Don’t be Scammed by Cyber Criminals

IRS TAX TIP 2012-08, January 12, 2012

The Internal Revenue Service receives thousands of reports each year from taxpayers who receive suspicious emails, phone calls, faxes or notices claiming to be from the IRS. Many of these scams fraudulently use the IRS name or logo as a lure to make the communication appear more authentic and enticing. The goal of these scams – known as phishing – is to trick you into revealing your personal and financial information. The scammers can then use your information – like your Social Security number, bank account or credit card numbers – to commit identity theft or steal your money.

Here are five things the IRS wants you to know about phishing scams.

1. The IRS never asks for detailed personal and financial information like PIN numbers, passwords or similar secret access information for credit card, bank or other financial accounts.

2. The IRS does not initiate contact with taxpayers by email to request personal or financial information. If you receive an e-mail from someone claiming to be the IRS or directing you to an IRS site:

   • Do not reply to the message.
   • Do not open any attachments. Attachments may contain malicious code that will infect your computer.
   • Do not click on any links. If you clicked on links in a suspicious e-mail or phishing website and entered confidential information, visit the IRS website and enter the search term 'identity theft' for more information and resources to help.

3. The address of the official IRS website is www.irs.gov. Do not be confused or misled by sites claiming to be the IRS but ending in .com, .net, .org or other designations instead of .gov. If you discover a website that claims to be the IRS but you suspect it is bogus, do not provide any personal information on the suspicious site and report it to the IRS.

4. If you receive a phone call, fax or letter in the mail from an individual claiming to be from the IRS but you suspect they are not an IRS employee, contact the IRS at 1-800-829-1040 to determine if the IRS has a legitimate need to contact you. Report any bogus correspondence. You can forward a suspicious email to phishing@irs.gov.

5. You can help shut down these schemes and prevent others from being victimized. Details on how to report specific types of scams and what to do if you’ve been victimized are available at www.irs.gov. Click on "phishing" on the home page.