

## Relay Black Lists (RBL)

Although there are slight variations, at a high-level RBL's work pretty much the same. Their goal is to dis-allow spammers, individuals, or machines known to distribute SPAM from being able to send e-mail on the internet.

At a very high-level, here is how it works:

A individual or company that sends out SPAM or mass mailings typically does not want to be identified directly. In order to accomplish this, they obfuscate information in the e-mail. This is done in several ways:

- They modify the 'FROM' and field and some other SMTP fields of an e-mail so that replies can not be sent back to them and identification is very difficult. Accomplishing this is a trivial exercise and in today's world there are thousands of free programs that will do this for individuals. As such, you do not have to be technical at all to accomplish this. With these fields modified, locating the individual, company, or their e-mail address becomes very difficult. Often, they provide you with an URL to a website, where you can 'order' some product or service however there is no way to contact them directly.
- They find other servers which 'relay' messages. When they send a mass mailing, actually direct the mail to one or more of these relay servers. These servers then send the message to their destinations. This further obfuscates the origin of the messages. Causing any investigation to determine the source of the mailings to be targeted to the wrong individuals and companies.

When your e-mail server / service or SPAM server /service uses and RBL the following happens during the transmission of every e-mail to your server:

- Server connecting to your e-mail server to send mail, must sent it's IP Address. This is necessary in order that communication can be established between the two servers to transmit the messages.
- Once a connection between the two e-mail servers is established, your server connects to the RBL service and transmits the IP Address of the server wishing to send e-mail.
- The RBL service checks its database to determine if the IP Address is considered an 'open relay' (Ability to be used to send SPAM).
- If the answer from the service is 'yes' it is an open relay, your e-mail server, transmits a error code to the source server, and terminates the connection, not permitting any transmission of e-mails.
- If the answer from the RBL services is 'no' it is not an open relay, your e-mail server, transmits an 'o.k.' code to the source server and e-mail delivery continues.

A few years ago, RBL lists were present; however they were not widely used for several reasons. Most commercial software did not support RBL services. The ability to use these services was limited to freeware, unix and open source type of solutions. In contrast, today it is difficult to find commercial software that does not support RBL services. Another reason for not using an RBL service was that most commercial e-mail servers had the ability to be used as an 'open relay' by default and in most cases the ability to disable this was not available on the products. So by subscribing to a RBL service, a company would typically disallow e-mail from companies that you wished to receive e-mail from. Today, if a company is on a RBL list this is not taken lightly by management. Critical e-mails can be stopped from being delivered; it gives a bad perception of the company to the outside world. And with the worms, viruses and other 'bad' stuff, subscribing to a RBL list offers an excellent means of protection. SPAM and unwanted e-mail was not as prevalent as it is today. Many companies and individuals did not have e-mail or were not using it often. Today, most businesses give all employees and e-mail addresses as it has become a required form of communication in today's world. This makes the effort of marketing to these e-mail addresses worth while. All these e-mail addresses make creating lists of e-mail addresses and selling these lists worth while as well. All these factors make SPAM and mass mailing worth while.

Content filtering, SPAM detection engines are other solutions that can also enhance the removal of SPAM and unwanted e-mail in your environment. However, In my experience as a consultant for companies with this problem, subscribing to one or more RBL services alone, stop more than half of the SPAM and unwanted e-mail your company receives. Often these services can be implemented right on your existing mail server, or with freely available solutions.