campaign currently underway. This awareness effort highlights the many tactics of ...

Aug. 04, 2017

Scammers are trying a new phishing email scam impersonating tax software providers and attempting to steal usernames and passwords, according to the IRS, state tax agencies and the tax industry.

This sophisticated scam yet again displays cybercriminals' tax savvy and underscores the need for tax professionals to take strong security measures to protect their clients and protect their business. This is the time of year when many software providers

issue software upgrades and when tax professionals are working to meet the Oct. 15

Update" and highlights an "Important Software System Upgrade." It thanks recipients for continuing to trust the software provider to serve their tax preparation needs and mimics the software providers' email templates.

The e-mail informs the recipients that due to a recent software upgrade, the preparer must revalidate their login credentials. It provides a link to a fictitious website that mirrors the software provider's actual login page.

Instead of upgrading software, the tax professionals are providing their information to cybercriminals who use the stolen credentials to access the preparers' accounts and to steal client information.

The Security Summit reminds tax professionals that software providers do not embed links into emails asking them to validate passwords. Also, tax professionals and taxpayers should never open a link or an attachment from a suspicious email.

Tax professionals can review additional tips to protect clients and themselves at Protect Your Clients, Protect Yourself on IRS.gov.

Tax professionals who receive emails purportedly from their tax software providers seeking login credentials should send those scam emails to their tax software provider.

For Windows users, follow this process to help the investigation of these scam emails:

1. Use "Save As" to save the scam. Under "save as type" in the drop-down menu, select "plain text" and save to the desktop. Do not click on any links.
2. Open a new email and attach this saved email as a file.
3. Send a new email containing the attachment to the tax software provider, as well as a copy to Phishing@IRS.gov.