Phishing and Other Schemes Using the IRS Name

The IRS periodically alerts taxpayers to schemes that fraudulently use the IRS name, logo or Web site clone to gain access to consumers' financial information in order to steal their identity and assets.

The scams may take place through e-mail, fax or phone. When they take place via e-mail, they are called "phishing" scams. The IRS website has information that can help you protect yourself from tax scams of all kinds. Search the site using the term: phishing.

The following is a list of recent schemes:

IR-2016-145 The IRS issues an urgent alert to tax professionals who use IRS e-services to beware of an email asking them to update their accounts and directing them to a fake website.

IR-2016-123 IRS and its Security Summit partners alert taxpayers to be on guard against fake emails purporting to contain an IRS tax bill related to the Affordable Care Act. Generally, the scam involves an email that includes a fraudulent version of CP2000 notices for tax year 2015 as an attachment.

IR-2016-99 The IRS has seen an increase in "robo-calls" where scammers leave urgent callback requests through the phone telling taxpayers to call back to settle their "tax bill." These fake calls generally claim to be the last warning before legal action is taken. In the latest trend, IRS impersonators are demanding payments on iTunes and other gift cards. The IRS reminds taxpayers that any request to settle a tax bill by putting money on any form of gift card is a clear indication of a scam.

IR-2016-81 IRS warns taxpayers about bogus phone calls from IRS impersonators demanding payment for a non-existent tax, the "Federal Student Tax." Scammers try to convince people to wire money immediately to the scammer. If the victim does not fall quickly enough for this fake "federal student tax", the scammer threatens to report the student to the police.

IR-2016-55 IRS warns taxpayers of a phishing scam targeting Washington D.C., Maryland and Virginia residents where the email scammers are citing tax fraud and trying to trick victims into verifying "the last four digits of their social security number" by clicking on a link provided. As a further attempt to trick residents of the Capital region, the email scam even suggests that information from recent data breaches across the nation may be involved.

IR-2016-40 This variation tries to play off the current tax season. Scammers call saying they have your tax return, and they just need to verify a few details to process your return. The scam tries to get you to give up personal information such as a Social Security number or personal financial information, such as bank numbers or credit cards.

Don't fall victim to tax scams. Remember — if it sounds too good to be true, it probably is.

Additional IRS scam-related information:

- IR-2016-89, IRS Warns Consumers of Possible Scams Relating to Orlando Mass Shooting
- IRS Summertime Tax Tip 2016-01, IRS Says be Alert for Tax Scams
- Special Edition Tax Tip 2016-05, Don't be Fooled; IRS Scams Continue to Pose Serious Threat
- Special Edition Tax Tip 2016-03, IRS Releases Dirty Dozen Scam List: Don't be a Victim
- Tax Tip 2016-19, Scam Calls and Emails Using IRS as Bait Persist
- IR-2016-14, Phone Scams Continue to be a Serious Threat, Remain on IRS "Dirty Dozen" List of Tax Scams for the 2016 Filing Season

See Suspicious e-Mails and Identity Theft.