

# 8 Surefire Ways to Spot an EBAY Scam E-Mail and Protect Yourself from Identity Theft

*Article by: Mike Makler*

Ebay is a great site and is used by many to buy and sell new and used Items. It truly is the worlds Largest Garage Sale Unfortunately when an online site becomes as big and popular as E-Bay the scam artists seem to just naturally follow. These Scam artists will often try to steal your Identity and get your bank or credit card information in addition to your E-Bay Id and Password

A Typical Ebay Scam Artist will send you an e-mail requesting that you update your account. Often this request to update your account is made under some false pretence like it is suspended or has been suspected of Fraudulent use. Here is a Copy of a recent Ebay Scam E-mail I received <http://ewguru.com/ebay-scam>. You will notice the E-Bay Link on this page looks real. Don't click it. You can however do a right click properties and notice that it is in fact a phony link.

E-bay has an excellent online Tutorial that teaches how to spot and protect yourself from spoof e-mails <http://ewguru.com/spoof-emails>

Here are 8 Surefire Ways to Spot an EBAY Scam E-Mail and Protect Yourself from Identity Theft

## 1 - Wrong E-Mail Address

Any E-mail Sent to an E-mail Address that is Not Your Primary Ebay E-mail Account is more then likely a scam.

## 2 - Fake links.

While many emails have links included, just remember that these links can be forged too. After you click on the Link a Real E-Bay Address should appear. To determine if the Web address in your browser is a real eBay address, look for ".ebay.com" immediately before the first "/".

## 3 - Requests Personal Information

Any E-mail that requests you enter personal information like User ID, password or bank account number either by clicking on a link in the E-mail or completing a form within the e-mail are a strong indication the e-mail is a SCAM

## 4 - Urgent Subject Lines

Subject likes \*\*\* Please Verify & Update Your Account \*\*\*

## 5 - Generic greetings.

Lot's of emails begin with a Greeting, such as: "Dear Ebay member instead of the Name you used when you registered for your account

## 6 - Scare to Action

Many Fake emails try to trick you with the threat that your account is in jeopardy if you don't sign in and fix it NOW!

## 7 - HTML Website Fakes

Emails that appear to be websites. Some emails will look like a website in order to get you to enter personal information. Ebay never asks for personal information in an e-mail.

## 8. Misspellings and bad grammar

Fake emails may contain misspellings, incorrect grammar, missing words. Many Times these are used to trick the E-mail Filters

**A quick review** If you receive an E-mail with a Link requesting you to click on the link and sign in to your E-bay account, Don't Do It!

If you receive an E-mail that looks like an Ebay Sign in Form, Don't Sign in!

If you are unsure if the e-mail is Real or fake forward it to [spoof@ebay.com](mailto:spoof@ebay.com) and request assistance.

If you absolutely must login to your Ebay account then I would highly recommend you do the Following. Close all open

Browser sessions. Run a Spyware check on your computer You can get a free Spyware program here (<http://ewguru.com/sware>) then type in <http://www.ebay.com/> directly into your Browser window and Login from the E-bay Web Page. Never click on a Login Link from Any E-Mail.

**About The Author:**

Mike Makler has been Marketing Online Since 2001 When he Built an Organization of over 100,000 Members

Get Mike's Newsletter:

<http://ewguru.com/newsletter>

More Articles by Mike:

<http://ewguru.com/tips>

Permission Based E-Mail Marketing Methods

<http://ewguru.com/hbiz/amazingoffer.html>

Copyright © 2005-2006 Mike Makler the Coolest Guy in the Universe

[You have permission to publish this article electronically or in print, free of charge, as long as the bylines are included. A courtesy copy of your publication would be appreciated [getarticles At Ewguru .Com](mailto:getarticles@Ewguru.Com)]