

Suspicious Emails and Identity Theft

Last updated June 13, 2008

WASHINGTON -- The Internal Revenue Service has issued several recent consumer warnings on the fraudulent use of the IRS name or logo by scammers trying to gain access to consumers' financial information in order to steal their identity and assets. When identity theft takes place over the Internet, it is called phishing.

Suspicious e-Mail/Phishing

Phishing (as in "fishing for information" and "hooking" victims) is a scam where Internet fraudsters send e-mail messages to trick unsuspecting victims into revealing personal and financial information that can be used to steal the victims' identity. Current scams include phony e-mails which claim to come from the IRS and which lure the victims into the scam by telling them that they are due a tax refund.

- [IR-2008-11](#), IRS Warns of New E-Mail and Telephone Scams Using the IRS Name; Advance Payment Scams Starting
- [IR-2007-183](#), IRS Warns of E-Mail Scam Soliciting Donations to California Wildfire Victims
- [IR-2007-148](#), IRS Warns of New E-mail Scam Offering Cash for Participation in "Member Satisfaction Survey"
- [IR-2007-109](#), IRS Warns Taxpayers of New E-mail Scams
- [IR-2007-75](#), IRS Warns of Phony e-Mails Claiming to Come from the IRS
- [IR-2006-116](#), Electronic Federal Tax Payment System Cited in New E-mail Scam
- [IR-2006-104](#), IRS Renews E-mail Alert Following New Scams
- [IR-2006-49](#), IRS Establishes e-Mail Box for Taxpayers to Report Phony e-Mails
- [Sample of a suspicious/phishing e-mail](#)
- [Is it a phishing Web site?](#)
- [How to Protect Yourself from Suspicious E-Mails or Phishing Schemes](#)

The good news is that you can help shut down these schemes and prevent others from being victimized. If you receive a suspicious e-mail that claims to come from the IRS, you can relay that e-mail to a new IRS mailbox, phishing@irs.gov. Follow instructions in the link below for sending the bogus e-mail to ensure that it retains critical elements found in the original e-mail. The IRS can use the information, URLs and links in the suspicious e-mails you send to trace the hosting Web site and alert authorities to help shut down the fraudulent sites. Unfortunately, due to the expected volume, the IRS will not be able to acknowledge receipt or respond to you.

- phishing@irs.gov
- [Instructions for submitting phishing e-mails to IRS](#)
- [IR-2006-49](#), IRS Establishes e-Mail Box for Taxpayers to Report Phony e-Mails

Identity Theft

Identity theft can be committed through e-mail (phishing) or other means, such as regular mail, fax or telephone, or even by going through someone's trash.

Identity theft occurs when someone uses your personal information such as your name, Social Security number or other identifying information without your permission to commit fraud or other crimes. Typically, identity thieves use someone's personal 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. 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 good name and credit record. In the meantime, victims may lose job opportunities, be refused loans, education, housing or cars, or even get arrested for crimes they didn't commit.

- [Identity Theft Companion Learning Guide](#) , What Law Enforcement is Doing to Stop the Thieves
- [Identity Theft and Your Tax Records](#)
- [Social Security announces public warning of identity theft e-mail scam](#)

Recent Schemes

When the IRS learns about schemes involving use of the IRS name, it tries to alert consumers as well as authorities that can shut down the scheme, if possible. The most recent schemes are listed below.

- In a new scam, both a form and cover letter, supposedly from the IRS, are faxed to people with instructions to fax the completed form back to the number contained in the form. The letter says that the IRS requires an update of the recipient's tax information and promises to deposit a nominal tax refund to the recipient's bank account in return. The form is a "substitute and recertification" Form 1040, titled "Certificate of Current Status of Beneficial Owner For United States Tax Recertification & Withholding." The form requests detailed personal and financial information, such as mother's maiden name and bank account and PIN numbers, that can be used to steal the identity and access the bank accounts of anyone who responds to this scam. In reality, there is no such form and the IRS does not ask taxpayers to provide the type of information specified on the form. [Added June 13, 2008.]
- Some people have received phone calls about the economic stimulus payments, in which the caller impersonates an IRS employee. The caller asks the taxpayer for their Social Security and bank account numbers, claiming that the IRS needs the information to complete the processing of the taxpayer's stimulus payment. In reality, the IRS uses the information contained on the taxpayer's tax return to process stimulus payments, rather than contacting taxpayers by phone or e-mail. [Added April 21, 2008.]

- An e-mail claiming to come from the IRS about the "2008 Economic Stimulus Refund" tell recipients to click on a link to fill out a form, apparently for direct deposit of the payment into their bank account. This appears to be an identity theft scheme to obtain recipients' personal and financial information so the scammers can clean out their victims' financial accounts. In reality, taxpayers do not have to fill out a separate form to get a stimulus payment or have it directly deposited; all they had to do was file a tax return and include direct deposit information on the return. [Added April 21, 2008.]
- A scheme in which a tax refund form is e-mailed, supposedly by the Taxpayer Advocate Service (a genuine and independent organization within the IRS which assists taxpayers with unresolved problems), is particularly blatant in the amount and type of information it requests. The top of the form tells the recipient that they are eligible for a tax refund for a specified amount. The form asks for name, address and phone number and a substantial amount of financial information, such as bank account number, credit card number and expiration date, ATM PIN number and more. It also asks for mother's maiden name (frequently used by many people as an account security password). At the bottom is a phony name and signature, claiming to be that of the Taxpayer Advocate. The implication is that the taxpayer must fill in and submit the form to receive a tax refund. In reality, taxpayers claim their tax refunds through the filing of an annual tax return, not a separate application form. [Added April 9, 2008.]
- A new variation of the refund scheme (see items below) is directed toward organizations that distribute funds to other organizations or individuals. In an attempt to seem legitimate, the scam e-mail claims to be sent by, and contains the name and supposed signature of, the Director of the IRS Exempt Organizations area of the IRS. The e-mail asks recipients to click on a link to access a form for a tax refund. In reality, taxpayers claim their tax refunds through the filing of an annual tax return, not a separate application form.
- In a variation, an e-mail scam claims to come from the IRS and the Taxpayer Advocate Service (a genuine and independent organization within the IRS whose employees assist taxpayers with unresolved tax problems). The e-mail says that the recipient is eligible for a tax refund and directs the recipient to click on a link that leads to a fake IRS Web site.
- A scam e-mail that appears to be a solicitation from the IRS and the U.S. government for charitable contributions to victims of the recent Southern California wildfires has been making the rounds. A link in the e-mail, when clicked, sends the e-mail recipients to a Web site that looks like the IRS Web site, but isn't. They are then directed to click on a link that opens a donation form that asks for personal and financial information. The scammers can use that information to gain access to the e-mail recipients' financial accounts.

- A recent e-mail scam tells taxpayers that the IRS has calculated their "fiscal activity" and that they are eligible to receive a tax refund of a certain amount. Taxpayers receive a page of, or are sent to, a Web site (titled "Get Your Tax Refund!") that copies the appearance of the genuine "Where's My Refund?" interactive page on the genuine IRS Web site. Like the real "Where's My Refund?" page, taxpayers are asked to enter their SSNs and filing status. However, the phony Web page asks taxpayers to enter their credit card account numbers instead of the exact amount of refund as shown on their tax return, as the real "Where's My Refund?" page does.
- In a new phishing scam, an e-mail purporting to come from the IRS advises taxpayers they can receive \$80 by filling out an online customer satisfaction survey. 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.
- In another recent scam, consumers have received a "Tax Avoidance Investigation" e-mail claiming to come from the IRS' "Fraud Department" in which the recipient is asked to complete an "investigation form," for which there is a link contained in the e-mail, because of possible fraud that the recipient committed. It is believed that clicking on the link may activate a Trojan Horse.
- An e-mail scheme claiming to come from the IRS's Criminal Investigation division tells the recipient that they are 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 e-mail link and attachment contain a Trojan Horse that can take over the person's computer hard drive and allow someone to have remote access to the computer.
- Another scheme suggests that a customer has filed a complaint against a company, of which the e-mail recipient is a member, and that the IRS can act as an arbitrator. This appears to be aimed at business as well as individual taxpayers.
- One e-mail scam, fraught with grammatical errors and typos, looks like a page from the IRS Web site and claims to be from the "IRS Antifraud Commission" (sic), a fictitious group. The e-mail claims someone has enrolled the taxpayer's credit card in EFTPS and has tried to pay taxes with it. The e-mail also says there have been fraud attempts involving the taxpayer's bank account. The e-mail claims money was lost and "remaining funds" (sic) are blocked. Recipients are asked to click on a link that will help them recover their funds, but the subsequent site asks for personal information that the thieves could use to steal the taxpayer's identity.
- E-mails claiming to come from tax-refunds@irs.gov, admin@irs.gov and similar variations told the recipients that they were eligible to receive a tax refund for a given amount. It directed recipients to claim the refund by using a link contained in the e-mail which sent the recipient to a Web site. The site, a copy of the IRS Web site, displayed an interactive page similar to a genuine IRS one; however, it had been

modified to ask for personal and financial information that the genuine IRS interactive page does not require.

The Treasury Inspector General for Tax Administration (TIGTA) has found numerous separate Web sites in at least 20 different countries hosting variations on this scheme.

- A bogus IRS letter and Form W-8BEN (Certificate of Foreign Status of Beneficial Owner for United States Tax Withholding) asked non-residents to provide personal information such as account numbers, PINs, mother's maiden name and passport number. The legitimate IRS Form W-8BEN, which is used by financial institutions to establish appropriate tax withholding for foreign individuals, does not ask for any of this information.

For more information on the various schemes, see the following:

- [IR-2007-37](#), Fraudulent Telephone Tax Refunds, Abusive Roth IRAs Top Off 2007 "Dirty Dozen" Tax Scams
- [IR-2005-136](#), IRS Warns of e-Mail Scam About Tax Refunds
- [TIGTA Computer Security Bulletin](#)
- [TIGTA Report on Phishing](#)
- [Alert on QI Identity Theft](#)

To Report Fraud

For other than phishing schemes, you may report the fraudulent misuse of the IRS name, logo, forms or other IRS property by calling the TIGTA toll-free hotline at 1-800-366-4484 or visiting the [TIGTA Web site](#).

Other Federal Resources

For more information on understanding and preventing identity theft and suspicious e-mails (phishing), or dealing with their aftermath, check out the following federal resources:

- [Department of the Treasury's identity theft resource page](#)
- Federal Trade Commission's (FTC) [consumer Web site](#)
- FTC's [OnGuardOnLine](#) Web site
- [Firstgov](#)
- [Social Security Administration \(SSA\)](#)

Source: [Internal Revenue Service Website](#)