

This Free E-Book is brought to you by Natural-Aging.com.

100% Effective Natural Hormone Treatment
Menopause, Andropause And Other Hormone Imbalances
Impair Healthy Healing In People Over The Age Of 30!

Black Hole Lists

By Richard Lowe

Black Hole Lists by Richard Lowe

When you send an email across the internet, you must first log into your ISP's email system. Generally, you set the login information (username and password) in some setup screen, then quickly forget about it. However, behind the scenes your username and password are used to log in each and every time you send email.

When the email system receives your message it opens a connection to the recipient email system and delivers the message. This is the way email normally works, at least on properly configured email systems.

Unfortunately, many emails systems are not properly configured (or have older, buggy software). These systems have become the bane of the internet and are one of the primary reasons that spam is so hard to fight.

These email servers are known as open relays. You see, email systems also have the ability to send messages to one another. This is known as relaying. In the good old days of the internet, back when it was a small network of universities and military installations, spam was not a significant issue. During those innocent times, there was little security because there were not many offenders. Thus, email systems did not protect themselves very well.

What is there to protect against? Spammers use open relay systems to hide their identity. What happens is simple. A spammer sends messages using one of these open relay systems and bypasses the normal security. The spammer is basically hijacking the email

Black Hole Lists

server to do his dirty work for him.

You see, email messages are actually enclosed in an electronic envelope which identifies where the message came from. So if a spammer sends a message through his own ISP's email server, then it could be tracked back to him because he has an account on that server.

However, if he hijacks an open relay, he can send all of the messages that he wants without worrying about being tracked. The email message identifies the open relay as the system where the email came from; however, the spammer is not a legitimate user.

The open relay does not (unless it goes to great lengths) have a clue where the messages came from.

A spammer must rub his hands together in glee when he finds one of these systems. I can just imagine the evil laugh as the spammer presses the return key to send literally hundreds of thousands or even millions of messages through the open relay system.

This cannot happen on a properly configured, secured and patched email server.

Open relays are a big problem, and to combat that problem a number of services have appeared. These are called Blackhole Lists, and what they do is simply list all of the open relays that they know about. ISPs and others can subscribe to these lists and use them to block email messages.

Here's the process. A system is determined to be an open relay. It is added to one or more Blackhole lists. ISPs that subscribe to the lists will bounce (return to sender) any messages that originate from the open relay email system. This means ALL users from that email system are blocked. Every single one of them.

I know that seems cruel, but look at it this way. The open relay is encouraging spammers and is an unwitting accomplice in their operations. In fact, many of these open relays do not even know they are causing a problem, and the first inkling that they get is when their users complain that things are running slowly or when problems occur with their servers.

The Blackhole lists are often run by individuals or small groups who believe in the anti-spam cause. They are often unpaid

Black Hole Lists

volunteers who simply want to help clean up the internet. They are also extraordinarily successful and many ISPs use their services.

To give you an idea of how successful this approach has been, there was a blackhole list called ORBZ. This was run by a young man named Ian Gulliver, a 20-year-old systems administrator from Ghent, New York. Ian is an extraordinary person and created one of the most successful blackhole lists ever.

What ORBZ did is send messages to email systems to determine if they were open relays. If it determined that the email system had this problem it added it to its list. This was very successful until the end of March, 2002.

At that time, ORBZ probed the email server of Battle Creek, MI. Unfortunately, this system used the Lotus email system, which has

a known bug. The probe caused the email server to slow down considerably, and it was interpreted by the city as a hacker attack.

The poor ORBZ administrator found himself the subject of a search warrant signed by a Michigan judge that authorized the search and seizure of all data relating to ORBZ accounts.

Ian almost immediately shut down the ORBZ system (he reopened the service a few days later with some major changes and a new name), which led directly to a huge amount of spam suddenly being received all over the internet. The closure of a single blackhole list had dramatic and noticeable results.

The upside is that blackhole lists prevent a tremendous amount of spam from getting sent throughout the internet. They are very efficient and the concept is simple and straightforward.

On the downside, blackhole lists are not governed by anyone and answer to no one. They add open relays (and other spam sources) to their lists using their own rules, and usually assume the suspected spammer is guilty until proven innocent.

They are, however, a necessary and vital piece in the war against spam.

Richard Lowe Jr. is the webmaster of Internet Tips And Secrets at <http://www.internet-tips.net> – Visit

our website any time to read over 1,000 complete FREE articles about how to improve your internet profits, enjoyment and knowledge.

My Emails Are Not Being Delivered. Black Lists and White Lists Explained

By Karen Fegarty

My Emails Are Not Being Delivered. Black Lists and White Lists Explained by Karen Fegarty

My Emails Are Not Being Delivered. Black Lists and White Lists Explained.

by Karen Fegarty

Over 40% of all emails within your marketing campaign are not being delivered. You may not even be aware of this, as many ISPs will not send back a bounce message. In fact if you are sending messages to AOL customers, AOL is now blocking over 80% of the messages that come into their servers.

One of the main reasons that this is occurring is that your IP or Domain may be Black Listed. All major ISP's and many corporate email systems now check against Black Lists and will refuse to deliver any emails that come from an IP that is Black Listed.

But what exactly is a Black List?

DNS black lists are lists of domains and IP's that are known to originate Spam. Many anti-spam software programs used by corporations and ISP's use these lists to control Spam by refusing any email that originates from one of these domains or IPs.

Unfortunately there are many instances of false positives as there are few checks and often little objectivity when listing a particular IP. In order for a black list to know that a domain is sending Spam, the offence must be reported. It may take only one report via a web form for you to be listed.

You may be listed maliciously through one complaint of a client, or that of a competitor. Many Black Lists, as well, will list not only the IP that is suspected as spamming, but will list any IPs in that range of addresses. If someone using the same Internet provider as you is accused of spamming and is placed on a Black List, you may be listed as well.

DNS blacklists are usually maintained by anti-spam organizations or by individuals.

What are some of the most popular Black Lists that ISPs are using?

Some of these include:

MAPS – <http://www.mail-abuse.com/>

Black Hole Lists

Spam Cop – <http://www.spamcop.net/>
SpamHaus – <http://www.spamhaus.org/>
SPEWS.org – <http://www.spews.org/>
ORDB.org – Open Relay Database – <http://www.ordb.org/>

How do I know if I am on a Black List?

Unfortunately, you really can't be 100% sure if you have been black listed. You may be on someone's black list and not even know it. There are, however, ways to check most of the lists.

One way is to check your server log when sending your campaigns. You will often see an email bounce notice indicating that the message has bounced because you are on a particular black list.

Many of the major black lists also allow you to enter your IP into a form on their site. These checks will tell you whether you appear, or not, on their list.

A useful tool, is the Black List Monitor. <http://www.blacklistmonitor.com> – It automatically checks your IP against most of the major Black Lists and tells you which ones you are listed on. It also gives you help in getting removed. All your IPs are constantly monitored for any changes, listings, or delistings.

But what is a White List and how can this help?

Many corporations and ISPs will create a white list. This is a list of trusted IP addresses that they feel confident will not send spam to their customers. If your IP is listed on a particular white list then your email messages will be delivered to the destination email address. It is important for reputable marketers to work with the major ISP's such as AOL to ensure that you are on their white list. For most, it can be a lengthy process, but well worth your efforts.

Other third-party email certification programs now exist. Bonded sender www.bondedsender.com is one such agency. By joining Bonded Sender, senders improve deliverability rates and differentiate their brand. Senders go through a formal application process, adhere to email standards and post a bond against potential complaints. Major ISPs such as MSN/Hotmail now check against Bond Sender's white list and allow these email to pass.

Knowing if you are on a black list, getting removed if you are and getting established on white lists is critical if you are email marketing. The more messages delivered equals more sales!

Author Karen Fegarty is with MailWorkZ the creator of Black ListMonitor— advanced service that continuously checks all the major blacklists for you, and then some. Don't be treatedunfairly! Keep a

handle on who may have you blacklisted. Get a free trial and find out more at <http://www.blacklistmonitor.com>.



This Free E-Book has been brought to you by Natural-Aging.com.

[100% Effective Natural Hormone Treatment](#)
Menopause, Andropause And Other Hormone Imbalances
Impair Healthy Healing In People Over The Age Of 30!