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

Consumers Warned of New Surge in IRS E-mail Schemes during 2016 Tax Season; Tax Industry Also Targeted

IR-2016-28, Feb. 18, 2016

WASHINGTON - The Internal Revenue Service renewed a consumer alert for e-mail schemes after seeing an approximate 400 percent surge in phishing and malware incidents so far this tax season.

The emails are designed to trick taxpayers into thinking these are official communications from the IRS or others in the tax industry, including tax software companies. The phishing schemes can ask taxpayers about a wide range of topics. E-mails can seek information related to refunds, filing status, confirming personal information, ordering transcripts and verifying PIN information.

Variations of these scams can be seen via text messages, and the communications are being reported in every section of the country.

"This dramatic jump in these scams comes at the busiest time of tax season," said IRS Commissioner John Koskinen. "Watch out for fraudsters slipping these official-looking emails into inboxes, trying to confuse people at the very time they work on their taxes. We urge people not to click on these emails."

This tax season the IRS has observed fraudsters more frequently asking for personal tax information, which could be used to help file false tax returns.

When people click on these email links, they are taken to sites designed to imitate an official-looking website, such as IRS.gov. The sites ask for Social Security numbers and other personal information. The sites also may carry malware, which can infect people's computers and allow criminals to access your files or track your keystrokes to gain information.

The IRS has seen an increase in reported phishing and malware schemes, including:

- There were 1,026 incidents reported in January, up from 254 from a year earlier.
- The trend continued in February, nearly doubling the reported number of incidents compared to a year ago. In all, 363 incidents were reported from Feb. 1-16, compared to the 201 incidents reported for the entire month of February 2015.
- This year's 1,389 incidents have already topped the 2014 yearly total of 1,361, and they are halfway to matching the 2015 total of 2,748.

"While more attention has focused on the continuing IRS phone scams, we are deeply worried this increase in email schemes threatens more taxpayers," Koskinen said. "We continue to work cooperatively with our partners on this issue, and we have taken steps to strengthen our processing systems and fraud filters to watch for scam artists trying to use stolen information to file bogus tax returns."

As the email scams increase, the IRS is working on this issue through the Security Summit initiative with state revenue departments and the tax industry. Many software companies, tax professionals and state revenue departments have seen variations in the schemes.

For example, tax professionals are also reporting phishing scams that are seeking their online credentials to IRS services, for example the IRS Tax Professional PTIN System. Tax professionals are also reporting that many of their clients are seeing the e-mail schemes.

As part of the effort to protect taxpayers, the IRS has teamed up with state revenue departments and the tax industry to make sure taxpayers understand the dangers to their personal and financial data as part of the "Taxes. Security. Together" campaign.

If a taxpayer receives an unsolicited email that appears to be from either the IRS e-services portal or an organization closely linked to the IRS, report it by sending it to phishing@irs.gov. Learn more by going to the Report Phishing and Online Scams page.

It is important to keep in mind the IRS generally does not initiate contact with taxpayers by email to request personal or financial information. This includes any type of electronic communication, such as text messages and social media channels. The IRS has information online that can help protect taxpayers from email scams.

Phishing and malware schemes again made the IRS "Dirty Dozen" tax scam list this year. Check out the last IRS Phishing Scam news release for more info.

What to look for in these scams

Taxpayers receive an official-looking email from what appears to be an official source, whether the IRS or someone in the tax industry.

The underlying messages frequently ask taxpayers to update important information by clicking on a web link. The links may be masked to appear to go to official pages, but they can go to a scam page designed to look like the official page. The IRS urges people not to click on these links but instead send the email to phishing@irs.gov.

Recent email examples the IRS has seen include subject lines and underlying text referencing:

- Numerous variations about people's tax refund.
- Update your filing details, which can include references to W-2.
- Confirm your personal information.
- Get my IP Pin.
- Get my E-file Pin.
- Order a transcript.
- Complete your tax return information.

Numbers provided are for phishing and malware incidents combined.

Additional IRS Resources:

- www.irs.gov/identitytheft
- IRS and Partner Statements on the October 2015 Security Summit Meeting
- Fact Sheet 2016-1, IRS, States and Tax Industry Combat Identity Theft and Refund Fraud on Many Fronts

- Fact Sheet 2016-2, IRS, States and Tax Industry Urge Taxpayers to Join the Effort to Combat Identity Theft
- Fact Sheet 2016-3, IRS Identity Theft Victim Assistance: How It Works
- Fact Sheet 2016-4, How New Identity Security Changes May Affect Taxpayers for 2016

--30--