

# *Sy Accountancy Corporation*

Member, American Institute of CPAs  
704 Mira Monte Place, Pasadena, California 91101  
Tel (626) 744-0200 ▪ Fax (626) 744-0300 ▪ vsy@victorsycpa.com

## **IRS WARNS PUBLIC OF SUSPICIOUS EMAILS**

By Victor Sy, CPA

There are many e-mail scams circulating that fraudulently use the Internal Revenue Service name or logo as a lure. The goal of the scam – known as phishing – is to trick you into revealing personal and financial information. The scammers can then use your personal information – such as your Social Security number, bank account or credit card numbers – to commit identity theft and steal your money.

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

1. The IRS does not send unsolicited e-mails about a person's tax account or ask for detailed personal and financial information via e-mail.
2. The IRS never asks taxpayers for their PIN numbers, passwords or similar secret access information for their credit card, bank or other financial accounts.
3. 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 Web site and entered confidential information, visit IRS.gov and enter the search term 'identity theft' for more information and resources to help.
4. You can help shut down these schemes and prevent others from being victimized. If you receive a suspicious e-mail that claims to come from the IRS, you can forward that e-mail to a special IRS mailbox, [phishing@irs.gov](mailto:phishing@irs.gov). You can forward the message as received or provide the Internet header of the e-mail. The Internet header has additional information to help us locate the sender.
5. Remember, the official IRS Web site is <http://www.irs.gov/>. Do not be confused or misled by sites claiming to be the IRS but end in [.com, .net, .org](#) or other designations instead of .gov.

**Link:** [Suspicious e-Mails and Identity Theft](#)