

**INTERNAL REVENUE SERVICE  
WARNING TO TAYPAYERS**

**NEW EMAIL SCAMS**

A new scam targeting taxpayers are emails telling taxpayers that the IRS has calculated their “fiscal activity” and that they are eligible to receive a tax refund, but not providing a specific dollar amount. In the email taxpayers receive a form to complete, or are sent to a web site titled “Get Your Tax Refund” that copies the appearance of the genuine IRS page titled “Where’s My Refund?” from the IRS website. Just like the genuine IRS website page, taxpayers are asked to enter their Social Security Number and Tax Return filing status. However the phony web page asks taxpayers to enter their credit card account numbers. Note from the IRS, they will never request information through an email. If you email them first, they may respond with an email. The IRS does not initiate contact with taxpayers through email, only through written correspondence.

Another recent scam being reported by the IRS is a phishing scam. Taxpayers receive an email claiming to be from the IRS advising taxpayers they can receive \$80 by filling out an online customer satisfaction survey. The IRS urges taxpayers to ignore this solicitation and not provide any requested information. Again, the IRS does not initiate contact with taxpayers through email.

This next scam, taxpayers again receive an email. This time claiming to be from the IRS “Fraud Investigation Department”. The recipient of the email is asked to complete an “investigation form” through a link provided in the email. It is believed that clicking on the link may activate a Trojan Horse. A Trojan Horse can take over a person’s computer hard drive and allow someone to have remote access to the computer.

The latest version of an email scam intended to fool people into believing they are under investigation by the agency’s Criminal Investigation division. It appears to be aimed at business taxpayers as well as individual taxpayers. The email falsely states that the person is under a criminal probe for submitting a false tax return to the California Franchise Tax Board. The email tries to entice the recipient to click on a link or open an attachment to learn more information about the complaint being made against them. Just like the previous situation, the link or attachment may be a Trojan Horse. A different version of this email will notify the taxpayer that the IRS can act an arbitrator.

The IRS warns there are several versions of these emails being distributed. Some entice the taxpayers to click their way to a fake IRS Web site and ask for bank account numbers. Another states that the IRS is “holding” a refund for them and asks for financial information. Still another email claims the IRS’s “anti-fraud commission” is investigating their tax returns.

Always remember the IRS does not send out unsolicited emails or ask for detailed personal and financial information. Additionally, the IRS never asks people for the PIN numbers, passwords for similar secret access information for their credit card, bank or other financial accounts.

If you or someone you know is a recipient of a questionable email claiming to come from the IRS, do not click on any attachments or links, and do not respond to the email. Instead, forward the email to [phishing@irs.gov](mailto:phishing@irs.gov) and follow the instructions for reporting it.