



ANSWER QUEST TIP SHEET

WE ANSWER YOUR TECHNOLOGY QUESTIONS

BI-MONTHLY NEWSLETTER

SEP / OCT 2003

Who's really sending you that message?

Just because the e-mail says it came from Microsoft.com, Ebay.com or AnswerQuest.com doesn't mean it really did. Email headers can tell the story of how a message came to your mailbox. Here's how to check that out.

Do NOT open the e-mail. (Outlook 2000 is my example. But all e-mail software should have a way to view this information). Right-click on the e-mail you want to check and then click on OPTIONS. At the bottom of this dialog box you will see INTERNET HEADERS. This is the important information. Here's an example of what a REAL message header from Microsoft looks like:

```
Return-Path: <0_52663_C99372F7-427F-7948-AECC-8F9ED91CF341_US@Newsletters.Microsoft.com>
Received: from delivery.pens.Microsoft.com (delivery.pens.Microsoft.com [207.46.248.66])
    by mail.netfox.net (8.12.8/8.12.8) with ESMTP id h8MHMkRh013084
    for <llink@answerquest.com>; Mon, 22 Sep 2003 13:22:47 -0400
Received: from TK2MSFTDDSQ01 ([10.40.1.65]) by delivery.pens.Microsoft.com with
Microsoft SMTPSVC(6.0.3790.0);
    Mon, 22 Sep 2003 10:22:34 -0700
Reply-To: <3_52663_C99372F7-427F-7948-AECC-8F9ED91CF341_US@Newsletters.Microsoft.com>
From: "Microsoft" <0_52663_C99372F7-427F-7948-AECC-8F9ED91CF341_US@Newsletters.Microsoft.com>
To: <llink@answerquest.com>
Subject: Inside Office newsletter - Special Launch Events Issue
Date: Mon, 22 Sep 2003 10:22:34 -0700
Message-ID: <bdfcf01c3812e$1c6dea30$4101280a@phx.gbl>
MIME-Version: 1.0
Content-Type: text/html;
    charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
```

You can see that it's from Microsoft... but is it? You can verify this by going to <http://ww1.arin.net/whois> and type in the IP address associated with the RECEIVED IP address **207.46.248.66** verifying that is really owned by Microsoft. Then it says BY MAIL.NETFOX.NET. This is the company that hosts AnswerQuest.com's website and e-mail.

Here's an e-mail I received asking for me to update my information on eBay.com. It says it's from users-support29@ebay.com. But is it? Look at the RECEIVED line. It says host35-81.pool80117.interbusiness.it. IT is Italy. So unless eBay has moved to Italy, this isn't real! In the e-mail itself, it had a web link to go to. That web link did NOT go to eBay.com. It went to an unknown server! This was someone trying to gain information illegally.

```
Return-Path: <users-support29@eBay.com>
Received: from microsoft.com (host35-81.pool80117.interbusiness.it [80.117.81.35])
    by mail.netfox.net (8.12.8/8.12.8) with SMTP id h8JD11Rh007508
    for <llink@answerquest.com>; Fri, 19 Sep 2003 09:47:02 -0400
Date: Fri, 19 Sep 2003 13:44:29 +0000
From: eBay <users-support29@eBay.com>
Subject: Official Notice for all eBay users
To: Llink <llink@answerquest.com>
References: <E5LALL349496B226@answerquest.com>
In-Reply-To: <E5LALL349496B226@answerquest.com>
Message-ID: <DG60G2A7JC06F966@eBay.com>
Reply-To: eBay <user-suppl1@eBay.com>
Sender: eBay <users-support30@eBay.com>
```

You are receiving this newsletter because either you requested it or someone you know forwarded this newsletter to you. If you would like to discontinue receiving the Answer Quest Tip Sheet, please e-mail aqnews@answerquest.com or call (410) 538-3698.

This newsletter can not be reproduced without prior permission from Answer Quest Technologies, Inc. Copies can be made or forwarded as long as done so in the newsletter's entirety. Newsletter Archives are now available ONLINE at <http://www.answerquest.com/archive/newsletter.htm>

MIME-Version: 1.0
Content-Type: text/html
Content-Transfer-Encoding: 8bit

In the last few months, I've received probably hundreds of e-mails that BOUNCED back to me (a term that means the e-mail address that the message was addressed to is not active so it returned the message to who was in the REPLY TO field). What's the problem with this? I didn't send them!! Someone out there is sending e-mail messages from webmaster@answerquest.com and a few other e-mail addresses I use. If in doubt, do not reply to the message but instead e-mail me directly at info@answerquest.com and ask if I sent you the e-mail. The only other e-mail address you will receive from me is through bCentral.com's List Manager. Here's an example from last month's e-mail newsletter I sent to you:

```
Return-Path: <552-return-22-751298@lb.bcentral.com>
Received: from tybclbsmtpa06.PROD.TYBCENTRAL.COM (tybclbsmtpa06.listbuilder.com
[204.71.191.32])
    by mail.netfox.net (8.12.8/8.12.8) with ESMTTP id h74Go5ar015549
    for <sales@answerquest.com>; Mon, 4 Aug 2003 12:50:06 -0400
Received: from mail pickup service by tybclbsmtpa06.PROD.TYBCENTRAL.COM with Microsoft
SMTPSVC;
    Mon, 4 Aug 2003 09:49:03 -0700
Reply-To: <552-feedback-22@lb.bcentral.com>
From: Answer Quest Tip Sheet <AQTNews@lb.bcentral.com>
Sender: <552-return-22-751298@lb.bcentral.com>
To: List Member <sales@answerquest.com>
Subject: e-mail Rules - Answer Quest Tip Sheet - Jul/Aug '03
Date: Mon, 4 Aug 2003 09:48:40 -0700
MIME-Version: 1.0
Content-Type: text/plain; charset="utf-8"
Message-ID: <TYBCLBSMTPA06f4yp8A00008d1c@tybclbsmtpa06.PROD.TYBCENTRAL.COM>
```

Here are some simple rules to follow:

- Never give out personal information, credit card numbers, password, etc via e-mail. It is very **unsecured!** This means that anyone can intercept the message, gather the information and forward it on without anyone's knowledge. Companies like eBay and Paypal will NEVER ask you for information via e-mail.
- Never open a file that is supposed to be from Microsoft; they NEVER send you attachments. Microsoft will ALWAYS direct you to their website <http://windowsupdate.microsoft.com> for updates.
- Never open file attachments in an e-mail that looks suspicious or if you do not know who is sending it. This is getting MORE difficult because of viruses that pose as e-mail coming from your friends.
- ALWAYS make sure your Anti-Virus software is up to date (I use Symantec's Norton Anti-Virus on all my computers).
- ALWAYS make sure your Windows is updated by going to <http://windowsupdate.microsoft.com> for updates.
- Be careful clicking on a web link in an e-mail. You can be directed to **fake** websites! A great example is <http://www.whitehouse.gov>, which is the official White House page, but <http://www.whitehouse.net> is a spoof. Sometimes people will even go as far as copying the entire site so you cannot tell the difference except the web address.
- On the same note, ALWAYS be suspicious if an e-mail tells you to go to an IP address instead of a WEB SITE NAME. For example, <http://www.answerquest.com> 's IP address is 162.33.205.109. Every name you type in is associated with a number. But numbers do NOT have to be associated to a name! Every person who connects to the Internet has a number assigned to them and their ISP's name assigned to it. What does this mean? Instead of going to Ebay.com to update your information, you could be going to Joe Doe's home computer where he's collecting people's account passwords for illegal uses!

And finally, let Outlook help protect you. These are important option settings that need to be changed (and I'll explain why).

First, never use the PREVIEW PANE setting. It is possible with the PREVIEW PANE turned on for an e-mail message to run a program script without actually double-clicking to open the message. To turn off the PREVIEW in Outlook 2000, on the Menu toolbar - click on VIEW, click on PREVIEW PANE. Make sure the button for PREVIEW PANE is not chosen. You could leave AUTOPREVIEW on because this shows a small portion of the message as PLAIN TEXT. It's the ones that come through as web pages with HTML that can run malicious program scripts automatically.

