

## IRS Warns Taxpayers of New E-mail Scams

WASHINGTON — The Internal Revenue Service today alerted taxpayers to the latest versions of an e-mail scam intended to fool people into believing they are under investigation by the agency's Criminal Investigation division.

The e-mail purporting to be from IRS Criminal Investigation falsely states that the person is under a criminal probe for submitting a false tax return to the California Franchise Board. The e-mail seeks to entice people to click on a link or open an attachment to learn more information about the complaint against them. The IRS warned people that the e-mail link and attachment is a Trojan Horse that can take over the person's computer hard drive and allow someone to have remote access to the computer.

The IRS urged people not to click the link in the e-mail or open the attachment.

Similar e-mail variations suggest a customer has filed a complaint against a company and the IRS can act as an arbitrator. The latest versions appear aimed at business taxpayers as well as individual taxpayers.

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

"Everyone should beware of these scam artists," said Kevin M. Brown, Acting IRS Commissioner. "Always exercise caution when you receive unsolicited e-mails or e-mails from senders you don't know."

Recipients of questionable e-mails claiming to come from the IRS should not open any attachments or click on any links contained in the e-mails. Instead, they should forward the e-mails to [phishing@irs.gov](mailto:phishing@irs.gov) (the instructions may be found on IRS.gov by entering the term "phishing" in the search box).

The IRS also sees other e-mail scams that involve tricking victims into revealing private personal and financial information over the Internet is known as "phishing" for information.

The IRS and the Treasury Inspector General for Tax Administration work with the U.S. Computer Emergency Readiness Team (US-CERT) and various Internet service providers and international CERT teams to have the phishing sites taken offline as soon as they are reported.

Since the establishment of the mail box last year, the IRS has received more than 17,700 e-mails from taxpayers reporting more than 240 separate phishing incidents. To date, investigations by TIGTA have identified host sites in at least 27 different countries, as well as in the United States.

Other fraudulent e-mail scams try to entice taxpayers to click their way to a fake IRS Web site and ask for bank account numbers. Another widespread e-mail tells taxpayers the IRS is holding

a refund (often \$63.80) for them and seeks financial account information. Still another email claims the IRS's 'anti-fraud commission' is investigating their tax returns.

**Related items:**

- [Suspicious e-Mails and Identity Theft](#)