

How to Find the Spammer's ISP

Another important tool is to complain to the spammer's ISP. ISPs will be glad to take action against spammers as most have rules against using their networks to send spam. Since spammers routinely send out millions of e-mails, an ISP's network can become overwhelmed and can slow down or fail as a result. Also, when complaints start coming in from those who were spammed, ISPs are alerted to the fact that their network was used inappropriately and often cut the spammer off immediately.

What is a Full Header?

An e-mail message is divided into two parts, the "header" and the "body." **Headers** contain all the technical information, such as who the sender and recipient are, and what intermediate computer systems the message passed through on its way to the recipient's mailbox.

The **body** contains the actual message. A blank line typically separates the header and body. In some mail programs, the headers are shown separately. Most people are only familiar with "friendly" e-mail headers – these are what you see in your mail program – typically the "To:" and "From:" lines. However, there is a lot of useful information beyond the "friendly header" contained in the "full header."

Example of a **friendly header**:

From: Smith_Poll@smbpol.grcc.com
Reply: Smith_Poll@smbol.grcc.com
Subject: Smith Online Poll Activity Survey

Example of a **full header**: (You will need to include the full header information in the junk email complaint form.)

Received: from slave2 for slipry
with Cubic Zirconium's Puppipop (v1.18a 1996/12/26 VIRTUAL) Tue Feb 1 06:58:50
2000
X-From_: owner-nolist-bounces*SLIPRY**AJ*-NET@HEROES.GRCC.COM Mon Jan 31
05:50:14 2000
Return-Path:
Received: from saturn.grcc.com ([255.255.255.1])
by slaveZ.AJ.net (8.9#.8/8.9#.5) with ESMT PJ id FAC18108
for ; Mon, 31 Jan 2000 05:50:14 -0800
X-Intended-For:
Message-Id: <2000013111350.FAA18108@slave1.aa.net>
Received: from heroes (heroes.grcc.com) by saturn.grcc.com (LSMTP for Windows NT
v1.1b) with SMTP id <1.00134977@saturn.grcc.com>; Mon, 31 Jan 2000 8:41:30 -
0500
Date: Mon, 31 Jan 2000 08:28:43 -0500
From: Smith_Poll@smbol.grcc.com
Reply: Smith_Poll@smbol.grcc.com
Subject: Smith Online Poll Activity Survey
To: SLIPRY@AJ.NET

How do I Find the Full Header?

In order to retrieve the full header you need to determine what e-mail program you use and how to extract a message's full header. Below is a list of commonly used e-mail programs and the methods built into each one to obtain full header information from e-mail messages. If your e-mail program is not listed, you may need to contact your e-mail program's technical support for help.

Elm, Pine, and Mutt	:	Press "h" from the message selection menu to view the full headers of the currently selected message.
Eudora	:	Open the message. Under the title bar are four options. The second from the left is a dialog box - click on that to display the full headers.
Hotmail	:	Go into "Options," "Preferences," and choose "Message headers." You'll want to choose the "Full" option to display Received: headers. "Advanced" will display that as well as MIME headers. Note: sometimes Hotmail uses older mail servers Messages sent through those mail servers won't show any headers.
Lotus Notes 4.6.x	:	Open the offending mail. Click on "Actions," then "Delivery information." Cut and paste the text from the bottom box, marked "Delivery information."
Netscape Mail	:	Choose "OPTIONS" from the options menu bar. Listed as an option is "Show Headers." Choose full headers.
Outlook Express	:	While viewing the e-mail message, select the menu item "File" then "Properties." When the dialog box pops up, select the "Details" tab, which will show header information only. Select the "Message Source" button, which will display the entire e-mail message, including headers and body.
Microsoft Outlook 97	:	While viewing the e-mail message, select the "Options" folder tab at the top of the message frame. This will show you the routing information of the message. For e-mail complaint purposes, first begin composing your message, then copy and paste this routing information, then switch back to the message window and copy the message and paste it in below the routing information
Outlook 2000	:	Double click on the message to open it up, click on "View", then "Options", and you will see the message headers in a box at the bottom of the window. You can copy/paste them from that window.
Forte' Agent	:	While in Agent, Click the "select Message option, "header, and "all." This displays all header information within the e-mail itself. You can then cut and paste as necessary.
Forte'Free Agent	:	While in Agent, Click the "select Message option, "header," and "all." This displays all header information within the e-mail itself. You can then cut and paste as necessary.
Pegasus	:	Choose "Reader" from the options menu bar. Listed as an

option is "Show all Headers." This does not work for HTML messages, however. To view header information in HTML messages, select the message properties, and uncheck "Contains HTML data."

Now that I have the Header, How do I Track the Spammer?

In the header, e-mail leaves evidence of each intermediate step it took in its journey from the sender to your e-mail box. Much like a passport, the header contains a stamp of every network the e-mail message passed through on its journey.

In the example below, look at the "Received lines" in the header and read from top to bottom:

To: waconsumer@anyone.com

Received: from relay.somebodyelse.com (upandup5.somebodyelse.com [123.45.67.8]) by anyone.com with SMTP id WAA12684 for < waconsumer@anyone.com >; Sun, 01 Oct 2000 23:03:08 -0800

Received: from forged.example.com (ima.spammer.com [23.45.67.89]) by relay.somebodyelse.com (8.8.3/8.8.3) with SMTP id GAA02044 for < waconsumer@anyone.com >; Sun, 01 Oct 2000 01:23:46 -0500

What it means: Your e-mail address (in the "To" field) received this message from upandup5.somebodyelse.com (the entry in the first "received" field). It received the message from ima.spammer.com (the entry in the second "received" field). Intermediate sites, such as somebodyelse.com in this example, may simply be sites that allow anyone to forward mail using their mailer. Don't assume they are connected with the spammer or the spammer's provider. Nevertheless, you might want to let them know their system is being used for this purpose.

With experience, you will learn more about Received lines, and the ways that they can vary. But the basic principle is still to read them from top to bottom, and to understand that each computer that handled the message – the sender, the receiver and all in between --added a Received line to the header.

Once you've tracked down a spammer's ISP, you can get contact information by using the methods described earlier and forward the spam to them directly. Or, you can find out if the ISP has an e-mail address specifically to report spammers.

With this information, you should now be better equipped to do your own cyber-sleuthing. You might also search the web for anti-spam websites, spam newsgroups, and other related resources to report violators or to simply gain other helpful information.