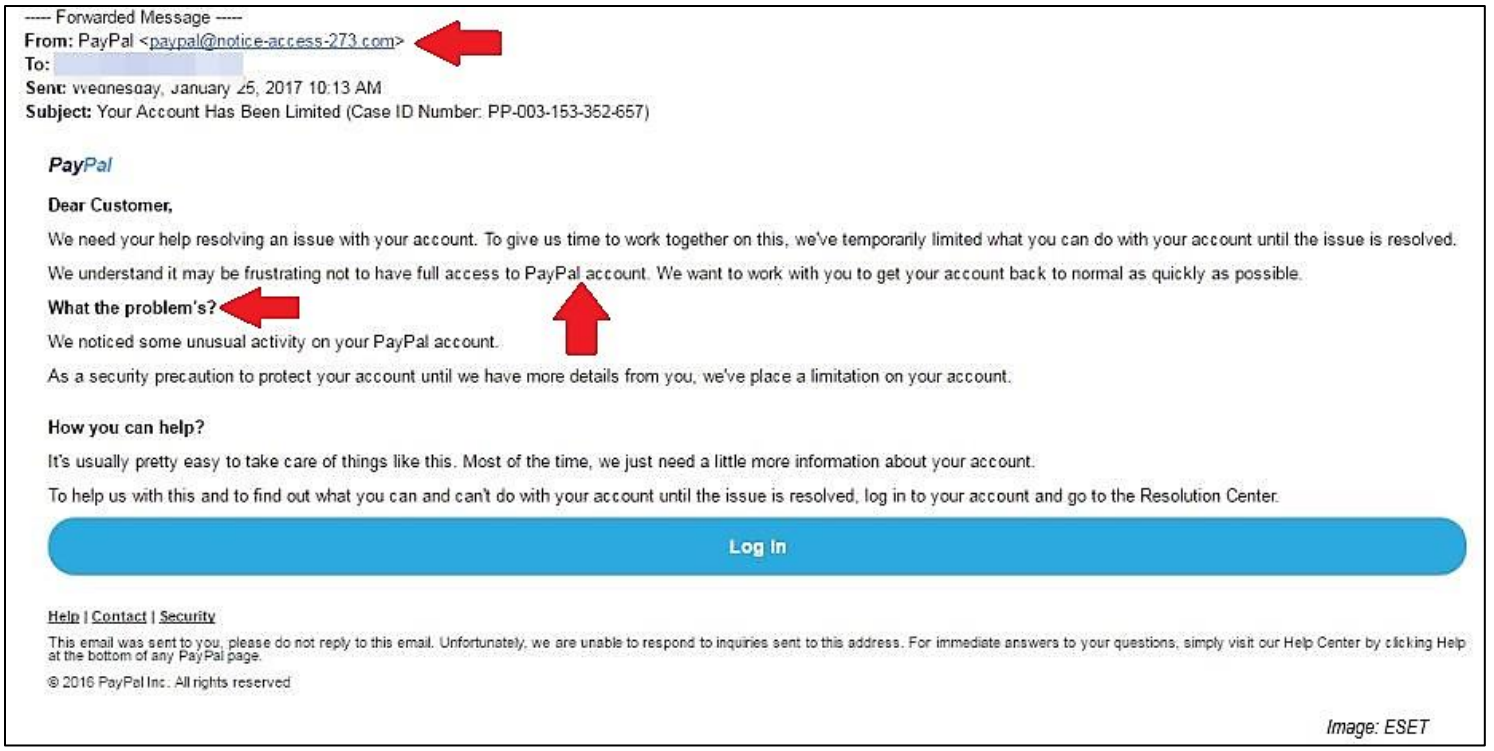
Amazingly Realistic PayPal Phishing Email is Working Overtime

Published February 6, 2017

There is yet another phishing scam targeting PayPal users. This one is an example of how the fraudsters and scammers are getting pretty good at tricking their victims. It even uses the actual PayPal logo (or an incredibly well-done facsimile of it), the PayPal color schemes, and claims there is an issue with the user's account that needs to be corrected. Until it is, there will be limited access and functionality to the account.

The email received is not bad, but still does have the tell-tell signs of phishing, if you are paying close attention. There are few language mistakes (for example, one heading is "What the Problem's") and there is a generic greeting of "Dear Customer." It also has a sender address that is nothing similar to PayPal's domain (in the example seen, it was "notice-access-273.com").



----- Forwarded Message -----
From: PayPal <paypal@notice-access-273.com>
To:
Sent: Wednesday, January 25, 2017 10:13 AM
Subject: Your Account Has Been Limited (Case ID Number: PP-003-153-352-657)

PayPal

Dear Customer,

We need your help resolving an issue with your account. To give us time to work together on this, we've temporarily limited what you can do with your account until the issue is resolved.

We understand it may be frustrating not to have full access to PayPal account. We want to work with you to get your account back to normal as quickly as possible.

What the problem's?

We noticed some unusual activity on your PayPal account.

As a security precaution to protect your account until we have more details from you, we've place a limitation on your account.

How you can help?

It's usually pretty easy to take care of things like this. Most of the time, we just need a little more information about your account.

To help us with this and to find out what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

Log In

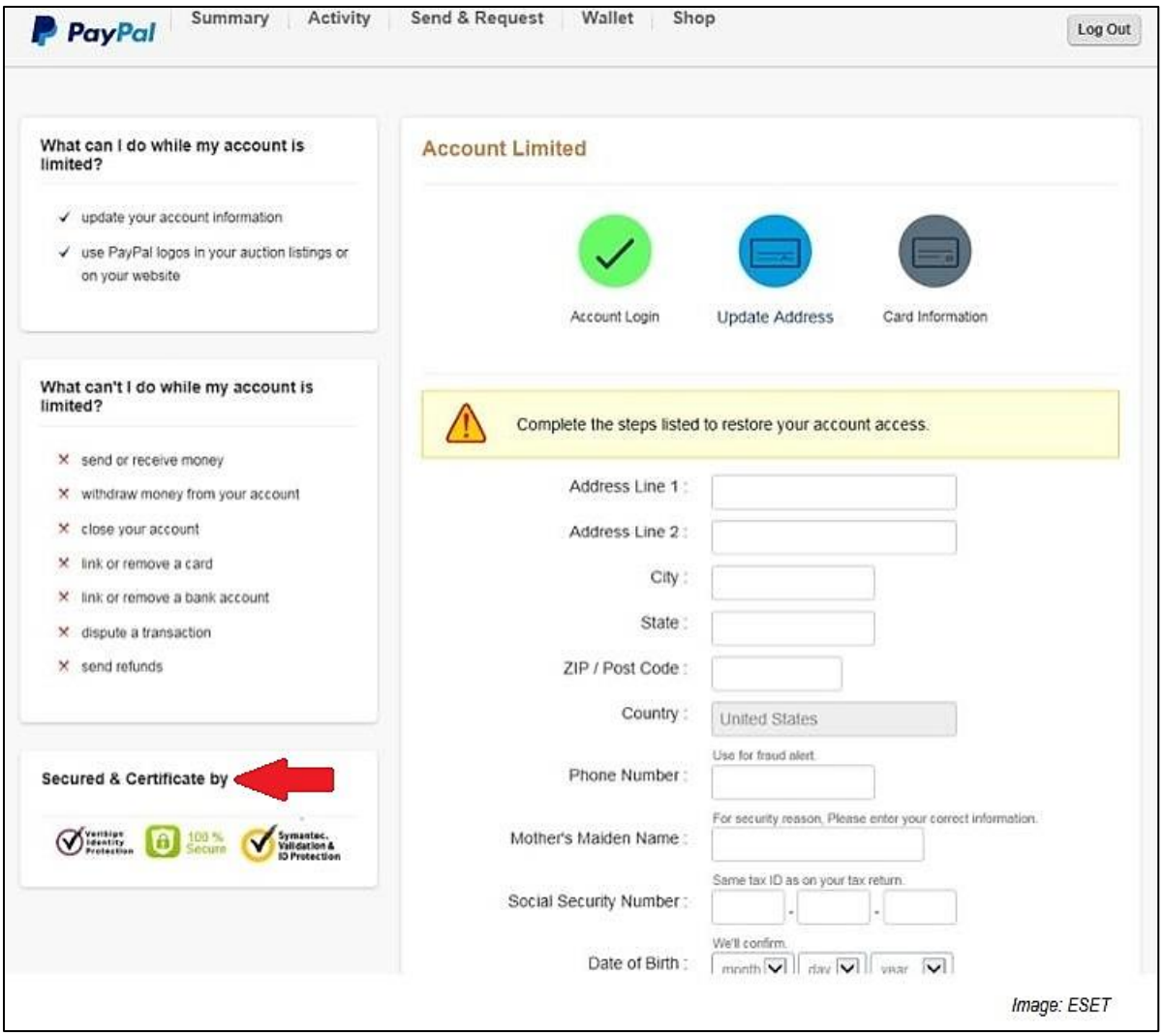
Help | Contact | Security

This email was sent to you, please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking Help at the bottom of any PayPal page.

© 2016 PayPal Inc. All rights reserved

Image: ESET

However, if the reader is tricked into thinking there is a problem, the button included in the email that supposedly goes to the PayPal login screen, actually goes to a fake site. Now, the phoniness of that site is very difficult to detect. It has the PayPal logo nicely done. At the bottom are the logos for a 100% secure site by Symantec, but the wording is not quite right: "*Secured & Certificate by Symantec*." If you are looking for the green lock next to the URL to ensure you have landed on a secure site, you will see it. Per ESET, the thieves are transmitting the form over an HTTPS link.



Along the side of the screen are some FAQs about having limited access. A subsequent screen after clicking the "continue" button has a list of items to fill in. These include address, social security number, and mother's maiden name.

Always be on the lookout for phishing. With the plethora of data breaches occurring these days and the sophistication of the fraudsters on the rise, it's ever more important to pay close attention when an email is received that says something is wrong with an account that stores such sensitive information. Never click links or attachments included in those. Go directly to your account and login from a previously saved link or by manually typing the URL into the address bar. If you receive a suspicious email or find a fake PayPal-related site, you can report it to PayPal as well. There is more information in its Help Center.

PayPal is a particularly attractive target for such scams because it's tied to payment card and bank account numbers. If they get your login credentials, it's not much more effort for them to steal from you. **Always take the time to read messages carefully and if there is any suspicion at all, don't click.**