



Fraudulent Emails

It has recently been brought to our attention that there is a new email fraud that is targeting everyone and being used to steal sensitive business information. Essentially, the target victim will receive an email stating that their payment ID (EIN) has been rejected for one of their tax payments and you must go to a specific website to reenter the information. Upon entering the website you were directed to, you will be asked to provide updated addresses, tax information, EIN, passwords, and even bank account information, which can be used to steal money and assets from you.

First off, the IRS will never contact you through email unless you have emailed them directly. If you receive an email that seems suspicious to you, DO NOT follow the link provided, and do not reply to the email. Contact our office immediately at 610-275-7544, we will have you either email or fax the message you received to us, and will then be able to help you determine whether it is a fraudulent email or not. Further more, the IRS is aware of this scam and would like anyone who receives fraudulent emails to forward them to the IRS at phishing@irs.gov. This will help the IRS keep track of the different scams and email addresses used by the scammers, and hopefully shut down their operation.

Below are some warning signs that the notification you have received is fraudulent. For more information on the topic you can follow the link below to an article on the IRS website explaining the frauds more in-depth.

<http://www.irs.gov/newsroom/article/0,,id=160334,00.html>

(If clicking on the web address above does not bring you to the IRS website, you can copy and paste it into your browser address bar and press enter.)

Warning Signs that the Email you Received is Fraudulent:

- The subject line states that this is your 2nd or 3rd notice, and you don't recall receiving a prior notice. Not only should you be questioning the fact that you haven't received a prior notice, but also, if you called in your payment through the telefile system, you would receive a notice through the mail and not email.
- The email address from which the email is sent is customers@eftps.gov, the website you are directed to is <http://eftps.gov/R21>, or the return reason is Code R21. The IRS warns that this is not a government email address or web address, and there is no error code R21. Anything coming from that address should be forwarded directly to their phishing inbox at phishing@irs.gov.

- There is no contact information for the sender aside from their email address and the website they provide. The IRS will always send mailing addresses and phone numbers to reach them at in case there is a discrepancy with the claim.
- If any of the information pertaining to your company that is used in the email is outdated or very far off base from your actual information, then it is most likely a fraud. For example, in the attached example email (we blacked out the email address that the notice was sent to) the email address used by the scammers to contact the targeted victim hasn't been used by their company for a number of years. Also, the Federal Tax Payment ID of 010375169 shown in the email has no resemblance to the clients' actual EIN number.
- Also, please remember, the IRS will never send an unsolicited email to you asking for personal information.