from external attacks.
- Use backup software/services to protect data. Making a copy of files can be crucial, especially if the user becomes a victim of a ransomware attack.
- Use drive encryption to secure computer locations where sensitive files are stored. Encryption makes data on the files unreadable to unauthorized users.

- Create and secure Virtual Private Networks. A VPN provides a secure, encrypted tunnel to transmit data between a remote user via the Internet and the company network. Search for “Best VPNs” to find a legitimate vendor; major technology sites often provide lists of top services.

The IRS also reminds tax professionals that federal law, enforced by the Federal Trade Commission, requires all professional tax preparers to create and implement a data security plan. The IRS also recommends tax professionals create a data theft response plan, which includes contacting the IRS Stakeholder Liaisons to report a theft.

Additional resources
Tax professionals also can get help with security recommendations by reviewing IRS Publication 4557, Safeguarding Taxpayer Data, and Small Business Information Security: The Fundamentals by the National Institute of Standards and Technology. The IRS Identity Theft Central pages for tax pros, individuals and businesses have important details as well.

Publication 5293, Data Security Resource Guide for Tax Professionals, provides a compilation of data theft information available on IRS.gov. Also, tax professionals should stay connected to the IRS through subscriptions to e-News for Tax Professionals and Social Media.

For more information, see Boost Security Immunity: Fighting Against Identity Theft.

-30-