



March 14, 2011

## IRS Imposters Abound at Tax Time

Tax season is always the time when tax scammers increase their activities.

Although the warning has been given many times before, it does no harm to repeat it. Do not respond to emails that come in the name of the IRS. The IRS will never send you an email for any reason the least of which is to ask for personal details such as your bank account, credit card or Social Security numbers. These are different forms of phishing scams.

Every year, the IRS is inundated with reports from taxpayers who receive emails, phone calls or other forms of communication supposedly from the IRS. If you offer your personal details in response to such notices, you will fall victim to identity theft or have your money stolen electronically.

Bill Bunson, a spokesman for the IRS said, "The majority (of phishing scams) arrive as an e-mail, and they're going to claim to be from the IRS, and they're going to want personal and financial information that the IRS already has or can obtain."

The way the IRS communicates with you is by mail or through a phone call. Furthermore, the IRS will never ask you for your detailed personal or financial information such as your account passwords, PIN numbers or

other such access information to your accounts.

You should also never respond to any email that comes supposedly from the IRS, open any attachment or click any link in such emails. Clicking on links may expose your computer to viruses or malware. According to Bunson, about half of the email phishing scams come from overseas.

In addition, you should reject any website that claims to be the IRS but does not end with a .gov but instead may end with .com, .info, .net or .org. If you come across such a website, report it to the IRS. The correct IRS website is [www.irs.gov](http://www.irs.gov). You should visit the IRS website for more information on phishing scams and identity theft.

If you become suspicious of any form of communication purportedly from the IRS, you can call the IRS at 1-800-829-1040 to verify it.