NAEA
NATIONAL ASSOCIATION OF ENROLLED AGENTS
POWERING AMERICA'S TAX EXPERTS®

Taxpayer Alert: How to Recognize and Avoid Identity Theft Scams

Across the nation, identity thieves are using legitimate information to scam honest taxpayers, and frequently posing as the IRS to do so. The IRS is taking this seriously, and has created the IRS Identity Theft Protection Unit to address the growing problem. Being aware of some of the most common scams can help protect you from having your personal information used to commit fraud or other crimes.

Phony IRS emails. In a "phishing" scam, an official-looking email shows an IRS logo that lures the consumer to a website that requests personal and financial information, such as a Social Security number, bank account, or credit card numbers. In truth, the IRS does not send out unsolicited e-mails, and does not use email to ask for detailed personal or financial information such as PIN numbers, passwords or similar secret access information for credit cards or bank accounts. The IRS does not initiate contact with taxpayer via email. The only genuine IRS website is www.IRS.gov.

Refund scam. In a refund scam, a 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 website to complete a form to submit the tax refund request. The form then asks for personal and financial information. In fact, the IRS does not notify taxpayers of refunds via e-mail. And, taxpayers do not have to complete a special form or provide detailed financial information to obtain a refund. Refunds are based on information reported on the tax return.

Antifraud Commission scam. In this case, the scammer sends an e-mail stating the IRS "Antifraud Commission" 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, as a result, some of the recipient's money was lost and the remaining funds were blocked. The e-mail includes a link that sends the recipient to a website where he or she is directed to enter personal and financial information in order to unblock their funds. Don't take the bait! The IRS does not have an Antifraud Commission and 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.

Other email scams from fraudsters posing as IRS personnel include notifications of lottery winnings, a notice that more than one return was filed by the taxpayer, and notification of W-2s received from an unknown employer. Scams can also take the form of "assisting" taxpayers in filing returns to collect fraudulent refunds, promotion of tax evasion techniques, or reporting false income for purposes of increasing refundable credits.

A taxpayer who believes there is a risk of identity theft due to lost or stolen personal information should contact the IRS immediately so the agency can take action to secure his or her tax account. The taxpayer should contact the IRS Identity Protection Specialized Unit at 800.908.4490.

Get help. A taxpayer who believes they may have received a fraudulent or otherwise questionable communication related to taxes should contact a licensed tax professional. Enrolled agents (EAs) are America's tax experts. They are the only federally-licensed tax practitioners who specialize in taxation and also have *unlimited* rights to represent taxpayers before the IRS. That means that if you get a letter from the IRS, or worse, are audited or are the target of a collection action, your EA can speak directly to the IRS on your behalf. Find an EA in your area on the directory at www.naea.org.