

## Heading Off Spam

A Full Header; PC Magazine, 4/08/03

Spam is infuriating, but the worst thing you can do is hit the Reply button and vent your frustration on the sender. If you're lucky, the message will go nowhere. If you're not, the reply will confirm to the spammer that your e-mail address is valid, and you'll get more spam than ever.

A more effective response is to report the spam to the offender's ISP, but spammers go to great lengths to cover their tracks. This article will teach you how to identify where spam originates so you can lodge effective complaints that could shut down spammers' Web and ISP accounts.

The From: and To: fields that you see in every e-mail message represent a small portion of an e-mail's header, and both of these fields can be easily forged. To see where a message truly originated, you must view the full header. Antispam tools, such as those we reviewed in "[Slam the Spam](#)" (February 25, 2003), examine headers and other message information to identify and filter out spam, but they don't always catch everything, and they don't complain to the ISPs for you.

How you view a header depends on the e-mail client. For Outlook Express, right-click on the message, choose Properties, click on the Details tab, and then click on the Message Source button. To learn how to view full headers with other e-mail clients, visit <http://spamcop.net/fom-serve/cache/19.html>.

```
Return-Path: <Permutat@aol.com>  
Received: from smtpauth1.sover.net (mailgate1.sover.net [209.198.87.60])  
by mailhub2.sover.net (8.11.6/8.11.6) with ESMTIP id gB6E4ga10458  
for <slc@mailhub2.sover.net>; Fri, 6 Dec 2002 09:04:42 -0500 (EST)  
Received: from imo-r02.mx.aol.com (imo-r02.mx.aol.com [152.163.225.98])  
by smtpauth1.sover.net (8.11.6/8.11.6) with ESMTIP id gB6E4gD08755  
for <slc@sover.net>; Fri, 6 Dec 2002 09:04:42 -0500 (EST)  
Received: from Permutat@aol.com  
by imo-r02.mx.aol.com (mail_out_v34.13.) id 1.105.215e7ef8 (25305)  
for <slc@sover.net>; Fri, 6 Dec 2002 09:04:31 -0500 (EST)  
From: Permutat@aol.com  
Message-ID: <105.215e7ef8.2b22086e@aol.com>  
Date: Fri, 6 Dec 2002 09:04:30 EST  
Subject: normal message  
To: slc@sover.net  
MIME-Version: 1.0  
Content-Type: multipart/alternative; boundary="part1_105.215e7ef8.2b22086e_boun  
X-Mailer: AOL 7.0 for Windows US sub 10637
```

Figure 1

This is the full header for an unforged e-mail message. The highlighted sections are the most difficult to forge. They contain the clues to the source of the message.

[Figure 1](#) shows the full header for an unaltered e-mail message. The Received: block and the Message-ID: are the most difficult lines to forge, because they are added after a spam message leaves the offender's computer. These sections contain the clues to the message's source. On an unforged message, the Message-ID: line is added by the mail server that sends out the message. It usually ends with @ and the domain of the sender. In this example, the sender is Permutat@aol.com, and the Message-ID: ends with @aol.com. When the domain names in these two fields don't match, it's a sign that the sender is trying to remain anonymous.

The Received: block is the most revealing portion of the header. Most messages pass through at least three computers before arriving at the recipient's machine: the sender's computer, the sending mail server, and the recipient's mail server, from which the recipient retrieves the message. With more complicated setups—those with firewalls, for example—the message will pass through even more stops.

Every machine the message passes through adds a Received: line. The lines are added from bottom to top, so the top-most line is the last stop the message made. Because the Received: lines reveal exactly where a message has been, spammers sometimes try to confuse matters by adding fake Received: lines to their messages. Any forged Received: lines appear at the bottom of the list.

### **Decoding the Received: Block**

The server name in the from clause of the Received: line can be forged easily, but receiving mail servers can check the true identity through reverse DNS, which shows the sending server's IP address. The IP address results appear in parentheses after the server name entered by the sender, which with spam is almost always forged. You can look up the IP address of the named server (more on this later) to see whether the data in the header is accurate or forged.

Read the Received: block from the bottom up until you find the injection point—the last forged line—which is where a message enters the Internet stream. This is generally the last line where the IP address doesn't match the server name. Most of the lines below the injection point are forgeries, although sometimes the line just below the injection point reveals the spammer's dial-up ISP.

To find the domain name associated with the IP address, you'll need a whois utility. Note that there are three whois databases to check, each for a different part of the world. A search at Geektools checks all three ([www.geektools.com/cgi-bin/proxy.cgi](http://www.geektools.com/cgi-bin/proxy.cgi)).

Before filing a complaint, you should visit the Web site of the party that sent out the spam. Sometimes it belongs to a company that's in the business of sending spam, and complaining won't help. In this case, use a traceroute utility (again entering the IP address) to find the next service provider up in the chain and send your complaint there. You'll find a good traceroute utility at <http://samspade.org/t>.

If you want someone else to do the legwork, sign up for SpamCop's free reporting service: <http://spamcop.net/anonsignup.shtml>. You just copy the full header and text of the spam into an edit box and click a button. SpamCop figures out where the message came from, tests the servers it finds to determine whether they are open relays (servers that send e-mail from any source), and composes complaint messages to all the correct parties. You review the suggested addresses for sending complaints, uncheck any you think are incorrect, and hit the Send button.

There's another benefit to reporting e-mail abuse—besides the double satisfaction of revenge and promoting the greater good. Spammers use suppression lists for people who cause problems. If you get a reputation as someone who will complain to the authorities, you may actually start to see a decrease in your spam.

[Subscribe to PC Magazine](#)