INTERNAL REVENUE SERVICE
IRS News Release

Media Relations Office | Washington, D.C. | Media Contact: 202.622.4000
www.IRS.gov/newsroom | Public Contact: 800.829.1040

Scammers Use e-Mail, Fax to Pose as IRS

IR-2008-88, July 10, 2008

WASHINGTON — The Internal Revenue Service cautions taxpayers to be on the lookout for a new wave of scams using the IRS name in identity theft e-mails, or phishing, that have circulated during the last two months.

In May and June alone, taxpayers reported almost 700 separate phishing incidents to the IRS. In 2008 so far, taxpayers have reported about 1,600 phishing incidents to the IRS.

“Taxpayers should take steps to keep their personal information out of the hands of identity thieves,” said IRS Commissioner Doug Shulman. “That includes not falling for any of the phony e-mails or faxes now in circulation pretending to come from the IRS.”

The most common scams involve tax refunds and, this year, economic stimulus payments.

Although most of these scams consist of e-mails requesting detailed personal information, the IRS generally does not send e-mails to taxpayers, does not discuss tax account matters with taxpayers in e-mails, and does not request security-related personal information, such as PIN numbers, from taxpayers.

Refund e-Mail Scam

There are several variations of the refund scam, in which an e-mail claiming to come from the IRS falsely informs the recipient that he or she is eligible for a tax refund for a specific amount. The bogus e-mail instructs the recipient to click on a link to access a refund claim form. The form requests personal information that the scammers can use to access the e-mail recipient’s bank or credit card account.

This notification is phony. The IRS does not send unsolicited e-mail about tax account matters to 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 the IRS Web site at IRS.gov, the only official IRS Web site.

Economic Stimulus Payments Scam

In this scam, a taxpayer receives an e-mail pretending to come from the IRS which tells the recipient he or she is eligible for an economic stimulus payment. The message recommends

direct deposit into the taxpayer's checking or savings account. To receive the payment, recipients must click on a link to complete and submit an online form by a certain date; otherwise, the e-mail warns, payment may be delayed. The form requests personal and financial data, including checking or savings account numbers that the scammers can use to gain access to the accounts.

In reality, the way members of the public receive their economic stimulus payment is to file a tax return with the IRS, not a special form. Additionally, the IRS does not request personal or financial information via e-mail.

Information on how to obtain an economic stimulus payment may be found in the Economic Stimulus Payment Information Center on the IRS Web site (www.irs.gov). For more information on stimulus-related scams, see IR-2008-11.

Substitute Form 1040 Fax Scam

This scam consists of a cover letter and form that are faxed, rather than e-mailed. The cover letter is addressed "Dear Valued Tax Payer (sic)" and appears to be signed by an IRS employee. The letter says that the IRS is updating its files and that recipients who supply the requested information will receive a nominal tax refund. It also states that those who fail to immediately return the completed form risk additional tax and withholding. The attached form is labeled a substitute Form 1040 and is titled "Certificate of Current Status of Beneficial Owner For United States Tax Recertification & Withholding." It requests a large amount of detailed personal and financial information, such as mother's maiden name (often used in security screening), bank account numbers, estimated assets and more. It asks the recipient to sign and fax back the completed form, as well as a copy of the recipient's driver's license and passport.

The letter, signature and form are all fraudulent. Moreover, the IRS does not send unsolicited faxes to taxpayers and does not request such detailed personal and financial information.

This is a variant of earlier scams. For more information, see news releases IR-2004-104 and IR-2004-75.

Company Report Scam

This e-mail appears to come from an IRS.gov e-mail address, addresses recipients by name and references the company the recipient works for. These personalized details may convince the recipient that the e-mail is legitimate. The e-mail says that the IRS has a report on the company and asks the recipient to review a copy by clicking on a link to download the report. However, when the link is clicked, malware is downloaded to the recipient's computer.

There are various types of malware, which can hijack a victim's computer hard drive to give someone remote access to the computer, search for passwords and other information and send them to the scammer, or cause other types of identity theft or damage.

The IRS does not compile reports on companies or send e-mails to company staff asking them to review a report. Generally, the IRS does not send unsolicited e-mails to taxpayers.

Tax Court Scam

In this scam, an e-mail that appears to come from the U.S. Tax Court contains a petition involving a court case between the IRS and the recipient. The document instructs the recipient to download other files. The downloads transfer malware, or malicious code, to the recipient's computer.

There are various types of malware, which, for example, can hijack a victim's computer hard drive to give someone remote access to the computer, or can search for passwords and other information and send them to the scammer.

The truth is that the Tax Court is not e-mailing notices to anyone who currently has a case before the court. Visit the court's Web site at http://www.ustaxcourt.gov/ for more information. Recipients are advised to avoid clicking on any links in the e-mail and to delete the e-mail.

How Scams Work

To lure their victims, phishing scams use the name of a known institution, such as the IRS, to either offer a reward for taking a simple action, such as providing information, or threaten or imply an unpleasant consequence, such as losing a refund, for failing to take the requested action.

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 scammers 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 or may be refused loans, education, housing or cars.

What to Do

Anyone wishing to access the IRS Web site should type **www.irs.gov** into their Internet address window, rather than clicking on a link in an e-mail or opening an attachment, either of which may download malicious code or send the recipient to a phony Web site.

Those who have received a questionable e-mail claiming to come from the IRS may forward it to the following address: phishing@irs.gov. Use the instructions contained in an article on IRS.gov 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.

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

Related Information:

- FS-2008-9, Identity Theft E-Mails Scams a Growing Problem
- IR-2007-109, IRS Warns Taxpayers of New E-mail Scams
- Suspicious e-Mails and Identity Theft

—30—