



## N E W S & I N S I G H T S

### IRS WARNS TAXPAYERS TO BEWARE OF TAX SCAMS

FEBRUARY 14, 2017

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 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. 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.

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](mailto:phishing@irs.gov).