

# 8 Surefire Ways to Spot an E-Mail Identity Theft Scam!

---

*Article by: Mike Makler*

The E-Mail Identity Theft Scam is running Rampant. These E-Mail Scam artists will go to great lengths to Get Your Bank Account information and Steal your Identity. Learn how to Protect To Yourself Now!

A Typical E-Mail Identity Theft Scam will send you an e-mail requesting that you update your Bank Account Information. Often this request to update your account is made under some false pretence like it is suspended or has been suspected of Fraudulent use.

E-bay has an excellent online Tutorial that teaches how to spot and protect yourself from spoof e-mails, While this Tutorial talks specifically about E-Bay many of the Tell Tale Signs are very Similar and would apply to E-Mail Identity Theft Scams <http://ewguru.com/spoof-emails>

Here are 8 Surefire ways to spot an E-Mail Identity Theft Scam E-Mail

## 1 - Wrong E-Mail Address

Any E-mail Sent to an E-mail Address that is Not the E-mail Account you used when you signed up for the 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. It is always best to type the e-mail address of the bank directly into your browser window (<http://www.yourbank.com>)

## 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 Account Holder instead of the Name you used when you registered for your account are more then likely scams. Your bank Knows your Name.

## 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. Banks 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 Bank account, Don't Do It!

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

If you are unsure if the e-mail is Real or fake call your bank and ask.

### 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