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

IRS Warns of Phony e-Mails Claiming to Come from the IRS

IR-2007-75, April 2, 2007

WASHINGTON — The Internal Revenue Service today alerted taxpayers about Internet scams in which fraudulent e-mails are sent that appear to be from the IRS.

The e-mails direct the consumer to a Web link that requests personal and financial information, such as Social Security, bank account or credit card numbers. The practice of tricking victims into revealing private personal and financial information over the Internet is known as “phishing” for information.

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.

The information fraudulently obtained by scammers is used to steal the taxpayer’s identity and then his or her financial assets. Generally, identity thieves use someone’s personal data to steal his or her 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 and even file fraudulent tax returns to obtain refunds rightfully belonging to the victim.

“Don’t be fooled by these shameless scam artists. The IRS doesn’t send unsolicited e-mail,” said IRS Commissioner Mark W. Everson. “Always exercise caution when you receive unsolicited e-mails or e-mails from senders you don’t know, and always verify the source.”

Last year, the IRS established an electronic mail box, phishing@irs.gov, to receive copies of possibly fraudulent e-mails involving misuse of the IRS name, logo or Web site for investigation. Since the establishment of the mail box, the IRS has received more than 17,700 e-mails from taxpayers reporting more than 240 separate phishing incidents. To date, investigations by the Treasury Inspector General for Tax Administration (TIGTA) have identified host sites in at least 27 different countries, as well as in the United States.

In the on-going e-mail schemes that use the IRS name, about which the IRS has warned the public before, the recipients are asked to click on links to take them to the “IRS” Web site. The links appear authentic and connect the victim to sites that resemble the genuine IRS Web site (www.irs.gov). The sites then prompt the victim for personal identifiers, credit card numbers, PIN numbers or similar financial information. The phony sites appear legitimate because most of the images and content are copied from actual pages on the genuine IRS Web site before being modified by the fraudsters to include their loaded questions.

—More—

The schemes have a few variations. In one, the bogus e-mail tells the recipient that he or she is eligible to receive a federal tax refund for a given amount (often $63.80) and sends the recipient to a Web site to complete a form to “submit the tax refund request.” The form then asks for the personal and financial information.

The IRS does not notify taxpayers of refunds via e-mail. Additionally, taxpayers do not have to complete a special form or provide detailed financial information to obtain a refund. Refunds are based on information contained on the federal income tax return filed by the taxpayer.

In another scheme, the e-mail states that the IRS’s “Antifraud Comission” (sic) has found that someone tried to pay their taxes through the Electronic Federal Tax Payment System, or EFTPS, using the e-mail recipient’s credit card and that, as a result, some of the recipient’s money was lost and the remaining “founds” (sic) were blocked. The e-mail contains visual elements copied from the genuine IRS Web site in an attempt to make the e-mail appear legitimate. The e-mail includes a link that sends the recipient to a Web site that asks the recipient to enter personal and financial information, such as SSN and account numbers, in order to unblock their funds.

The IRS does not have an Antifraud Commission, does not have the authority to freeze a taxpayer’s credit card or bank account because of potential theft or fraud perpetrated against the taxpayer, and does not use e-mail to initiate contact with taxpayers.

A third, recent scheme asks the recipient to wire thousands of dollars in order to retrieve the winnings on a lottery. One such e-mail instructed the recipient to wire $42,000 to retrieve the winnings on a British lottery. This e-mail used a simulated IRS letterhead with the actual address of an IRS office at 290 Broadway, Manhattan, NYC, in an attempt to persuade the recipient of the legitimacy of the e-mail.

The IRS does not handle lottery distributions and does not initiate contact with taxpayers via e-mail. Additionally, lottery winnings are generally reported by the winner to the IRS with his or her annual federal income tax return, at which time any taxes due must be paid.

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 (the instructions may be found on IRS.gov by entering the term phishing in the search box) or notify TIGTA’s toll-free hotline at 1-800-366-4484. The IRS and TIGTA 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.

Recently, the IRS has become aware of commercial Internet sites that bear a striking resemblance to the real IRS site or that contain the some form of the IRS name in their address but with a .com, .net, .org or other designation in the address instead of .gov. Though these sites may not be phishing sites — that is, they may not request private financial data in an attempt to steal the consumer’s identity — the IRS urges consumers not to be misled into thinking such sites are the genuine IRS Web site or have some connection to the real IRS.

—More—

The only genuine IRS Web site is IRS.gov.

More information on phishing schemes and others, including abusive tax avoidance transactions, frivolous arguments and more, may be found on the Compliance and Enforcement page at IRS.gov.

—30—