

# EFTPS Phishing Scam Targets Tax Payers

by [rahsheen](#)  
October 7, 2010



A new phishing scam is on the rise and is targeting well-meaning people just trying to get right with the IRS. According to McAfee, the scam targets individuals using the Electronic Federal Tax Payment System (EFTPS) to pay their taxes. This system has been in place since 1996 and was established by the U.S. Department of the Treasury to allow people to easily pay their taxes online.

The recent fraudulent format uses an email message that claims to be a rejected tax payment and directs users to a fake website for additional information.

This scam follows the standard format of emailing potential victims, claiming something needs to be updated. In this case, it's especially heinous because the attackers are using the IRS to scare people. Many people are using the EFTPS system to pay taxes they owe on a payment plan.

These plans are set up by the IRS and can sometimes be very reasonable depending on your situation. The flip-side of that is that the IRS will quickly terminate your agreement if you miss even a single payment. This means you could be subject to wage garnishment, liens, and maybe even jail time. There is no negotiating. Most EFTPS users who receive this fraudulent email are probably breaking their index finger trying to click the link for more info.

The scam message:

Subject:

Your EFTPS Tax Payment ID has been rejected.

Body:

Report ID: \*\*\*. Your Federal Tax Payment ID: \*\*\* has been rejected. Return Reason Code R##  
– The identification number used in the Company Identification Field is not valid. Please, check

the information and refer to Code R## to get details about your company payment in transaction contacts section: [http://www.eftps\\*\\*\\*\\*\\*7.com/contacts](http://www.eftps*****7.com/contacts)

These types of scams can only work with your cooperation. They will try the dirties tricks to get you to click some random, unsolicited link in order to get your information and/or your money. We saw this recently when [scammers used Haiti disaster as a tool](#). If you have any suspicion whatsoever about whether an email is a scam or not, it probably is.

Most importantly, remember this bit of information: **The IRS does not initiate contact with a taxpayer via email.** Not a “call me”, not a “you’re overdue” and especially not a “you owe us some more money.”

Most of the important institutions in your life, like the IRS and your bank, will rarely contact you about anything important via email. Don’t blindly trust the information your email interface shows you. View the headers (“show details” or “view original” in Gmail) and look at the actual email addresses and Reply-To address.

If you’re suspicious of a link in your email, IM’s, Twitter, Facebook, or anywhere, one simple check you can do is hover over it and look at your browser’s status bar to verify where it goes. The best thing you can do is just leave it alone and find another way to contact the alleged source.