

# IRS News Release

Media Relations Office

Washington, D.C.

Media Contact: 202.622.4000

[www.IRS.gov/newsroom](http://www.IRS.gov/newsroom)

Public Contact: 800.829.1040

## Phishing Remains on the IRS “Dirty Dozen” List of Tax Scams for the 2016 Filing Season

### **IRS YouTube Video:**

Phishing-Malware: [English](#) | [Spanish](#) | [ASL](#)

Taxes. Security. Together. – [English](#)

IR-2016-15, Feb. 3, 2016

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 2016 filing season.

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 to get the victim’s money, passwords, Social Security number and identity.

"Criminals are constantly looking for new ways to trick you out of your personal financial information so be extremely cautious about opening strange emails," said IRS Commissioner John Koskinen. "The IRS won't send you an email about a tax bill or refund out of the blue. We urge taxpayers not to click on any unexpected emails claiming to be from the IRS."

Scam emails and websites also can infect your computer with malware without you even 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.

Illegal 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.

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). 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.

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.

**Additional IRS Resources:**

- [Report Phishing and Online Scams](#)
- [www.irs.gov/identitytheft](http://www.irs.gov/identitytheft)
- [IRS and Partner Statements on the October 2015 Security Summit Meeting](#)
- [IRS Fact Sheet 2016-1: IRS, States and Tax Industry Combat Identity Theft and Refund Fraud on Many Fronts](#)
- [IRS Fact Sheet 2016-2: IRS, States and Tax Industry Urge Taxpayers to Join the Effort to Combat Identity Theft](#)
- [IRS Fact Sheet 2016-3: IRS Identity Theft Victim Assistance: How It Works](#)
- [IRS Fact Sheet 2016-4: How New Identity Security Changes May Affect Taxpayers for 2016](#)