Avoid Health Care-related IRS Scams

Following numerous reports of scammers sending fraudulent versions of CP2000 notices during the 2015 tax year, the IRS and its Security Summit partners are warning taxpayers to be on high alert for the 2016 tax year and all subsequent tax years.

What Is a CP2000 Notice?
The CP2000 is a notice generated by the IRS Automated Underreporter Program that is commonly mailed by the IRS to taxpayers through the U.S. Postal Service.

The IRS will mail out a CP2000 notice if the income or payment information it has on file does not match the information reported on a tax return. The notice provides instructions to taxpayers about what to do if they agree or disagree that additional tax is owed. It also requests that a check be made out to "United States Treasury" if the taxpayer agrees additional tax is owed.

The Scam
This scam involves an unsolicited email claiming to contain an IRS tax bill (CP2000) as an attachment. The fraudulent notices request taxpayers to mail a check made out to the "I.R.S." to the "Austin Processing Center" and includes a post office box address. There is also a "payment" link within the email itself.

Receiving an electronic CP2000 notice is the largest indicator of suspicious activity. Additional things to look for include:

- The CP2000 notice is issued from an Austin, Texas, address.
- The CP2000 notice is requesting information regarding 2014 coverage.
- The payment voucher lists the letter number as 105C.

It is important to note that this information is specific to the 2015 tax year. Scammers are looking to stay one step ahead of law enforcement and consumers, so they will likely employ different tactics moving forward. Taxpayers should take precautionary measures to avoid falling victim to scams.

Common IRS impersonation scams take the form of phishing emails, aggressive letters and threatening phone calls.

How Can I Protect Myself?
Remember, the IRS will **never** initiate contact with you electronically. If you receive any form of electronic communication from someone claiming to be with the IRS, report it promptly. The IRS has published guidelines on how to report phishing and online scams. If you receive an email related to this specific scam, immediately forward it to phishing@irs.gov and delete it from your account. Do not reply to the sender or open any attachments.

If you have received a CP2000 notice in the mail and are concerned over its legitimacy, visit the IRS's "Understanding Your CP2000 Notice" webpage, which includes an image of a real notice used by the IRS. For concerns over other notices received in the mail, visit the IRS's "Understanding Your IRS Notice or Letter" webpage.

ConnectPay® PAYROLL SERVICES