



February 22, 2012

Annual Top Twelve Tax Scams part 1

Every year, the IRS releases the top twelve tax scams, dubbed the “Dirty Dozen” to warn taxpayers of these schemes designed to steal money from unsuspecting victims in various ways. While anyone may encounter any of these scams anytime, it is during tax season that most of these schemes are prevalent. IRS Commissioner Doug Shulman commented, “Taxpayers should be careful and avoid falling into a trap with the Dirty Dozen. Scam artists will tempt people in-person, on-line and by e-mail with misleading promises about lost refunds and free money. Don’t be fooled by these scams.”

Here are the top twelve tax scams for this year.

1. Identity theft

Not surprisingly, identity theft has topped the list this year. The number of cases of identity theft has been on the rise of late. Last year, the IRS managed to prevent more than \$1.4 billion of taxpayer funds from getting into the wrong hands due to identity theft.

In light of this, the IRS has stepped up legal enforcement to punish those convicted of identity theft. In addition, the agency has also beefed up its security measures aimed at detecting fraudulent tax submissions and refund claims. The IRS now employs a comprehensive screening process to prevent, detect and resolve identity theft incidents.

Learn to spot the tell-tale signs that your identity may have been stolen. If you receive notice from the IRS that your tax return has already been submitted or that you have received wages from an unrecognized employer, these may indicate that your personal particulars have been compromised. If you feel your personal information has been stolen and used for fraudulent tax purposes, contact the IRS Identity Protection Specialized Unit. For more information, visit the special identity theft page at www.irs.gov/identitytheft.

2. Phishing

Phishing is where a scammer tries to obtain your personal details such as Social Security number and financial details like bank or credit card numbers through email. It is often linked with a false website cloned to look like the IRS website. An email may inform you that you are due for a refund from the IRS

and request that you furnish your bank account number for a direct deposit. The email usually looks genuine with the IRS logo and may link to a website that claims to be the IRS website or another associated with it.

If you respond to the email by providing the financial information requested or if you click on any link in the email, it would result in your money being transferred out of your bank account or a virus being sent to your computer.

If you receive an email purportedly from the IRS, do not respond to it. The IRS never communicates with you through email. You should immediately forward the email to the IRS at phishing@irs.gov and then delete it without clicking any link therein.

We shall continue with more of the IRS' Dirty Dozen tax scams tomorrow. Stay tuned.