THE LAW OFFICES OF
DARRIN T. MISH, PA
TAX ATTORNEYS FOR YOUR MOST SERIOUS IRS PROBLEMS

IRS PROBLEM SOLVER BLOG
Experienced, Nationally Recognized Tax Attorneys for your Most Serious IRS Problems

February 19, 2011

Email Scam Warning from IRS

When tax season comes around you will almost always find email scams. If you have received an email that looks like it is from the IRS, do not believe it. It's a scam. The IRS will never email you about your taxes, whether it's for your business tax or personal tax.

Most email scams are phishing scams, aimed at getting your personal particulars such as bank account numbers, Social Security numbers and other personal details so that the scammers can gain access to your funds.

Some email messages say that you are due for a refund and require you to click a button or link and fill out a refund form. The IRS does not issue refund forms. Another form or email scam tells you that your payment did not go through and they require your bank account number.

These days, email scams have become so sophisticated that scammers can access your information once you click on a link, even if you did not disclose your personal details. So do not click any link or open any attachment in an email. Sometimes, doing so may expose your computer to viruses and malware or other malicious programs that allow them to steal information right off the computer. You might not intentionally give them information, but they can take it anyway.

In fact, a link or an attachment in an email supposedly from the IRS is a tell-tale sign of email scams. The links generally lead you to a website that masquerades as the IRS website. Remember the only URL that leads to the genuine IRS site is www.irs.gov, nothing else.

Here are other tell-tale signs of an email scam:

• The email gets the name of the IRS or other federal agency names wrong

• The message threatens some consequence if you do not do what it says, such as tax penalties or additional taxes

• There is an incentive for you to respond to the email such as a tax refund or a monetary reward

• Asks for security-related information like your mother's maiden name either in the email itself or in the website the link in the email sends you to.

• The message contains grammar and spelling errors. Many such scams originate from overseas in non-native English speaking countries.

• The email contains a really long URL in any link or one that does not start with www.irs.gov. Sometimes the link may not contain the actual URL, so to see the actual URL, hover your mouse over the link without clicking it and look at the status bar at the lower part of your computer screen. The URL should appear.