http://www.MSCNews.net/news/index.cfm?nk=60913

IRS Reminds Taxpayers to Recognize Phishing Scams
The Internal Revenue Service and its Security Summit partners cautioned taxpayers today to avoid identity theft by watching for phishing scams that can increase around the tax season.

The IRS, state tax agencies and the tax industry - all partners in the fight against identity theft- reminded taxpayers that the easiest way for an identity thief to steal taxpayer information is by simply asking for it. As a result, each day people fall victim to phishing scams through emails, texts, or phone and mistakenly turn over important data. In turn, cybercriminals try to use that data to file fraudulent tax returns or commit other crimes.

This is the second reminder to taxpayers during the "National Tax Security Awareness Week." This week, the IRS, states and the tax community are sharing information to taxpayers and tax professionals as a part of the ongoing Security Summit effort to combat refund fraud and identity theft.

Surge in Email, Phishing and Malware Schemes

The IRS saw an approximate 400 percent surge in phishing and malware incidents during the 2016 tax season.

Scam 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. These phishing schemes can ask taxpayers about a wide range of topics. Emails can seek information related to tax refunds, filing status, confirming personal information, ordering transcripts, verifying PIN information and asking people to verify their tax software account.

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

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, which could be used to help file false tax returns. 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.

For more details, see:

- IR-2016-28, Consumers Warned of New Surge in IRS Email Schemes during 2016 Tax Season; Tax Industry Also Targeted
- IR-2016-15, Phishing Remains on the IRS "Dirty Dozen" List of Tax Scams for the 2016 Filing Season

As part of the "Taxes. Security. Together." campaign aimed at encouraging taxpayers to take stronger measures to protect their financial and tax data, the IRS and its Security Summit partners urged people not to give out personal information based on an unsolicited email request.

The campaign calls for taxpayers take the time to examine, identify and avoid emails that:

- **Contain a link.** Scammers often pose as the IRS, financial institutions, credit card companies or even tax companies or software providers. These scams may claim they need the recipient

to update their account or request they change a password. The email offers a link to a spoofing site that may look similar to the legitimate official website. Taxpayers should follow a simple rule: Don't click on the link. If in doubt, they should go directly to the legitimate website to access the account.

- **Contain an attachment.** Another option for scammers is to include an attachment to the email. This attachment may be infected with malware that can download malicious software onto the recipient's computer without their knowledge. If it is spyware, it can track the recipient's keystrokes to obtain information about their passwords, Social Security number, credit cards or other sensitive data. Remember, taxpayers shouldn't open attachments from unknown sources.
- **Are from a "government" agency or "financial institution."** Scammers attempt to frighten people into opening email links by posing as government agencies, financial institutions and even tax companies. Thieves often try to imitate the official organizations, especially tax-related ones during the filing season.
- **Are from a "friend."** Scammers also hack email accounts and try to leverage the stolen email addresses. Recipients may receive an email from a "friend" that just does not seem right. It may be missing a subject for the subject line or contain odd requests or language as the underlying content. If the email seems "odd," taxpayers should avoid clicking on any links or opening attachments.
- **Contain a false "lookalike" URL**. The sending email may try to trick the recipient with the URL or web address. For example, instead of www.IRS.gov, it may be a false lookalike such as www.irs.gov.maliciousname.com. To verify the authenticity, a recipient can place their cursor over the text to view a pop-up of the real URL.

Learning to recognize and avoid phishing emails - and sharing that knowledge with family members - is critical to combating identity theft and data loss.

Additional steps that can help taxpayers protect their personal and financial data are available on the "Taxes. Security. Together." page as well as in Publication 4524, Security Awareness for Taxpayers. Also, taxpayers help spread the word on this week's messages using the hashtag #TaxSecurity in social media platforms.

Additional IRS Resources

IRS Tax Tip: Avoid Identity Theft; Learn How to Recognize Phishing Scam

IRS YouTube Videos:

- Security Summit: Be Cautious When Using Wi-Fi – English
- Phishing- Malware - English | Spanish | ASL