COMPTROLLER of MARYLAND
Serving the People

Peter Franchot

TAXPAYER *Tips*

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

ANNAPOLIS (February 2, 2017) — The Internal Revenue Service warns taxpayers to watch 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 already have been seen this month as scam artists work to confuse taxpayers during filing season. The IRS has 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 the taxpayer trusts or recognizes. 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.

IRS Commissioner John Koskinen said taxpayers should avoid opening surprise emails or clicking on web links claiming to be from the IRS and shouldn't be fooled by unexpected emails about big refunds, tax bills or requesting personal information. Scam emails and websites also can infect a taxpayer's computer with malware without the user knowing it. The malware can give the criminal access to the device, enabling them to access all sensitive files or track 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 shut down scams and prosecute the criminals behind them.

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.

For more information, visit IRS.gov.

###