

IRS Warns of New e-Mail Scam Offering Cash for Participation in “Member Satisfaction Survey”

WASHINGTON — The Internal Revenue Service today issued a consumer alert regarding a new, two-step e-mail scam that falsely promises recipients they will receive \$80 for participating in an online customer satisfaction survey.

In the scam, an unsuspecting taxpayer receives an unsolicited e-mail that appears to come from the IRS. The e-mail contains a URL linking to an online “Member Satisfaction Survey.”

“We have seen many e-mail scams using the IRS name,” IRS Deputy Commissioner for Operations Support Linda Stiff said. “The IRS does not initiate contact with taxpayers through e-mail. Taxpayers should always use caution when they receive unsolicited e-mails.”

In this case, the e-mail notifies the recipient that he or she has been randomly selected to participate in a survey. In return, the IRS will credit \$80 to the taxpayer’s account. There are references to the IRS in the “from” line and the “subject” line of the e-mail. The link to the survey and a copyright statement at the bottom of the e-mail also reference the IRS. The survey form features the IRS logo.

In addition to standard customer satisfaction survey questions, the survey requests the name and phone number of the participant and also asks for credit card information. Once the fraudsters have a name and phone number, they will presumably call the participant and attempt to retrieve other financial information.

The apparent objectives of this scam are to use the participant’s name and financial data to withdraw funds from the taxpayer’s bank account, run up charges on a credit card or take out loans in the taxpayer’s name.

Tricking victims into revealing private personal and financial information over the Internet, telephone or other means is a practice known as “phishing.”

IRS Never Sends Unsolicited e-Mail

Taxpayers should be aware that the IRS does not send unsolicited e-mail. Additionally, the IRS never asks taxpayers for PIN numbers, passwords or similar secret access information for credit card, bank or other financial accounts.

Recipients of questionable e-mail that appears to come from the IRS should not open any attachments or click on any links contained in the e-mail. Instead, the e-mail should be forwarded to phishing@irs.gov.

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 30,000 e-mails from taxpayers reporting almost 400 separate phishing incidents. To date, investigations by TIGTA have identified host sites in at least 55 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 scam tells taxpayers the IRS is holding a refund for them — frequently \$63.80 — and seeking financial account information. Still another email claims the IRS’s “anti-fraud commission” is investigating their tax returns.

More information on phishing scams using the IRS name, logo or other identifier can be found on the only genuine IRS Web site, IRS.gov, either at IRS Warns Taxpayers of New E-mail Scams <http://www.irs.gov/newsroom/article/0,,id=170894,00.html> or Suspicious e-Mails and Identity Theft <http://www.irs.gov/newsroom/article/0,,id=155682,00.html> .