

Title:

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

Word Count:

1716

Summary:

Learn how to protect yourself from Spoof and fraudulent 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

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

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 or

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

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

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 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

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

"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 your email is a fake by looking at the

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

All real emails will only contain the company name in the very first part of the link; after h

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

Hotmail 1. Click on "Options" 2. Click on "Mail display settings" 3. The 3rd option can be use

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

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 ot

Test 4 - Click on the link

Only try this if your email has passed the previous 3 tests. Some spoof emails have been known

When you click the link in your email a web browser will open and take you to what looks like

"https://"

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

Any page not starting with https:// is a spoof. The second difference between the two pages is

Other Tips for spotting Spoofs

1. Punctuation Read your email carefully and look for any spelling mistakes. You can be sure t

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 ve

4. PIN number Any website asking for your PIN (personal identification number) is a spoof. Do

5. Popup boxes Some spoof sites will include popup message boxes like the one below. Genuine s

6. False sense of urgency Most spoof emails will make you think that your account is at threat

7. eBay Messages Any genuine email sent to you from eBay will also appear in the "My Messages"

8. Ignore the email address Ignore the email address that the email was sent from. Almost all

service@paypal.com memberservices@paypal.com awconfirm@ebay.com safeharbour@ebay.com operator_

9. Download the eBay toolbar The eBay toolbar is a great piece of software that can be used to

Dan Thompson has been creating websites for over 7 years. You can visit his website and receive

This is a demo version of txt2pdf v.10.1

Developed by SANFACE Software <http://www.sanface.com/>

Available at <http://www.sanface.com/txt2pdf.html>