

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

may pose as a bank, credit card company, tax software provider or government agency.

Feb. 04, 2016



The Internal Revenue Service is warning 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

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

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.

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us