# *Step by Step Mail Relay Test*

## Email Relary Test - How To

An outside individual who uses your mail server to deliver email using a false email address is considered relaying mail via your server. A mail server that allows relaying is usually considered to be setup incorrectly and is frequently abused by spammers.  These spammers find and use unsecured mail servers to send out unsolicited commercial email.

Tracking down a spammer who uses mail servers open to relaying is difficult.  This is because the email appears to be coming from your server, rather than from the original sender. Such spam being delivered by your mail server can give your company a bad reputation.

How do you check your server for relaying?  Easy, just use a computer outside of your organization and type the commands included in the tables below - you'll want to do this from a command prompt.

In the following examples, mail.example.com is the mail server you are checking, sender@example.com  is a valid email account at mail.example.com (or a fake email address - try both), and youremail@outsideaddress.com is the email account you want this message to go to.

The parts you type are show in the table blow and replies from the server are shown to the right.  This is an example of a mail server that does NOT allow relaying.

```
telnet server01 25

HELO server01

MAIL FROM: hacking@creaking.nl

RCPT TO: ruudb@arcadenetwerken.nl

DATA <CRLF>

Blah Blah Blah

<CRLF>.<CRLF>

QUIT
```

| You type this text | Server should respond with this |
|---|---|
| **TELNET mail.example.com 25** | Trying 10.10.10.1.<br>Connected to mail.example.com.<br>Escape character is '^]'.<br>220 mail.example.com |
| **HELO mail.example** | *250 OK* |
| **MAIL FROM:<sender@example.com>** | *250 OK - Mail from <sender@example.com>* |
| **RCPT TO:<youremail@outsideaddress.com>** | *550 Relaying is prohibited* |
| **QUIT** | 221 Closing connect, good bye |

This is an example of a mail server that DOES allow relaying.

| You type this text | Server should respond with this |
|---|---|
| **TELNET mail.example.com 25** | Trying 10.10.10.1.<br>Connected to mail.example.com.<br>Escape character is '^]'.<br>220 mail.example.com |
| **HELO mail.example** | *250 OK* |
| **MAIL FROM:<sender@example.com>** | *250 OK - Mail from <sender@example.com>* |
| **RCPT TO:<youremail@outsideaddress.com>** | *250 OK* |
| **DATA** | 354 End data with <CR><LF><CR><LF> |
| **From: sender@example.com**<br>**To: youremail@outsideaddress.com**<br>**Subject: Relay test**<br><br>**This is a relay test and only a test.**<br>(type <CR><LF>.<CR><LF> or [enter].[enter] to end data) | 250 OK: Queued as T22122A5 |
| **QUIT** | 221 Closing connect, good bye |

### *How do you prevent message relay if using MS Exchange?*

Before you start, check which version you are running - you must be running Microsoft Exchange Server 5.5 or greater, then follow these 7 steps.

1) Go to the Internet Mail Service Properties dialog box in Microsoft Exchange
2) Select the Routing tab at the top.
3) Select the option Reroute incoming SMTP mail (required for POP3/IMAP4 support).
4) Reroute incoming SMTP mail.
5) For each domain you host, you need an entry in the Routing section.
6) Click the Routing Restrictions button.

7) Make sure Hosts and clients with these IP addresses is checked. Leave the list of IP addresses blank.

Microsoft knowledge base has more information at http://support.microsoft.com/?kbid=304897

**Spam**

Most of us get spam every day. Some of us get a little, and some of us get a lot, but if you have an e-mail account it is always there. For example, this morning, here's one that came to my inbox:

> Subject: Adobe
>
> Suppose we tell you that you could really lose up to 82% of your unwanted body fat and keep it off in just a few months, would you be interested? We certainly hope so! Please visit our web site - Click here!

Obviously this is spam, yet it made it through the spam filters and I opened it because the subject line made it unknowable whether it was spam or not.

Spam is incredibly annoying, especially in large quantities. If you have a public e-mail address you can receive hundreds of spam messages for every legitimate message that arrives. Even with good filters, some of the spam makes it through. And filters can sometimes delete messages that you really do want to receive. Spam is free speech run amok.

Where does all of this spam e-mail (also known as "unsolicited commercial e-mail") come from? Why is there so much of it? Is there any way to stop it? In this article, we will answer these questions and many others as we take a dive into the sea of spam.

# The Source of Spam

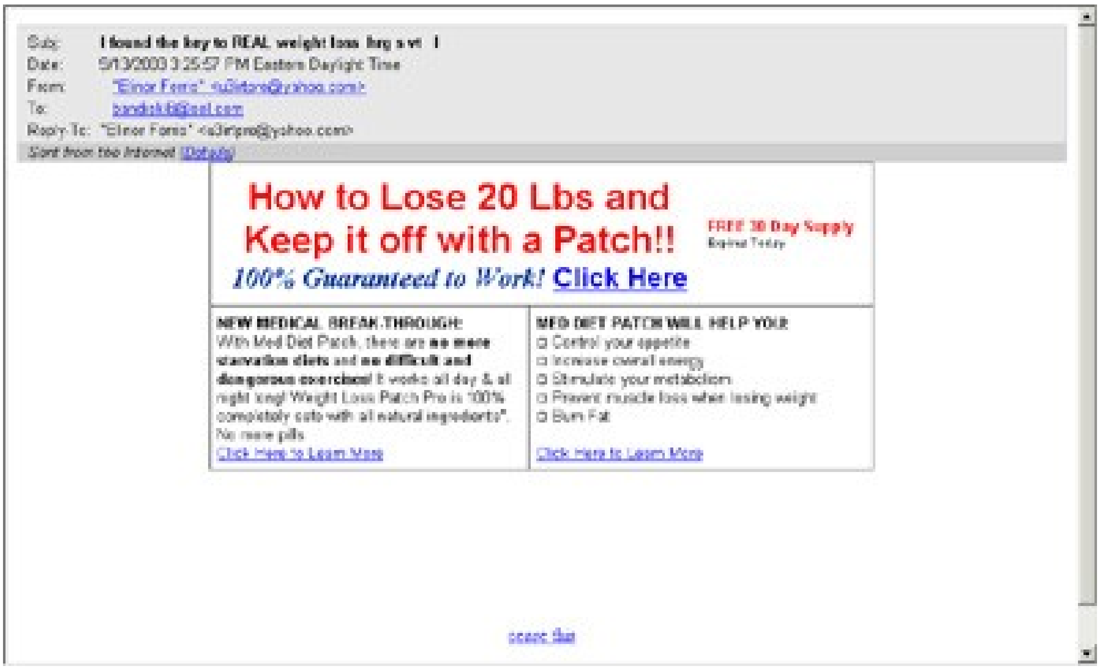
### As in, the Meat?

Where did the name "spam" come from? See Templetons.com to find out!

Spam is a huge problem for anyone who gets e-mail. According to Business Week magazine:

> In a single day in May [2003], No. 1 Internet service provider AOL Time Warner (AOL ) blocked 2 billion spam messages -- 88 per subscriber -- from hitting its customers' e-mail accounts. Microsoft (MSFT), which operates No. 2 Internet service provider MSN plus e-mail service Hotmail, says it blocks an average of 2.4 billion spams per day. According to research firm Radicati Group in Palo Alto, Calif., spam is expected to account for 45% of the 10.9 trillion messages sent around the world in 2003.

One of the problems with spam, and the reason why there is so much of it, is that it is so easy to create.



Subj: I found the key to REAL weight loss [illegible]
Date: 5/13/2003 3:25:57 PM Eastern Daylight Time
From: "Elnor Ferns" <[illegible]@yahoo.com>
To: [illegible]@aol.com
Reply To: "Elnor Ferns" <[illegible]@yahoo.com>
Sent from the Internet (Details)

How to Lose 20 Lbs and Keep it off with a Patch!!

100% Guaranteed to Work! Click Here

FREE 30 Day Supply
Expires Today

**NEW MEDICAL BREAK-THROUGH:**
With Med Diet Patch, there are **no more starvation diets** and **no difficult and dangerous exercises!** It works all day & all night long! Weight Loss Patch Pro is 100% completely safe with all natural ingredients*. No more pills
Click Here to Learn More

**MED DIET PATCH WILL HELP YOU:**
□ Control your appetite
□ Increase overall energy
□ Stimulate your metabolism
□ Prevent muscle loss when losing weight
□ Burn Fat

Click Here to Learn More

[illegible]

You could easily become a spammer yourself. Let's say that you have a recipe from your grandmother for the best blueberry muffins ever created. A friend suggests that you sell the recipe for $5.

You decide that your friend might be on to something, so you send an e-mail to the 100 people in your personal e-mail address book with the subject line, "These Blueberry Muffins Have Been Described as Heaven -- You Can Have the Recipe for $5!" Your e-mail contains a link to your blueberry muffin Web site. As a result of your 100 e-mails, you get two orders and make $10.

"Wow!" you think, "It cost me nothing to send those 100 e-mails, and I made $10. If I sent 1,000 e-mails I could make $100. If I sent a million e-mails I could make $100,000! I wonder where I could get a million e-mail addresses..."

As it turns out, there are hundreds of companies that will sell you CDs filled with millions of valid e-mail addresses. With Microsoft Word you could easily format those addresses into lines of 100 addresses each, and then cut and paste those lines into the "To:" field of any normal e-mail program. Every time you push the "Send" button, which would be about once every 5 seconds, you would make $10. You would be making something like $700 per hour.

This is the problem with spam. It is incredibly easy for you to send it. It costs you practically nothing to send it. And even with a response rate as low as one sale out of 10,000 e-mails, it can be quite lucrative for you to send it. Therefore, if you don't mind the fact that you are creating e-mail pollution for millions of people, you might decide to send e-mail messages about your grandmother's muffins all day long.

## How Do They Get My Address?

Where does a company get millions of valid e-mail addresses to put on a CD and sell to you? There are a number of primary sources.

The first is newsgroups and chat rooms, especially on big sites like AOL. People (especially first-time users) often use their screen names, or leave their actual e-mail addresses, in newsgroups. Spammers use pieces of software to extract the screen names and e-mail addresses automatically.

The second source for e-mail addresses is the Web itself. There are tens of millions of Web sites, and spammers can create search engines that spider the Web specifically looking for the telltale "@" sign that indicates an e-mail address. The programs that do the spidering are often called **spambots**.

The third source is sites created specifically to attract e-mail addresses. For example, a spammer creates a site that says, "Win $1 million!!! Just type your e-mail address here!" In the past, lots of large sites also sold the e-mail addresses of their members. Or the sites created "opt-in" e-mail lists by asking, "Would you like to receive e-mail newsletters from our partners?" If you answered yes, your address was then sold to a spammer.

Probably the most common source of e-mail addresses, however, is a "dictionary" search of the e-mail servers of large e-mail hosting companies like MSN, AOL or Hotmail. In the article Hotmail: A Spammer's Paradise?, the author describes the process:

> A dictionary attack utilizes software that opens a connection to the target mail server and then rapidly submits millions of random e-mail addresses. Many of these addresses have slight variations, such as "jdoe1abc@hotmail.com" and "jdoe2def@hotmail.com." The software then records which addresses are "live," and adds those addresses to the spammer's list. These lists are typically resold to many other spammers.

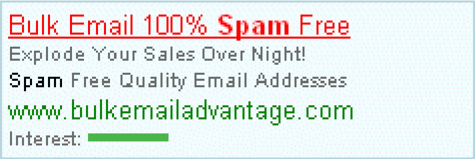
E-mail addresses generally are not private (just like your phone number is not private if it is listed in the phone book). Once a spammer gets a hold of your e-mail address and starts sharing it with other spammers, you are likely to get a lot of spam

## The Big Spamming Companies

If you would like to send a lot of spam, then there are a number of companies set up to send "bulk e-mail." The largest of these companies are able to send billions of spam e-mail messages a day. They increasingly operate out of foreign countries to avoid U.S. laws and lawsuits trying to block spam. Detroit Free Press: Spam king lives large off others' e-mail troubles describes a typical spam operation:

> The computers in Ralsky's basement control 190 e-mail servers -- 110 located in Southfield, 50 in Dallas and 30 more in Canada, China, Russia and India. Each computer, he said, is capable of sending out 650,000 messages every hour -- more than a billion a day -- routed through overseas Internet companies Ralsky said are eager to sell him bandwidth.

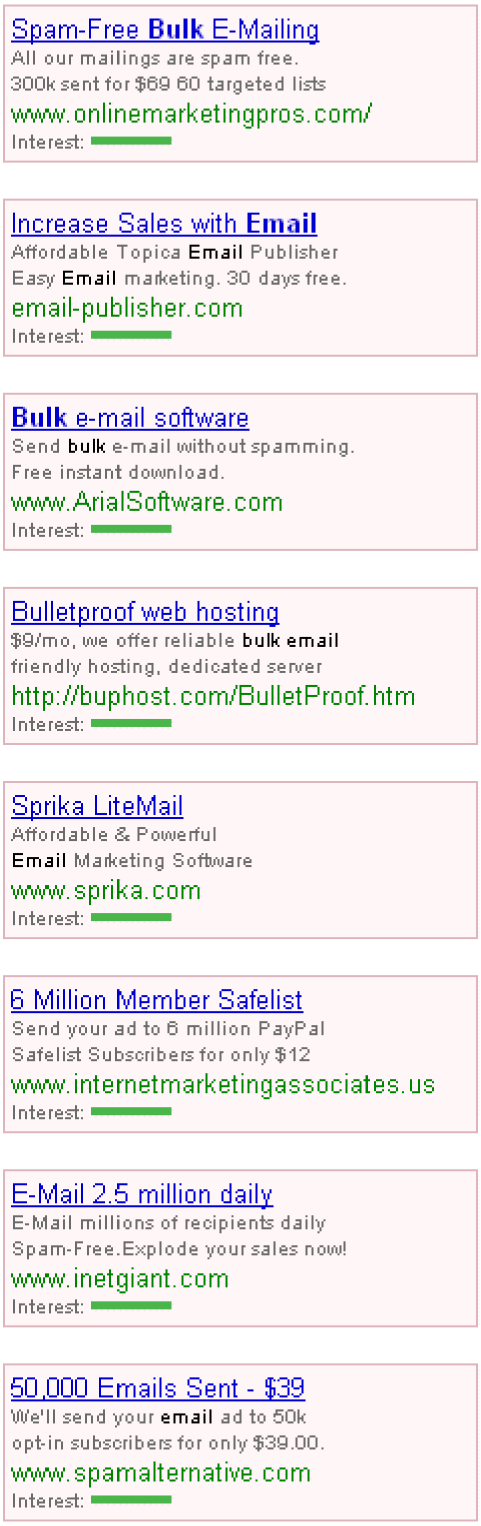
There are hundreds of companies like this. For example, here's a paid ad that appeared on Google in August 2003:



Bulk Email 100% **Spam** Free
Explode Your Sales Over Night!
**Spam** Free Quality Email Addresses
www.bulkemailadvantage.com
Interest:

The company is offering to send 500,000 e-mails for $99 and says, "Imagine emailing 500,000 recipients and 1 out of every 1,000 orders your product, that's 500 new orders!"

Similarly, if you type "bulk e-mail" as a search term in Google, you get this assortment of paid ads in late August 2003:



Spam-Free **Bulk** E-Mailing
All our mailings are spam free.
300k sent for $69 60 targeted lists
www.onlinemarketingpros.com/
Interest: ▬

Increase Sales with **Email**
Affordable Topica **Email** Publisher
Easy **Email** marketing. 30 days free.
email-publisher.com
Interest: ▬

**Bulk** e-mail software
Send **bulk** e-mail without spamming.
Free instant download.
www.ArialSoftware.com
Interest: ▬

Bulletproof web hosting
$9/mo, we offer reliable **bulk email**
friendly hosting, dedicated server
http://buphost.com/BulletProof.htm
Interest: ▬

Sprika LiteMail
Affordable & Powerful
**Email** Marketing Software
www.sprika.com
Interest: ▬

6 Million Member Safelist
Send your ad to 6 million PayPal
Safelist Subscribers for only $12
www.internetmarketingassociates.us
Interest: ▬

E-Mail 2.5 million daily
E-Mail millions of recipients daily
Spam-Free.Explode your sales now!
www.inetgiant.com
Interest: ▬

50,000 Emails Sent - $39
We'll send your **email** ad to 50k
opt-in subscribers for only $39.00.
www.spamalternative.com
Interest: ▬

## Stopping Spam

The best technology that is currently available to stop spam is **spam filtering software**. The simplest filters use keywords such as "sex,", "xxx," "viagra," etc., in the subject line to attempt to identify and delete spam. These simple filters are easy to sidestep by spelling "sex" as "s-e-x." There are, of course, thousands of ways to spell "sex" if you are willing to add extra characters like that, and it is difficult for the simple filters to keep up.

Also, simple filters are most likely to block "real" e-mail that you do want to receive. For example, if your friend sends you her favorite recipe for baked chicken breasts, the filter blocks the e-mail because of the word "breasts."

More advanced filters, known as heuristic filters and Bayesian filters, try to take this simple approach quite a bit further to statistically identify spam based on word patterns or word frequency. But there are still ways to get around them (mainly by using short messages).

Large ISPs tried blocking multiple e-mails with the same subject line or message body. This had the unwanted side-effect of blocking e-mail newsletters, so ISPs made "white lists" to identify legitimate newsletter senders. Then spammers sidestepped the issue by inserting different random characters into each subject line and message body. That's why you get e-mail messages with subject lines like:

**Women Wanted puklq**

The word "puklq" is random, and it is different on every e-mail the spammer sends.

There are several organizations that publish lists of IP addresses that are used by spammers. Any large spammer will have an array of server machines blasting out spam messages, and each server machine has its own IP address. Once spam is detected from an IP address, that IP address is put in a list (Spamhaus.org is one of many organizations that maintain such lists). Companies that host e-mail accounts can look at the sending IP address of every e-mail and filter out those that appear in the Spamhaus.org list.

Spammers get around this approach in two different ways. First, they change their IP addresses frequently. The unfortunate problem with this approach is that the old IP addresses that spammers discard get recycled, and the people who get these discarded IP addresses find them to be useless -- they are tainted by their former association with spam, and cannot be used for sending legitimate e-mail.

Lately, spammers have started to get more aggressive. For example, it is thought that recent viruses like SoBig.F were sent out specifically to recruit "zombie machines" for spammers. The **zombie machines** are generally personal computers owned by unsuspecting private citizens who happened to contract the SoBig virus. The virus opens their machine up to spammers, who can then route spam e-mails through their machines. Since the IP addresses of these machines are new, they do not appear in the IP address blacklists and millions of spam e-mails can route through them before they get blacklisted. The zombie machines have also been uses for denial of service attacks on places like Spamhaus.org.

Another front in the war against spam is legislation. For example, it has been suggested that the U.S. federal government set up a national "do not spam" list identical to the national Do Not Call list designed to block telemarketers. However, it is believed by most people that spammers are so obnoxious that they would set up spam servers in foreign countries and actually use the "do not spam" list as a source of fresh e-mail addresses.

Another solution would be an "opt-in" list. Under this proposal, only those people who specifically request spam e-mail would get it. However, the United States congress seems to be heading in the opposite direction. As noted on Spamhaus.org:

> With all of Europe set to implement Opt-in legislation by October, Europe has taken the lead in banning spam. But the United States is going in the opposite direction, legislating Opt-out instead of Opt-in and looks set to explode the spam problem many times worse than it is today, incredibly by actually legalizing spam instead of banning it. US Congress is just months away from giving Unsolicited Bulk e-mail the green light and unleashing the spamming power of 23 Million American businesses onto an Internet which already can not cope with the billions of unsolicited bulk mailings sent by just 200 businesses. As spammers applaud the introduction of pro-spam Bills, we look at why spammers now cheer so loudly for Congressman Billy Tauzin.

The final front in the war on spam is the elimination of e-mail in the traditional sense. Many businesses are being forced to take this approach. Even the White House has been forced to follow this path. Today, if you want to send e-mail to the president of the United States, you do it by filling out an online form. Even HowStuffWorks has been forced to use forms. It used to be that you could send e-mail directly to individual HowStuffWorks staff and departments, but those e-mail addresses started to receive so much spam that we now use a set of online forms, instead.

That may be what happens to all e-mail in the long run. The amount of spam, and the inability to control that spam, may become so unmanageable that the traditional e-mail system we know today collapses and gets replaced either with forms or with a set of advanced, secure servers that put spammers out of business.

For more information on spam and related topics, check out the links on the next page

All of these vendors are claiming that they are "spam-free." That is, they claim that they use e-mail lists where the recipients have specifically requested to receive bulk e-mail. This is often referred to "opt-in" e-mail. You may have ordered a product or filled out an online form that had a checkbox at the bottom that said, "Please unclick this check box if you would not like to receive e-mail from our partners," or something to that effect. You either did not see that checkbox because it was way at the bottom of the form, or you misread it. If your name gets onto the wrong opt-in lists, then you will receive a great deal of spam.

- Templetons.com: Reflections on the 25th Anniversary of Spam
- Templetons.com: Origin of the term "spam" to mean net abuse"
- Paul Graham: A Plan for Spam
- GetIT: Controlling spam
- 2004 Spam Conference
- InternetWeek: FCC Cans Wireless Spam - 8/5/04
- BBC News: Viagra spam forces legal action - 8/5/04
- PCWorld.com: Sobig May Be Working for Spammers - 8/29/03
- OrlandoWeekly.com: Spammed if you do. Spammed if you don't. - 8/28/03
- Silicon.com: Anti-spam firm sued by pork-product firm over word 'spam' - 7/03/03
- BusinessWeek.com: Before Spam Brings the Web to Its Knees - 6/10/03
- Ezine-Tips.com: Hotmail to Block Email Graphics - 5/08/03
- Mike Wendland: Spam king lives large off others' e-mail troubles - 11/22/02