http://www.MSCNews.net/news/index.cfm?nk=59377

New Phishing Scheme Mimics Software Providers

The Internal Revenue Service today alerted tax professionals to an emerging phishing email scam that pretends to be from tax software providers and tries to trick recipients into clicking on a bogus 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 payments.

In the new scheme identified as part of the IRS Security Summit process, tax professionals are receiving emails pretending to be from tax software companies. The email scheme requests the recipient to download and install an important software update via a link included in the e-mail.

Once recipients click on the embedded link, they are directed to a website prompting them to download a file appearing to be an update of their software package. The file 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 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 Publication 4557, Safeguarding Taxpayer Data, A Guide for Your Business, which provides a checklist to help safeguard taxpayer information and enhance office security.