

Re: Help please. Outlook express or comcast is creating misleading mail headers

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.inetexplorer.ie6_outlookexpress/2004-05/1

From: N. Miller (*local.part_at_blackhole.aosake.net*)

Date: 05/06/04

Date: Thu, 6 May 2004 09:13:48 -0700

In email <01fa01c43376\$3dee4740\$1401a8c0@upstairs>, <xx> says...

{For those of you looking for the original message, it was not posted to the group, but sent directly to me. The MID\$ won't lead to a news article, because none was posted.}

> N. Miller" <nsm@blackhole.aosake.net> wrote in message
> news:MPG.1afb8dca27e2e2fa989f2e@msnews.microsoft.com...

>> Looking again at your 'bad' line with the line from my headers above in
>> direct relationship:

>> Received: from upstairs
>> (h002078d247fe.ne.client2.attbi.com[24.91.21.158])
>> by comcast.net (sccrmhc11) with SMTP
>> id <2004042915055001100mob1je>;
>> Thu, 29 Apr 2004 15:05:50 +0000

>> Received: from hal9000
>> (c-67-171-201-211.client.comcast.net[67.171.201.211])
>> by comcast.net (rwcrmhc11) with SMTP
>> id <2004021305001801300ga2qte>
>> (Authid: ,,,);
>> Fri, 13 Feb 2004 05:00:19 +0000

> What is this Authid stuff? How can I add that to my mail header? I want to
> see if that helps my problem.

It is added by "smtp.comcast.com" when the email goes through them. You have to set MSOE to "My server requires authentication". You start by going to Tools > Accounts > Mail. Highlight the name of the account, and use the "Properties" button. Go to the Servers tab; the one where you set "smtp.comcast.com", and go down to the "Outgoing Mail Server" section. There is only one choice:

[X] My server requires authentication

Yes, put a check in the box. You shouldn't have to do anything else, if you set the incoming mail server with the same login credentials as you need to authenticate to the server.

> > *If you don't have "mail.comcast.net" in the MSOE outgoing mail server field, and the server name you do have is not recognized as an ISP's SMTP server, your email may be refused by remote MX servers. You now know three that will...*

> *I use "smtp.comcast.net" which is what comcast recommends for outgoing mail. I tried mail.comcast.net (which is for incoming mail) and it didn't let me send the mail to it (unable to open port). Thanks for thinking of something to try though.*

My error. I don't use Comcast, though I know people who do. I should have said "smtp.comcast.net" in the first place. Duh—oh.

> > *BAD – doesn't get through spam filters (sent through comcast)*
> > *Received: from upstairs*
> > *(h002078d247fe.ne.client2.attbi.com[24.91.21.158])*
> > *by comcast.net (sccrmhc11) with SMTP id*
> > *<2004042915055001100mob1je>; Thu, 29 Apr 2004 15:05:50 +0000*
> >
> > *No mail service should be rejecting email on this line. See my example below. This is just a handoff from your computer to a Comcast mailhost.*

> *This is the root of the problem. I know for sure that this is the part of the mail header that is being rejected because I have a detailed report from an ISP's spam filter report and this is the only part of my mail that the spam filter has a problem with. Yes, it is just a handoff, but they seem to think I am running a mailhost program and not using outlook express. In the old days my ip address never showed up in the mail headers, but the smtp mail host that comcast uses now includes that in all mail headers. That is a good thing in that it helps keep track of where the mail came from, but bad in that they make me look like a mailhost.*

Okay. Here are the complete headers, with email addresses munged for protection, of that example I gave above:

> *Return-path: <,,,@hotmail.com>*
> *Received: from rwormhc11.comcast.net (204.127.198.35) by aosake.net (Mercury/32 v4.01a) with ESMTP ID MG000004;*
> *12 Feb 2004 21:00:14 -0800*
> *Received: from hal9000 (c-67-171-201-211.client.comcast.net[67.171.201.211])*
> *by comcast.net (rwormhc11) with SMTP*
> *id <2004021305001801300ga2qte>*
> *(Authid: ,,,);*
> *Fri, 13 Feb 2004 05:00:19 +0000*
> *Message-ID: <000801c3f1ed\$fbfe5c40\$b87ba8c0@attbi.com>*

> *From: "J" <,,,@hotmail.com>*
> *To: "N" <,,,@aosake.net>*
> *Subject: wash your feet!*
> *Date: Thu, 12 Feb 2004 20:58:12 -0800*
> *MIME-Version: 1.0*
> *Content-Type: multipart/alternative;*
> *boundary="-----_NextPart_000_0005_01C3F1AA.ED227AA0"*
> *X-Priority: 3*
> *X-MSMail-Priority: Normal*
> *X-Mailer: Microsoft Outlook Express 6.00.2600.0000*
> *X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000*
> *X-PMFLAGS: 570966272 0 1 2F84EEE4.CNM*

The only part of the headers actually written by MSOE are from the "Message-ID:" to the bottom. Starting with the lower "Received:" line, and up to the "Return-Path:", the headers were written by, in order, the Comcast pick-up MTA (smtp.comcast.net), and the aosake.net MX. Incoming email filters should not be looking beyond that first "Received:" line, the one written by the MX that the filters are working for. Numerating which "Received:" line to check is not easy, once you are past the actual MX. Some receiving systems use a complex chain of internal servers; the filters have to know how to parse to the MX transaction, where the email was first received from the remote system. That is why server side filtering is better than client side filtering.

Which ISP is rejecting your messages?

> > ****Challenge/Response spam blocking****
> >
> > *****5 Trackers (what are Trackers?)*****

> *These trackers are not what you think – they are a bad name for simply*
> *email addresses that let mail go through unchallenged. I love*
> *challenge/response and besides, this email account doesn't get blocked*
> *and works great and isn't the problem. It's my comcast account that is*
> *the problem.*

Well, okay. It sounded like something to try an track whether a recipient opened their mail. There are ways to defeat that, and I make use of them. But C/R is considered unacceptable by a number of mail administrators; and, while my own domain and MTA are just a one-man hobby show, I guess running that MTA makes me a mail administrator, too. Here are some lines from my MTA filer:

> *# Challenge/Response*
> *If expression headers matches "Received: from*([166.150.163.12[89]*" Goto "Challenge/Response"*
> *If expression headers matches "Received: from*([166.150.163.1[3-8][0-9]*" Goto*
"Challenge/Response"
> *If expression headers matches "Received: from*([166.150.163.19[01]*" Goto "Challenge/Response"*

The routine labeled "Challenge/Response" logs a console message, then deletes the message. The rule was created after I received a message with the following headers:

```
> X-Apparently-To: ,,,@yahoo.com via 66.218.79.23; 02 Jun 2003 21:20:12 -0700 (PDT)
> X-YahooFilteredBulk: 66.227.18.1
> Return-Path: <x>
> Received: from 66.227.18.1 (EHLO texas.businessx.com) (66.227.18.1)
> by mta171.mail.scd.yahoo.com with SMTP; 02 Jun 2003 21:20:11 -0700 (PDT)
```

The ,,,@yahoo.com email address was forged by a spammer, making appear that I had sent the messages; even though the source IP address was not an SBC Global MTA (the ISP mailhost that I use). Idiot challenge system sent the challenge to the email address in the SMTP envelope, so this became one more bit of misery added to the 200+ idiot mail system bounces telling me that they couldn't deliver a message that I never sent. Any C/R system that just automatically sends a challenge to the SMTP envelope sender will similarly be discarded, as I find out the source MTA IP address. Someday I will run a local caching DNS server, not accessible from the Internet, and I will be able to create my own, local, DNSBLs for my MTA.

I don't block Comcast in the same manner, with client filters, because my filter is too stupid to distinguish between an internal Comcast hand off and an MTA to MX transaction; it would see the internal handoff and block the message on that. A bad thing. I can only use that kind of blocking when I know that I won't be getting email from the source IP addresses so blocked. China, India, Korea, Latin America come to mind.

Finally, your email surprised me. I had forgotten that my local part would actually work for anybody who stripped the 'blackhole' from the email address. That, plus the fact that you did not use MSOE's "Reply to Group" button, confused me. Had you just used MSOE's "Reply to Sender" button, you would have gotten my preferred email address. Oh, well. I fixed that, now.

--

Norman

~Win dain a lotica, En vai tu ri, Si lo ta

~Fin dein a loluca, En dragu a sei lain

~Vi fa-ru les shutai am, En riga-lint