INTERNAL REVENUE SERVICE
IRS News Release

Media Relations Office **Washington, D.C.** **Media Contact: 202.622.4000**
www.IRS.gov/newsroom Public Contact: 800.829.1040

Phishing Schemes Lead the IRS "Dirty Dozen" List of Tax Scams for 2017; Remain Tax-Time Threat

IRS YouTube Videos:
Phishing-Malware: English | Spanish | ASL
Taxes. Security. Together. – English
Security Summit: Be Cautious When Using Wi-Fi – English

IR-2017-x, Feb. 1, 2017

WASHINGTON — The Internal Revenue Service today warned taxpayers to watch out for fake emails or websites looking to steal personal information. These "phishing" schemes continue to be on the annual IRS list of "Dirty Dozen" tax scams for the 2017 filing season.

The IRS saw a big spike in phishing and malware incidents during the 2016 tax season. New and evolving phishing schemes have already been seen this month as scam artists work to confuse taxpayers during filing season.. The IRS has already seen email schemes in recent weeks targeting tax professionals, payroll professionals, human resources personnel, schools as well as average taxpayers.

In these email schemes. Criminals pose as a person or organization you trust and/or recognize. They may hack an email account and send mass emails under another person's name. They may pose as a bank, credit card company, tax software provider or government agency. Criminals go to great lengths to create websites that appear legitimate but contain phony log-in pages. These criminals hope victims will take the bait and provide money, passwords, Social Security numbers and other information that can lead to identity theft.

"These email schemes continue to evolve and can fool even the most cautious person. Email messages can look like they come from the IRS or others in the tax community," said IRS Commissioner John Koskinen. "Taxpayers should avoid opening surprise emails or clicking on web links claiming to be from the IRS. Don't be fooled by unexpected emails about big refunds, tax bills or requesting personal information. That's not how the IRS communicates with taxpayers."

Scam emails and websites also can infect your computer with malware without you knowing it. The malware can give the criminal access to your device, enabling them to access all your sensitive files or track your keyboard strokes, exposing login information.

Compiled annually, the "Dirty Dozen" lists a variety of common scams that taxpayers may encounter anytime but many of these schemes peak during filing season as people prepare their returns or find people to help with their taxes.
For those perpetrating these schemes, the scams can lead to significant penalties and interest and possible criminal prosecution. IRS Criminal Investigation works closely with the Department of Justice (DOJ) to shutdown scams and prosecute the criminals behind them.

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.

Criminals increasingly are targeting tax professionals, deploying varies types of phishing emails in an attempt to access client data. The IRS, state tax agencies and the tax industry also launched a public awareness campaign called Protect Your Client; Protect Yourself to warn tax professionals, offer tips and compile alerts.

If a taxpayer receives an unsolicited email that appears to be from either the IRS or an organization closely linked to the IRS, such as the Electronic Federal Tax Payment System (EFTPS), report it by sending it to phishing@irs.gov. Learn more by going to the Report Phishing and Online Scams page.

Tax professionals who receive unsolicited and suspicious emails that appear to be from the IRS or related to the e-Services program also should report it by sending it to phishing@irs.gov.

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.

Each and every taxpayer has a set of fundamental rights they should be aware of when dealing with the IRS. These are your Taxpayer Bill of Rights. Explore your rights and our obligations to protect them on IRS.gov.

Related Items

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

—30—