

IRS Warns of New E-Mail and Telephone Scams Using the IRS Name; Advance Payment Scams Starting

IR-2008-11, Jan. 30, 2008

WASHINGTON — The Internal Revenue Service today warned taxpayers to beware of several current e-mail and telephone scams that use the IRS name as a lure. The IRS expects such scams to continue through the end of tax return filing season and beyond.

The IRS cautioned taxpayers to be on the lookout for scams involving proposed advance payment checks. Although the government has not yet enacted an economic stimulus package in which the IRS would provide advance payments, known informally as rebates to many Americans, a scam which uses the proposed rebates as bait has already cropped up.

The goal of the scams is to trick people into revealing personal and financial information, such as Social Security, bank account or credit card numbers, which the scammers can use to commit identity theft.

Typically, identity thieves use a victim's personal and financial data to empty the victim's financial accounts, run up charges on the victim's existing credit cards, apply for new loans, credit cards, services or benefits in the victim's name, file fraudulent tax returns or even commit crimes. Most of these fraudulent activities can be committed electronically from a remote location, including overseas. Committing these activities in cyberspace allows scamsters to act quickly and cover their tracks before the victim becomes aware of the theft.

People whose identities have been stolen can spend months or years — and their hard-earned money — cleaning up the mess thieves have made of their reputations and credit records. In the meantime, victims may lose job opportunities, may be refused loans, education, housing or cars, or even get arrested for crimes they didn't commit.

The most recent scams brought to IRS attention are described below.

Rebate Phone Call

At least one scheme using the word "rebate" as part of the lure has been identified. In that scam, consumers receive a phone call from someone identifying himself as an IRS employee. The caller tells the targeted victim that he is eligible for a sizable rebate for filing his taxes early. The caller then states that he needs the target's bank account information for the direct deposit of the rebate. If the target refuses, he is told that he cannot receive the rebate.

This phone call is a scam. No legislation has yet been enacted that would allow the IRS to provide advance payments to taxpayers or that determines the details of those payments. Moreover, the IRS does not force taxpayers to use direct deposit. Those who opt for direct deposit do so by completing the appropriate section of their tax return, with bank routing and account information, when they file; the IRS does not gather the information by telephone.

Refund e-Mail

The IRS has seen several variations of a refund-related bogus e-mail which falsely claims to come from the IRS, tells the recipient that he or she is eligible for a tax refund for a specific amount, and instructs the recipient to click on a link in the e-mail to access a refund claim form. The form asks the recipient to enter personal information that the scamsters can then use to access the e-mail recipient's bank or credit card account.

In a new wrinkle, the current version of the refund scam includes two paragraphs that appear to be directed toward tax-exempt organizations that distribute funds to other organizations or individuals. The e-mail contains the name and supposed signature of the Director of the IRS's Exempt Organizations business division.

This e-mail is a phony. The IRS does not send unsolicited e-mail about tax account matters to individual, business, tax-exempt or other taxpayers.

Filing a tax return is the only way to apply for a tax refund; there is no separate application form. Taxpayers who wish to find out if they are due a refund from their last annual tax return filing may use the "[Where's My Refund?](#)" interactive application on this Web site, IRS.gov. The only official IRS Web site is located here at www.irs.gov.

Audit e-Mail

Another new scam brought to IRS attention contains features not seen before by the IRS. Using a technique calculated to get almost anyone's attention, the e-mail notifies the recipient that his or her tax return will be audited. This is the first scam of which the IRS is aware that uses this to get the victim to respond.

Unusual for a scam e-mail, it may contain a salutation in the body addressed to the specific recipient by name. Most scam e-mails seen by the IRS are sent using the same technique used by spammers, in which hundreds of thousands of messages are sent to potential victims based on Internet address. Because of the volume, the typical scam e-mail is not personalized.

This e-mail instructs the recipient to click on links to complete forms with personal and account information, which the scammers will use to commit identity theft.

This e-mail is a phony. The IRS does not send unsolicited, tax-account related e-mails to taxpayers.

Changes to Tax Law e-Mail

This bogus e-mail is addressed to businesses, accountants and "Treasury" managers. It instructs them to download information on tax law changes by clicking on a series of links to publications on businesses, estate taxes, excise taxes, exempt organizations and IRAs and other retirement plans. The IRS believes that clicking on a link downloads malware onto the recipient's computer. Malware is malicious code that can take over the victim's computer hard drive, giving someone remote access to the computer, or it could look for passwords and other information and send them to the scamster. There are other types of malware, as well.

The urls contained in the link are not legitimate IRS Web addresses. All IRS.gov Web page addresses begin with <http://www.irs.gov/>.

Paper Check Phone Call

In a current telephone scam, a caller claims to be an IRS employee who is calling because the IRS sent a check to the individual being called. The caller states that because the check has not been cashed, the IRS wants to verify the individual's bank account number. The caller may have a foreign accent.

In reality, the IRS leaves it entirely up to the individual to choose to cash or not cash a paper check. The IRS has no business need to know, and does not ask for, bank account or similar

information, except when taxpayers indicate on their tax return that they are opting for the direct electronic deposit of their refund. In that case, however, it is the individual's responsibility to provide the IRS with the correct bank routing and account numbers on the tax return; the IRS does not contact taxpayers to verify the information.

What to Do

Anyone wishing to access the IRS Web site should initiate contact by typing the IRS.gov address into their Internet address window, rather than clicking on a link in an e-mail or opening an attachment.

Those who have received a questionable e-mail claiming to come from the IRS may forward it to a mailbox the IRS has established to receive such e-mails, phishing@irs.gov, using instructions contained in an article titled "[How to Protect Yourself from Suspicious E-Mails or Phishing Schemes](#)." Following the instructions will help the IRS track the suspicious e-mail to its origins and shut down the scam. Find the article by visiting IRS.gov and entering the words "suspicious e-mails" into the search box in the upper right corner of the front page.

Those who have received a questionable telephone call that claims to come from the IRS may also use the phishing@irs.gov mailbox to notify the IRS of the scam.

The IRS has issued previous warnings on scams that use the IRS to lure victims into believing the scam is legitimate. More information on identity theft, phishing and telephone scams using the IRS name, logo or spoofed (copied) Web site is available on this Web site. Enter the terms "phishing," "identity theft" or "e-mail scams" into the search box in the upper right corner of the front page.