Be Aware of Suspicious E-Mails

Be aware of e-mail scams that fraudulently use the IRS name or Logo as a lure. The goal of the scam is to trick people into revealing personal and financial information, such as Social Security, bank account or credit card numbers, which the scammers can use to commit identity theft and steal your money.

The IRS does not send unsolicited e-mails about a person's tax account or ask for detailed personal and financial information. Additionally, the IRS never asks people for the PIN numbers, passwords or similar secret access information for their credit card, bank or other financial accounts.

If you receive an e-mail from someone claiming to be the IRS or directing you to an IRS site,

- Do not reply.
- 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 our Identity Theft page on IRS.gov.

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 The e-mail must be forwarded using special instructions at IRS.gov, or it loses the encoding needed to track it to its source. The IRS can use the information, URLs and links in the suspicious e-mails you forward to trace the hosting Web site and alert authorities to help shut down the fraudulent sites. After you forward the e-mail to us, delete the message.

Remember that all of the web page addresses for the official IRS website, IRS.gov, begin with http://www.irs.gov. Don' t be confused or misled by internet sites that end in .com, .net, .org or other designations instead of .gov. The address of the official IRS governmental Web site is www.irs.gov.

Link:

- Suspicious e-Mails and Identity Theft