INTERNAL REVENUE SERVICE

IRS News Release

Media Relations Office	**Washington, D.C.**	Media Contact: 202.317.4000
www.IRS.gov/newsroom		Public Contact: 800.829.1040

IRS Warns of a New Wave of Attacks Focused on Tax Professionals

IR-2016-119, Sept. 2, 2016

WASHINGTON – The Internal Revenue Service today warned tax professionals of a new wave of attacks that allow identity thieves to file fraudulent tax returns by remotely taking over practitioners' computers.

As part of the Security Summit effort, the IRS urged tax professionals to review their tax preparation software settings and immediately enact all security measures, especially those settings that require usernames and passwords to access the products. The IRS is aware of approximately two dozen cases where tax professionals have been victimized in recent days.

The IRS, state tax agencies and the tax industry – working as partners in the Security Summit – recently launched the Protect Your Clients; Protect Yourself campaign to increase awareness that criminals increasingly are targeting tax professionals and the taxpayer data they possess.

"This latest incident reinforces the need for all tax professionals to review their computer settings as soon as possible," said IRS Commissioner John Koskinen. "Identity thieves continue to evolve and look for new areas to exploit, especially as our fraud filters become more effective. The prompt identification of these attacks is another example of the great benefits that result from the close working relationship the IRS now has with the tax industry and the states through the Security Summit initiative. Information is flowing more rapidly between our groups as we continue our efforts to protect taxpayers."

These attacks come as the Oct. 17 deadline approaches for extension filers. The IRS first warned of a similar remote take-over attack in the spring, just ahead of the April 15 deadline, another peak period for tax professionals.

Thieves are able to access tax professionals' computers and use remote technology to take control, accessing client data and completing and e-filing tax returns but directing refunds to criminals' own accounts.

Victims in the tax community learned of these thefts while reconciling e-file acknowledgements.

In addition to activating security measures for tax software products, IRS urges all tax preparers to take the following steps:

- Run a security “deep scan” to search for viruses and malware;
- Strengthen passwords for both computer access and software access; make sure your password is a minimum of eight digits (more is better) with a mix of numbers, letters and special characters and change them often;
- Be alert for phishing scams: do not click on links or open attachments from unknown senders;
- Educate all staff members about the dangers of phishing scams in the form of emails, texts and calls;
- Review any software that your employees use to remotely access your network and/or your IT support vendor uses to remotely troubleshoot technical problems and support your systems. Remote access software is a potential target for bad actors to gain entry and take control of a machine.

In addition, the IRS recently issued instructions to tax professionals on how to monitor their PTIN activity.

Tax professionals should review Publication 4557, Safeguarding Taxpayer Data, a Guide for Your Business, which provides a checklist to help safeguard taxpayer information and enhance office security. Also, practitioners should review Data Breach Information for Tax Professionals for information on what action they should take if they do become victims.

--30--