



Department of
Taxation

New IRS warning about phishing e-mail scheme

To maximize awareness, the Ohio Department of Taxation is sharing this message from the IRS warning of a new phishing e-mail scam that targets tax preparers. Please visit www.irs.gov for additional information.

Partners,

Late last week (8-11-2016), the Internal Revenue Service warned tax professionals of a new phishing e-mail scheme in which cybercriminals mimic software providers. The e-mail attempts to trick recipients into clicking on a bogus link which requests them to download and install an important software update. After clicking the link, the recipient is directed to a website which prompts them to download a file to update their software package. After completion of the download, the tax professional has unknowingly put a program onto their machine that is designed to track keystrokes which can lead to stolen 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 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 e-mails, 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.

Tax Professionals should review **IRS Publication 4557**, Safeguarding Taxpayer Data, A Guide for Your Business, which provides a checklist to help safeguard taxpayer information and enhance office security.