INTERNAL REVENUE SERVICE
IRS News Release

Media Relations Office | Washington, D.C. | Media Contact: 202.317.4000
www.irs.gov/newsroom | Public Contact: 800.829.1040

Security Summit Alert: Tax Professionals Warned of New Scam to "Unlock" Their Tax Software Accounts

IR-2017-39, Feb. 17, 2017

WASHINGTON – The Internal Revenue Service, state tax agencies and the tax industry today warned tax professionals to be alert to a new phishing email scam impersonating software providers.

The scam email comes with the subject line, "Access Locked." It tells recipients that access to their tax prep software accounts has been "suspended due to errors in your security details." The scam email asks the tax professional to address the issue by using an "unlock" link provided in the email.

However, the link will take the tax professional to a fake web page, where they are asked to enter their user name and password. Instead of unlocking accounts, the tax professionals actually are inadvertently providing their information to cybercriminals who use the stolen credentials to access the preparers' accounts and to steal client information.

The Security Summit partners, which includes the IRS, state tax agencies and the nation's tax community, remind tax professionals and taxpayers to never open a link or an attachment from a suspicious email. These scams can increase during the tax season.

Tax professionals can review additional tips to protect clients and themselves at the Security Summit's awareness campaign, Protect Your Clients, Protect Yourself, on IRS.gov.

For tax professionals who receive emails purportedly from their tax software providers suggesting their accounts have been suspended, they should send those scam emails to their tax software provider. For Windows users, please 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 your desk top. Do not click on any links.
2. Open a new email and attach this saved email as a file
3. Send your new email containing the attachment your tax software provider, as well as copy Phishing@IRS.gov.

-30-