US Residents: Be Aware Don't Get Scammed This Tax Season!

Every time tax season rolls around, so does *tax-scam season*. Starting in January, scam artists (especially online con artists) pose as the Internal Revenue Service (IRS). Their goal? To fool and defraud taxpayers—in other words, to scare you into giving them your money, your bank account information and your Social Security number. They do it by using a sophisticated but phony email trick called phishing. In a phishing campaign, the scammer sends you a fraudulent email that looks and sounds very real...and extremely serious. The email of choice during tax season looks as if it comes right from the Internal Revenue Service. The message? You owe money and you have to pay up NOW.

Stay safe during tax season.

The United States Computer Services Readiness Team (US-CERT) and the IRS have teamed up to get this message out to all taxpayers: Don't get scammed by IRS impersonators, and remain alert during tax season and year-round. More than that, they want you to join the fight against attempted scams by doing the following:

1. **Report suspicious phishing communications.**
    - Email: If you read an email claiming to be from the IRS, do not reply or click on attachments and/or links. Forward the email as-is to phishing@irs.gov (link sends e-mail), and then delete the original email.
    - Website: If you find a website that claims to be the IRS and suspect it is fraudulent, send the URL of the suspicious site to phishing@irs.gov (link sends e-mail) with subject line, "Suspicious website".
    - Text Message: If you receive a suspicious text message, do not reply or click on attachments and/or links. Forward the text as-is to 202-552-1226 (standard text rates apply), and then delete the original message (if you clicked on links in SMS and entered confidential information, visit the IRS' identity protection page).
2. **Understand how the IRS communicates electronically with taxpayers.**
    - The IRS does not initiate contact with taxpayers by email, text messages or social media channels to request personal or financial information.
    - This includes requests for PIN numbers, passwords or similar access information for credit cards, banks or other financial accounts.
        - The official website of the IRS is http://www.irs.gov/
        -
3. **Take action to avoid becoming a victim.**
    - If you believe you might have revealed sensitive information about your organization or access credentials, report it to the appropriate contacts within the organization, including network administrators. They can be alert for any suspicious or unusual activity.
    - If you are a victim of any of the above scams involving IRS impersonation, please report to phishing@irs.gov (link sends e-mail), and file a report with the Treasury Inspector General for Tax Administration (TIGTA), the Federal Trade Commission (FTC), and the police.

Spread the word.

Now that you've read this article, you know to be on the lookout for scam artists—but what about your parents, grandparents or any children over 16 who are first-time tax filers? At tax time, everyone is a potential target. Be sure to let them know about the scams that are out there. Share this article, help spread the word, and keep your family and friends protected. SOURCE: http://whatismyipaddress.com/irs-scam