

# I don't like Spam!

Bob Avery-Babel - 2003

So you want to get rid of the spam in your mailbox? If your email is not filtered at the server level there are other things you can do to minimize the spam you receive:

Probably the best way to stop spam entirely is to get a different email address and then guard that email address. Don't use it to subscribe to lists, don't post it anywhere on a public web page.

I often have one email account that I use to sign up for everything with. I get spam in that email account, but not in my other accounts.

Do Not Unsubscribe from "Mysterious Mailing Lists"

You know when you subscribe to a mailing list. If you receive something that says "click here" to unsubscribe, don't do it. It is a trap. If you click on the unsubscribe link and fill out the information the spammers will know they have a live email address! Only unsubscribe from lists that you know you are on, and remember subscribing to in the past.

Be aware of how you use your email address

If you post to newsgroups, and post your email address online it will be picked up by spammers. Again, you might not want to use your primary email address in public forums or newsgroups. Try searching for email addresses in a search engine like google.com sometime. If you are going to put your email address on a web page for contact information there are ways to encrypt your email address so it is harder for the spammers to figure it out.

Filtering Spam out of your inbox

Most email programs have the ability to filter by subject line, sender, and many other ways. Check out the features of your email client for more information on that. Email can be filtered and sent right to the trash bin or to a location you decide.

Who Sent this Spam to Me? It looks like I sent it to myself!

Spammers use all sorts of awful techniques to disguise junk email. Almost every part of an email message can be changed or hidden. The spammers may change the "received from" field to anything they want.

You can see who really sent the spam to you by looking at the headers of the message. Be warned, sometimes even headers can be faked. Also, if you determine where the spam came from, it might not even be the fault of that party. They may have had their mail servers cracked open by spammers to relay spam through.

So, you want to look at the headers of a message so you can trace the path from which the spam came from. Every email program has the ability to view the headers of the message. To find out how to look at the headers of each email program please visit this link:

<http://www.haltabuse.org/help/headers/index.shtml>

You can also check the headers of email messages to see the IP addresses of where they are coming from. They you can contact the ISP of the IP address and complain directly to the provider. The Internet Service provider may want to see an original copy of the email message itself with headers in tact.

What a header looks like:

Received: from tranq1.tranquility.net [206.156.230.1] by mail.adminsites.com with ESMTP

(SMTPD32-6.06 EVAL) id A995FE60100; Thu, 09 Jan 2003 06:39:17 -0800

Received: from somename ([206.152.67.154])

by tranq1.tranquility.net (8.11.1/8.11.1) with SMTP id h09EfGR40137

for <Bob@yellowbugcomputers.com>; Thu, 9 Jan 2003 08:41:16 -0600 (CST)

(envelope-from someone@someone.net)

Message-ID: <001001c2b7ed\$295eb540\$6700a8c0@someone.net>

Reply-To: "some name" <someone@someone.net>

From: "some name" <someone@someone.net>

To: "Bob Avery-Babel" <Bob@yellowbugcomputers.com>

Above, you can see that the original request came to IP address: 206.156.230.1 ( a Mail Server most likely) from: 206.152.67.154 (an actual user's machine). The mail was then delivered to the recipient's mail server: mail.adminsites.com, and was received by the recipient bob@yellowbugcomputers.com.

Who do these IP addresses belong to, so I know who to contact?

Visit <http://www.arin.net/whois/index.html> and type in the IP address that you are trying to locate. You should now have some contact information at your fingertips.

If you don't get any resolution with the Internet Service Provider you can also report them to a Blacklist for spam testing.

What is a blacklist?

A black list is a huge list of sites that are open mail relays, this means that they are misconfigured and let spam through to your mailbox. When an email server is identified as allowing spam through, it first is tested. If it is determined to be an "open mail relay" for spam it will then be placed on the black list.

Email servers can subscribe to these blacklists. If mail comes in to a mail server that has subscribed, the mail is checked against the lists, if it matches as coming from an open mail relay, it is dropped and not passed on to the intended recipient.

So, if you report an IP address to a black list there is a good chance it may get listed, and spam may stop coming from it.

One of the major black list websites can be found here:

<http://relays.osirusoft.com>

Can I block spam at my mail server?

There are ways to block spam at the server level. Server administrators can use the above mentioned black lists to filter spam. Each Mail server product also has various methods for blocking spam including blocking by standard mail delivery rules, and also blocking by keyword. Be sure to learn about the various functions of you mail server to maximize its use of spam filtering.

What are some other resources?

More on Black lists: <http://mail-abuse.org/rbl/usage.html>

Ways to track down who sent you spam: <http://www.more.net/security/spam.html>

<http://spamcop.net>

<http://www.spamrecycle.com>

Write your member of Congress! - <http://www.congress.org>