Title:
How to identify Spoof/Phishing emails - Protect yourself from identity theft.

Word Count:
1716

Summary:
Learn how to protect yourself from Spoof and fraudulant emails.

Keywords:
spoof, phishing, fraud, spoof emails

Article Body:
What is a spoof email?

Spoof emails (sometimes also called "Phishing") are emails that pretend to be from a company or bank. The most common often come from eBay, PayPal, Barclays Bank etc. These emails will then contain a web link, if you click on this link then you will be taken to a login page and asked to enter your details. Most of these scammers go a long way to try and get your details, most spoof emails contain links to identical websites and users are tricked into entering their personal information. If you submit your information through one of these spoof websites then the fraudster has all of your details and can commit crimes using your identity.

How do they get my email address?

You may wonder how the scammers got your address or knew you were a member of a particular bank or institution. Often it is just good luck on the part of the scammers. They normally do not target individuals, but send out thousands of scam emails to randomly generated email addresses, in the hope that just a few will be successful. They also trawl the web for valid addresses they can use, and swap this information with each other. If you have ever posted on an Internet forum or published something on the web, there's a good chance your address is out there somewhere just waiting to be found. If you have fallen victim before, your address is normally added to a list of 'easy victims', and you are likely to then receive even more scams.

How can I identify these emails?

Here are 4 simple tests that you can perform on any email you suspect is a

spoof. Your email can only pass the test if it passes ALL FOUR of the tests. If your email passes all of the four tests then you can be 99.9% certain that it is a genuine email. If your email passes all four of the tests then we would also advise you to check the "Other Tips" section just to double check that your email is genuine.

If your email fails

If your email fails JUST ONE of the four tests then the email is a spoof and shouldn't be replied to and should be deleted immediately from your computer. Even if your email fails the test, I would still advise you to check out the "Other Tips" page for more good ways to spot a spoof email.

If you are still in doubt

Unless you are 100% sure that your email is genuine, DO NOT click on any links within the email. Contact the company in question (See the "reporting a spoof" page) and ask them to confirm if the email is genuine or a spoof.

Test 1 - Who is the email addressed to?

Have a look at how the email addresses you. Most spoofs will say something along the lines of "Dear eBay user". This is the very first thing you should look for in a spoof email. Any email that doesn't address you by your name is a spoof. Ebay, PayPal and banks always address you by the name you registered with on their site, they NEVER send out emails saying

"Dear valued customer", "Dear member" etc.

If your email isn't addressed to you personally then it is a spoof! If your email is addressed to you then move onto the next test to see if it is a spoof email. Some more advanced spoof messages have started to include your name or email address instead of the generic "Dear member" or "Dear user". So even if your email were addressed to you I would strongly advise you to carry out the 3 other tests.

Test 2 - Where does the link go?

Most spoof emails will contain a link telling you to verify your details. You can quickly tell if your email is a spoof by hovering your mouse over the link. When your mouse is over the link, look in the bottom left hand corner of your screen and you will see the "link destination". The destination of a spoof link will usually look something like this:

"http://slp.clinker.net.mx/.sh/.a/index.htm?SignIn&ssPageName=h:h:sin:us"

Compare this with a real eBay link:

http://k2b-bulk.ebay.co.uk/ws/eBayISAPI.dll?MyeBaySellingSummary

And you can see the difference. You can easily check if you email is a fake by looking at the first part of the link destination, if the destination is a combination of numbers (102.382.54.23) or a link like the one in my spoof link above then the chances are that your email is a spoof.

Any non-spoof link will contain the name of the company in the first part of the link, eg:

http://cgi.ebay.co.uk http://cgi.ebay.com http://cgi.paypal.com

Please note: Some spoof links will contain the words "eBay" or "PayPal" in the final part of the link. These are also spoofs!

All real emails will only contain the company name in the very first part of the link; after http://. If you still aren't sure if you have a spoof email, move onto the next test.

Test 3 - Who really did send you the email?

This test may seem a little confusing but don't worry it isn't as difficult as it looks. What we are going to do is find out where the email came from. Most people don't know this but you can trace the origin of your emails in most mail programs. To do this we have to view the "FULL message header", here is how you do this in the following email programs. If your program isn't listed here please contact your email provider for instructions:

Hotmail 1. Click on "Options" 2. Click on "Mail display settings" 3. The 3rd option can be used to display the header settings, select "Full" from the check boxes 4. Click on "OK" to save your settings

Outlook Express 1. Right click on the email and select "Properties" 2. Select the "Details" tab

Now that we can view the message headers, here is how you identify a spoof:

Look in the part of the header that says "Received From". If the email has come

from anyone other than the sender it's a spoof. I had a spoof email and performed this test and notice that the email had been sent from a Yahoo account. Obviously a real email from eBay would not have been sent from a Yahoo address!

Test 4 - Click on the link

Only try this if your email has passed the previous 3 tests. Some spoof emails have been known to contain viruses that are activated by clicking on the link. Please ensure that you have a good virus scanner installed on your PC before proceeding. If you have important data on your PC you may also wish to backup that data on a removable backup device.

When you click the link in your email a web browser will open and take you to what looks like a legitimate login page. There are two ways to identify a spoof login page, and I will show you both of them! Have a look in the address bar at the top of the login page. Have a look at the http:// part of the URL. Any genuine login page from eBay, PayPal or your bank WONT start with "http://" it will start with:

"https://"

The "s" in https:// stands for "secure" and is there to show you that you are about to submit data over a secure connection.

Any page not starting with https:// is a spoof. The second difference between the two pages is the padlock icon in the bottom right hand of the screen. Notice that the spoof login page doesn't have a padlock, and the genuine eBay login page does. This padlock appears to show you that you are about to submit data over a secure connection. If your login page DOESNT have a padlock icon in the bottom corner of the screen then it is a spoof!

Other Tips for spotting Spoofs

1. Punctuation Read your email carefully and look for any spelling mistakes. You can be sure that any genuine emails wont contain simple spelling mistakes.

2. Adverts? Real emails from eBay don't contain adverts for burger king!

3. Hotmail identity check A new feature in hotmail now warns you if a senderID could not be verified. Any spoof email will contain this warning. (please note that recently I received a genuine email from eBay that contained this warning, so don't judge an email purely by this method)

4. PIN number Any website asking for your PIN (personal identification number) is a spoof. Do not enter your PIN number! If you have entered and submitted your PIN then contact your bank immediately.

5. Popup boxes Some spoof sites will include popup message boxes like the one below. Genuine sites don't use popup boxes telling you to enter details.

6. False sense of urgency Most spoof emails will make you think that your account is at threat if you don't act quickly. This is not the case.

7. eBay Messages Any genuine email sent to you from eBay will also appear in the "My Messages" section of eBay. To access your eBay messages, login to ebay and click on "My eBay". On the left hand side of the screen you will see a "My Messages" link. Click on this; if the email you received in your inbox isn't listed there then it is a spoof email.

8. Ignore the email address Ignore the email address that the email was sent from. Almost all spoof emails will appear as if they are from a genuine address. Some of the emails I receive are "from":

service@paypal.com memberservices@paypal.com awconfirm@ebay.com safeharbour@ebay.com operator_862736743@halifax.com

9. Download the eBay toolbar The eBay toolbar is a great piece of software that can be used to spot spoofs. As soon as you enter a spoof website from eBay or PayPal the toolbar will give you a warning telling you that web page is a spoof. The Ebay toolbar is FREE to download.

Dan Thompson has been creating websites for over 7 years. You can visit his website and receive 6 free e-books, check out the website on http://www.elpassobooks.co.uk