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

looking to do more than just peek at client information: The hackers are trying to take those networks over, says the IRS and state tax agencies. If that happens, the ...

Isaac M. O'Bannon • Sep. 21, 2017

How to Prevent Your Office Network From Being Hijacked

By Isaac M. O'Bannon, Managing Editor

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

completed those returns, e-filed them and secretly directed refunds to their own accounts.

Increasing awareness about remote takeovers is part of the "Don't Take the Bait" campaign, a 10-part series aimed at tax professionals. The IRS, state tax agencies and the tax industry, working together as the Security Summit, urge practitioners to learn to protect themselves from remote takeovers. This is part of the ongoing Protect Your Clients; Protect Yourself effort.

"This is another emerging threat to tax professionals that the IRS has seen on the rise," IRS Commissioner John Koskinen said. "A remote takeover can be devastating to practitioners' business as well as to the taxpayers they serve. It's critical for people to take steps to understand and prevent these security threats before it's too late."

A remote attack targets an individual computer or network as the cybercriminal exploits weaknesses in security settings to access the devices. Another line of attack uses malware to download malicious code that gives the criminals access to the network. Especially vulnerable are wireless networks, including mobile phones, modems and router devices, printers, fax machines and televisions that retain their factory-issued password settings. Sometimes, these devices have no protection at all.

There are multiple ways that cybercriminals can gain control of computers and other devices. Phishing emails with attachments can easily download malware that, when opened, give the criminal remote control of a computer.

Cybercriminals also can deploy certain tools that allow them to identify the location of and get access to unprotected wireless devices. For example, a printer with a factory-issued password can easily be accessed, and the criminals can see tax return information stored in its memory.

The IRS urges tax professionals to take the following steps to help protect themselves

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

- Identify and assess wireless devices connected to the nwww.cpapracticeadvisor.com/1236449etwork, including mobile phones, computers, printers, fax machines, routers, modems and televisions. Replace factory password settings with strong passwords.
- Strengthen passwords for devices and for software access. Make sure passwords are a minimum of eight digits (more is better) with a mix of numbers, letters and special characters;
- Be alert for phishing scams: do not click on links or open attachments from unknown, unsolicited or suspicious senders;
- Review any software that employees use to remotely access the network as well as those used by IT support vendors to remotely troubleshoot technical problems. Remote access software is a potential target for bad actors to gain entry and take control of a machine. Disable remote access software until it is needed.

===== +

Top Firm Management Social Media:

Will Harvey Teach Us the Dangers of Short Term Thinking? John Battelle via LinkedIn. http://bit.ly/2vJCZtX

3 Tips for Great Customer Experience at Accounting Firms. Amanda C. Watts via LinkedIn. http://bit.ly/2wmzDf8

How Team Members Read a Leader's Body Language. Carol Goman, Ph.D. via

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

===== +

Latest Firm Management News:

How Tomorrow's Managing Partners Will Change the Profession. This new crop of partners will take what they've learned in the coming years and likely change how accounting firms are managed. . http://cpapracticeadvisor.com/12360787

Value Pricing in the Real World. Value pricing for professional service firms really started to get discussed in the last decade. For over ten years, the virtues of assigning true value to your education, expertise, and work has been touted. www.cpapracticeadvisor.com/12360851

Summit Brings Together Firm leaders to Discuss the Future. A diverse and talented group of law firm and accounting firm leaders from around the world spent two days sharing their experience and best practices in firm leadership. www.cpapracticeadvisor.com/1236449

CohnReznick Internship Program Named Among Best. Interns are assigned projects on real client engagements across industries such as renewable energy, technology, life sciences, and real estate. www.cpapracticeadvisor.com/12362529

23% of Professionals Regret Leaving Former Job. In a recent survey from staffing firm Accountemps, 23 percent of workers polled said they have regrets about leaving their former job. www.cpapracticeadvisor.com/12360827

Firm Management • Technology

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