

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

other tax issues as a cover to trick people into giving up sensitive information such as passwords, Social Security numbers or credit card numbers or to make ...

Aug. 16, 2016



The [IRS](#) is warning tax pros that scammers are now using fake emails that pretend to be from tax software providers and tries to trick recipients into clicking on a bogus software update link.

The email scheme is the latest in a series of attempts by fraudsters to use the IRS or other tax issues as a cover to trick people into giving up sensitive information such as

passwords, Social Security numbers or credit card numbers or to make unnecessary

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

has a naming convention that uses the actual name of their software followed by an ".exe extension."

Upon completion, tax professionals believe they have downloaded a software update when in fact they have loaded a program designed to track the tax professional's key strokes, which is a common tactic used by cyber thieves to steal login information, passwords and other sensitive data.

Although the IRS knows of only a handful of cases to date, tax professionals are encouraged to be on the lookout for these scams and never to click on unexpected links in emails. Similar email schemes using tax software names have targeted **individual taxpayers**.

The IRS recently launched a new campaign to raise awareness among tax professionals about security threats posed by identity theft issues targeting their industry. The **Protect Your Clients; Protect Yourself** campaign features an ongoing effort to urge tax professionals to step up their security protections and be aware they increasingly are targets of cybercriminals.

### **The IRS urges all tax preparers to take the following steps:**

- Be alert for phishing scams: do not click on links or open attachments contained in e-mails and always utilize a software provider's main webpage for connecting to them.
- 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 8 digits long (more is better) with a mix of numbers, letters and special characters;
- 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

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

Taxes

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.

© 2024 Firmworks, LLC. All rights reserved