

How To Spot A Fraudulent Email

This E-book Is Brought To You By :

[Not Just Another Ezine](#)

You may give away this guide as a free report, but you may not sell, alter, copy or edit any of the information within without explicit permission from the author.

Published by Anna-Marie Stewart
Editor of Not Just Another Ezine <http://annamarketing.com>
Author of Forget The Hype! <http://annamarketing.com/FTH>

The necessary legal bits

Legal Notice and Terms of Agreement

Copyright © 2005 Anna-Marie Stewart. All rights reserved.

This e-book should be circulated as is, without changing any content. No part of this publication may be reproduced, without prior written permission from Anna-Marie Stewart. admin@annamarketing.com

While attempts have been made to verify information contained in this publication, in view of human errors or changes in technology in the future, neither the author nor the publisher assumes any responsibility for errors, omissions, interpretations or usage of the subject matter herein. This publication contains the opinions and ideas of its author and is intended for informational purposes only. The author and publisher shall in no event be held liable for any loss or other damages incurred from the usage of this publication.

Limits of Liability / Disclaimer of Warranty:

The authors and publisher of this book and the accompanying materials have used their best efforts in preparing this program. The authors and publisher make no representation or warranties with respect to the accuracy, applicability, fitness, or completeness of the contents of this program. They disclaim any warranties (expressed or implied), merchantability, or fitness for any particular purpose. The authors and publisher shall in no event be held liable for any loss or other damages, including but not limited to special, incidental, consequential, or other damages. As always, the advice of a competent legal, tax, accounting or other professional should be sought. The authors and publisher do not warrant the performance, effectiveness or applicability of any sites listed in this book. All links are for information purposes only and are not warranted for content, accuracy or any other implied or explicit purpose. This manual contains material protected under International and Federal Copyright Laws and Treaties. Any unauthorized use of this material is prohibited. Adobe, Adobe Acrobat and related names are the property of Adobe Systems Incorporated. No relationship with or endorsement of this publication by Adobe Systems Incorporated should be inferred.

How To Spot A Fraudulent Email

In my travels around the internet marketing forums, I noticed a lot of people were having problems with emails they were receiving from places like Paypal, EBay and various online banks.

The amount of phishing that's going on these days is almost incredible, what's worse is that so few people are actually aware of it, so I sat myself down and wrote an article in the hopes of helping a few more people avoid being scammed.

Have YOU been receiving suspicious looking emails from Paypal, telling you that your account is about to be closed or limited due to suspicious activities being registered by their staff?

It's definitely a phishing scam where people are out to fool you into giving them your info. Looking at the code, or headers will usually reveal anonymous urls, especially numbered ones, or urls that are definitely **not** pointing to paypal.

The 3 Dead Giveaways:

A). The email isn't addressed to you personally, but says "Dear customer". Paypal, and all other banks will always address you by name in their mails to you.

B). Ask around a bit, and you'll hear of others who've had the exact same messages. This is because the phishing is going on in mass mailings to thousands of people at a time.

C). I don't know about other email programs, but if you're using Outlook Express, you can usually see the REAL website address by running your mouse over the one in the email. It'll show up right at the bottom of your Outlook Express.

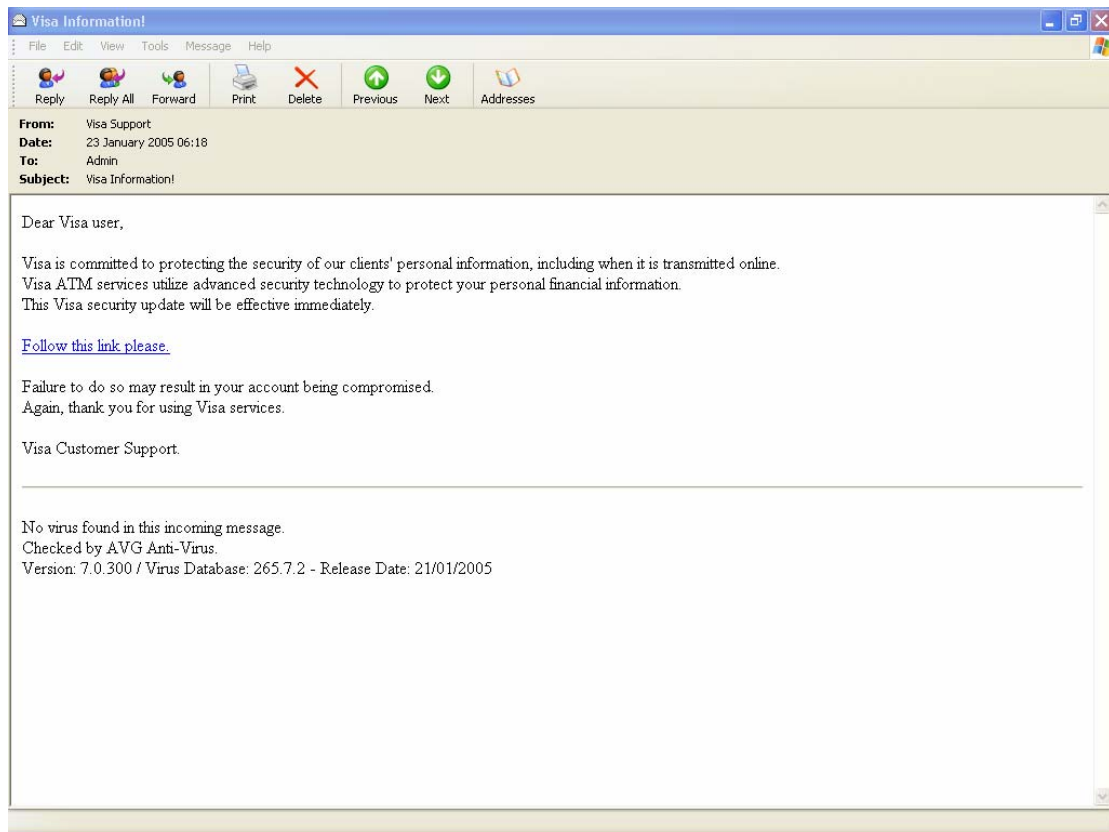
Another way to check is by checking the headers of the email. This is quite easy to do, although not many people seem to be aware of it. Read on for a quick step-by-step:

1. Open the email

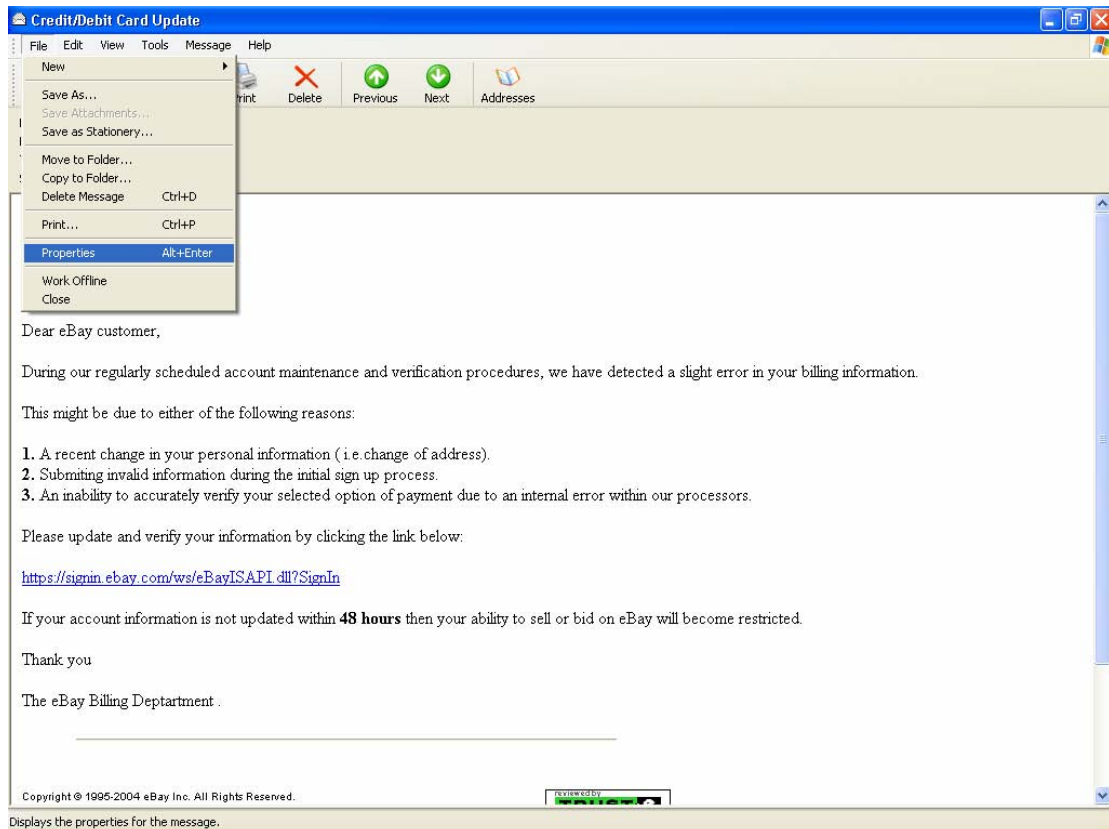
I've shown a few different examples of fraudulent emails here

The screenshot shows an email client window titled "PayPal Flagged Account". The email header includes: From: PayPal, Date: 23 January 2005 03:32, To: webmistress@annamarketing.com, Subject: PayPal Flagged Account. The main body of the email features the PayPal logo and the text: "Dear PayPal Member, Your account has been randomly flagged in our system as a part of our routine security measures. This is a must to ensure that only you have access and use of your PayPal account and to ensure a safe PayPal experience. We require all flagged accounts to verify their information on file with us. To verify your Information at this time, please visit our secure server webform by clicking the hyperlink below." A yellow button with the text "Click here to verify your Information" is present. Below this, it says "Thank you for using PayPal The PayPal Team". Further down, it states: "Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the 'Help' link in the footer of any page." At the bottom, it says: "To receive email notifications in plain text instead of HTML, update your preferences here" with a link to "https://www.paypal.com". On the right side of the email body, there is a grey box containing a virus scan report: "No virus found in this incoming message. Checked by AVG Anti-Virus. Version: 7.0.300 / Virus Database: 265.7.2 - Release Date: 21/01/2005". Below this is a section titled "Protect Your Account Info" with the text: "Make sure you never provide your password to fraudulent websites. To safely and securely access the PayPal website or your account, open up a new web browser (e.g. Internet Explorer or Netscape) and type in the PayPal URL (http://www.paypal.com/). PayPal will never ask you to enter your password in an email. For more information on protecting yourself from fraud, please review our Security Tips at".

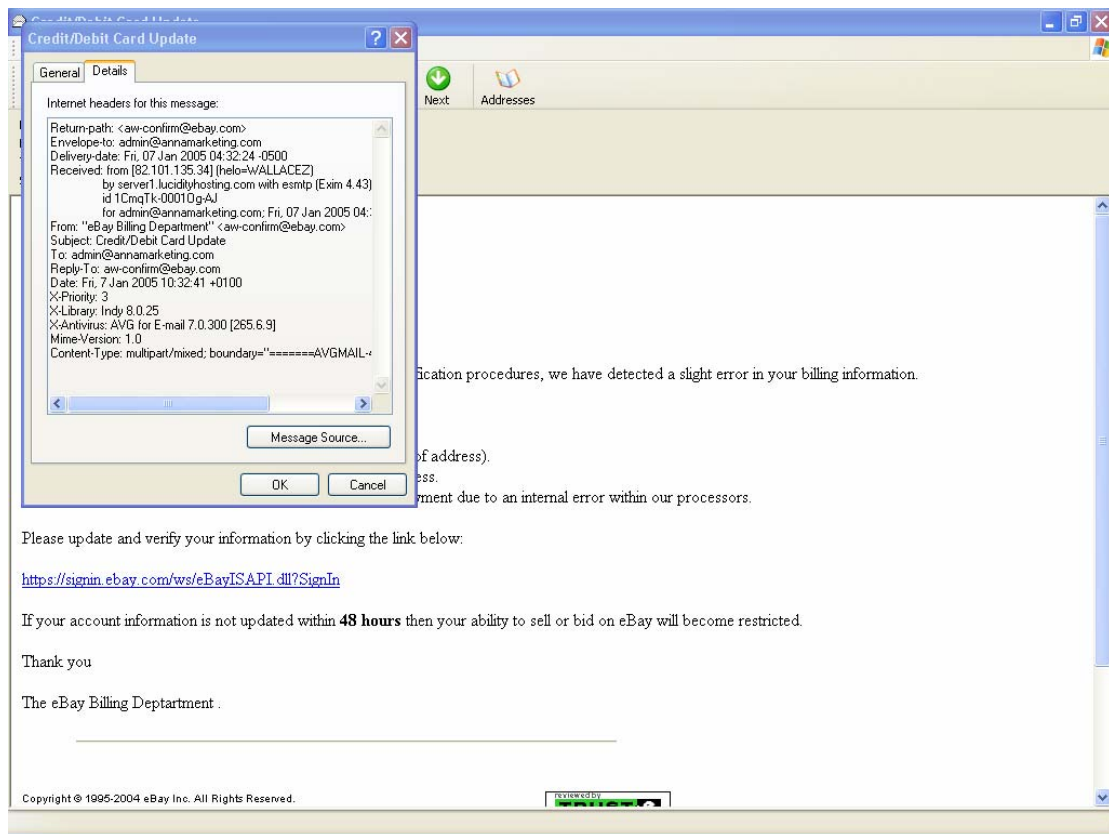
The screenshot shows an email client window titled "Your eBay account can be suspended.". The email header includes: From: aw-confirm@ebay.com, Date: 13 January 2005 00:04, To: admin@annamarketing.com, Subject: Your eBay account can be suspended. The main body of the email features the eBay logo and the text: "Dear eBay Member, We regret to inform you that your eBay account has been suspended due to concerns we have for the safety and integrity of the eBay community. Per the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us." Below this text is a form titled "Enter Your Ebay Information" with radio buttons for "Seller" and "Buyer". The form contains four input fields: "User ID", "Password", "Re-enter Password", and "Email Address".



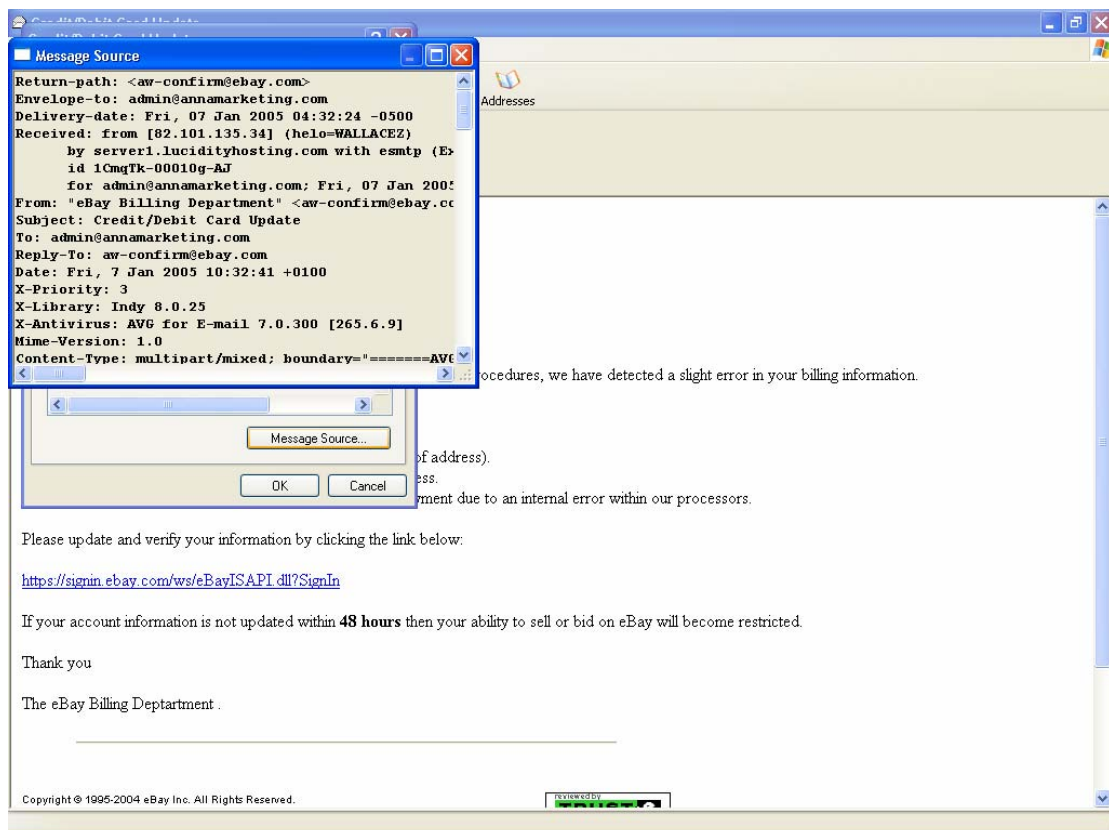
Next, click on File and then Properties



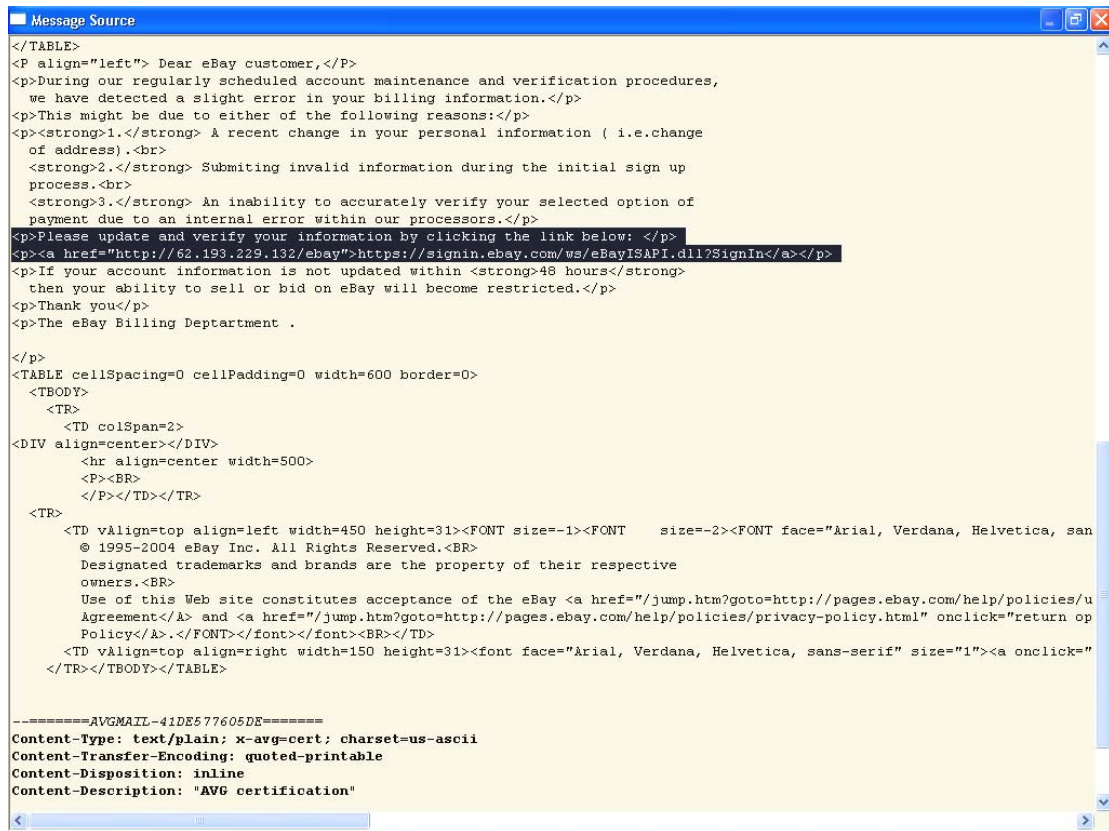
Now, click on Details



And Message Source



This will show you every single detail of the mail, all the HTML code, all the headers, where the mail originated and a whole lot more. Once you've checked all that, just close the source.



```
</TABLE>
<P align="left"> Dear eBay customer,</P>
<p>During our regularly scheduled account maintenance and verification procedures,
we have detected a slight error in your billing information.</p>
<p>This might be due to either of the following reasons:</p>
<p><strong>1.</strong> A recent change in your personal information ( i.e.change
of address).<br>
<strong>2.</strong> Submitting invalid information during the initial sign up
process.<br>
<strong>3.</strong> An inability to accurately verify your selected option of
payment due to an internal error within our processors.</p>
<p>Please update and verify your information by clicking the link below: </p>
<p><a href="http://62.193.229.132/ebay">https://signin.ebay.com/ws/eBayISAPI.dll?SignIn</a></p>
<p>If your account information is not updated within <strong>48 hours</strong>
then your ability to sell or bid on eBay will become restricted.</p>
<p>Thank you</p>
<p>The eBay Billing Department .

</p>
<TABLE cellSpacing=0 cellPadding=0 width=600 border=0>
<TBODY>
<TR>
<TD colspan=2>
<DIV align=center></DIV>
<hr align=center width=500>
<P><BR>
</P></TD></TR>
<TR>
<TD valign=top align=left width=450 height=31><FONT size=-1><FONT size=-2><FONT face="Arial, Verdana, Helvetica, san
@ 1995-2004 eBay Inc. All Rights Reserved.<BR>
Designated trademarks and brands are the property of their respective
owners.<BR>
Use of this Web site constitutes acceptance of the eBay <a href="/jump.htm?goto=http://pages.ebay.com/help/policies/u
Agreement/> and <a href="/jump.htm?goto=http://pages.ebay.com/help/policies/privacy-policy.html" onclick="return op
Policy/>.</FONT></font></font><BR></TD>
<TD valign=top align=right width=150 height=31><font face="Arial, Verdana, Helvetica, sans-serif" size="1"><a onclick="
</TR></TBODY></TABLE>

-----AVGMAIL-41DE577605DE-----
Content-Type: text/plain; x-avg=cert; charset=us-ascii
Content-Transfer-Encoding: quoted-printable
Content-Disposition: inline
Content-Description: "AVG certification"
```

All in all this will probably take up 2 minutes of your time but can definitely save you thousands of pounds, dollars or whichever currency you use, so make it a habit to "deep-check" any suspicious mails that you're unsure of.

Should you EVER receive anything like this, please deep-check and report to the main websites. Never click the links in the mails. Open a new browser window and TYPE IN the web-address, making sure you include https:// so that you get to their secure pages.

Don't let them scam you!

Anna-Marie Stewart

About the Author



Anna-Marie Stewart

Anna-Marie Stewart has been involved with internet marketing since 1999. She has always tried to help people "make a go of it" online, by sharing her own experiences with as many people as possible. She started out as most marketers do, with believing the hyped up promises of riches, fame and wealth, and burnt both her fingers and toes a few times, before finally deciding that enough was enough.

She now publishes "Not Just another Ezine" a **FREE** weekly newsletter at <http://annamarketing.com> -dedicated to helping newbie and semi-pro internet marketers avoid the pitfalls BEFORE getting burnt.

Anna-Marie lives in Cardigan, Wales with her 4 children and two dogs. She enjoys reading, writing, researching, the beach, night life, walks with the family and listening to "whatever's on at the moment".

You may give away this guide as a free report, but you may not sell, alter, copy or edit any of the information within without explicit permission from the author.

Published by Anna-Marie Stewart
Editor of Not Just Another Ezine <http://annamarketing.com>
Author of Forget The Hype! <http://annamarketing.com/FTH>