IRS Issues Warning On New Email Tax Scam

Tax season may be at an end for most taxpayers, but scammers aren't letting up. The Internal Revenue Service (IRS) recently warned taxpayers and tax professionals about a new IRS impersonation scam email.

The email subject line may vary, but according to the IRS, recent examples use phrases like "Automatic Income Tax Reminder" or "Electronic Tax Return Reminder." The emails include links that are meant to look like the IRS website with details about the taxpayer's refund, electronic return or tax account. The emails contain a "temporary password" or "one-time password" that purports to grant access to the files. However, these are actually malicious files. Once the malware files are installed on your computer, scammers may be able to secretly download software that tracks every keystroke, giving the bad guys access to information like passwords to your financial accounts.

Don't be fooled: the IRS does not send unsolicited emails and never emails taxpayers about the status of refunds.

IRS Commissioner Chuck Rettig confirmed, "The IRS does not send emails about your tax refund or sensitive financial information. This latest scheme is yet another reminder that tax scams are a year-round business for thieves. We urge you to be on-guard at all times."

The IRS doesn't initiate contact with taxpayers by email, text messages, or social media channels to request personal or financial information. This includes requests for PIN numbers or passwords used to access your credit cards, banks, or other financial accounts. The IRS also doesn't call to demand immediate payment using a specific payment method such as a prepaid debit card, gift card or wire transfer. The IRS will typically send a bill to a taxpayer who owes taxes.

Phishing and phone scams topped the 2019 "Dirty Dozen" list of tax scams. The common thread, according to the IRS: Scams put taxpayers at risk. Don’t engage or respond with scammers. Here’s what to do instead:

- If you receive a call from someone claiming to be from the IRS and you do not owe tax, or if you are immediately aware that it’s a scam, just hang up.
- If you receive a robocall or telephone message from someone claiming to be from the IRS and you do not owe tax, or if you are immediately aware that it’s a scam, don’t call them back.
- If you receive a phone call from someone claiming to be with the IRS, and you owe tax or think you may owe tax, do not give out any information. Call the IRS back at 1.800.829.1040 to find out more information.
- Never open a link or attachment from an unknown or suspicious source. If you’re not sure about the authenticity of an email, don’t click on hyperlinks. A better bet is to go directly to the source’s main web page.

- Use strong passwords to protect online accounts and use a unique password for each account. Longer is better, and don't hesitate to lie about important details on websites since crooks may know some of your personal details.
- Use two- or multi-factor authentication when possible. Two-factor authentication means that in addition to entering your username and password, you typically enter a security code sent to your mobile phone or other device.

If you believe you are a victim of an IRS impersonation scam, you should report it to the Treasury Inspector General for Tax Administration at its IRS Impersonation Scam Reporting site and to the IRS by emailing phishing@irs.gov with the subject line "IRS Impersonation Scam." That's how the IRS was alerted about the most recent scam: According to the IRS, taxpayers began notifying phishing@irs.gov about these unsolicited emails from IRS imposters.

The IRS and its Security Summit partners, consisting of state revenue departments and tax community partners, continue to be concerned about these scams.

Keep your personal information safe by remaining alert - and when in doubt, assume it's a scam.

By Kelly Phillips Erb