

---

***maps***

**Introduction to the  
Realtime Blackhole List (RBL)**

## Table of Contents

<b>Introduction.....</b>	<b>1</b>
<b>Rationale for Creating the RBL .....</b>	<b>2</b>
Theft of Service.....	2
Rights to Passage .....	2
Commerce is Good .....	2
Censorship and Free Speech .....	2
Historical Context of Spam.....	3
<b>Reasons for Listing an IP Address on the MAPS RBL .....</b>	<b>3</b>
Listing Due to Spam Origination .....	3
Listing Due to Use of Unconfirmed Mailing Lists .....	4
Listing Due to Spam Relaying.....	5
Listing Due to Open Proxy .....	5
Listing Due to Spam Support Services .....	6
Listing Due to Netblock Inheritance.....	8
<b>RBL Nomination Process .....</b>	<b>8</b>
<b>RBL Removal Process .....</b>	<b>9</b>

---

## Introduction

The MAPS Realtime Blackhole List (RBL<sup>®</sup>) was established in 1996 and is the most comprehensive, database of IP addresses that are known sources of unsolicited commercial and bulk email (a.k.a. spam). The MAPS RBL is a carefully maintained list of IP addresses that have been shown to send spam and/or allow their resources to be used by those who send spam.

At MAPS we believe that all information exchange on the Internet should be consensual, and unless you choose to receive email from a third party, you should not have to accept it. The RBL is our way of assisting email and network providers with identifying and refusing email from known senders of unsolicited email. By subscribing to the MAPS RBL Service, these providers can reduce the impact of spam on their own network and focus their resources on providing their customers with better support and services.

The MAPS RBL Service allows for the creation of intentional network outages ("blackholes") for the purpose of limiting the transport of known-to-be-unwanted mass email. Because it is a subscription system, no one is ever denied connectivity to a non-RBL-subscriber. We do not police the Internet, but rather offer a method to identify likely origins of spam.

Many of those involved with MAPS and the RBL over the years have spent most of their professional careers trying to improve open network connectivity. It is therefore with very mixed feelings that we deliberately seek to make any part of the network inaccessible to us or to make ourselves inaccessible to it. Our ultimate goal, however, is not to stop connectivity but rather to stop spam from abusing our resources.

## Rationale for Creating the RBL

### Theft of Service

Irrespective of the laws of whatever land a spammer, or a spam victim, is in, we consider spam to be theft of service. Internet users do not pay their access fees for the purpose of being annoyed. None of us bought our computers or modems for the use of so-called *advertisers*. Since the original ARPAnet, the written rules of the Internet community (see the Netiquette RFCs and their precursors from Usenet) have required that we each refrain from intentionally annoying other Internet citizens.

### Rights to Passage

No Internet user has any fundamental right to send you email or any other kind of traffic. All information exchange on the Internet is consensual, and unless you opt into some advertising feed, the automatic presumption on the part of all Internet users should be that you would be annoyed by email that promotes a unilateral cause (such as making money for the sender). By creating and maintaining the MAPS RBL we are exercising our right to refuse traffic from anyone we choose. We choose not to accept any traffic at all from known sources of spam. This is our right, as it would be within anyone's rights to make the same choice (or a different one, so long as only their own resources were affected by their choice).

### Commerce is Good

Commerce has fueled the wonderful growth of the open data services market (which is presently known by the brand name: ``Internet"). We like commerce. We do not like theft of service. It makes no difference to us whether spam is of a commercial nature; we regularly receive spam concerning the death of society mavens, or concerning our possibly immortal souls, or concerning the postcard-oriented last wish of a boy dying of cancer in Florida. It is all theft of service, no matter what its content. It serves the sender and was unsolicited by the recipient. Consensually commercial activities are good. Unsolicited mass email is always theft of service no matter what its topic.

### Censorship and Free Speech

The right to free speech, in places which recognize it, means the right to print leaflets, stand on street corners, and offer to give them to passers by. Just as there is no right to intentionally and misleadingly shout *fire!* in a crowded movie theatre, there is and can be no right to use someone else's printing press and delivery trucks to send your message to people who have not asked to see it. We are all, at MAPS and in every anti-spam coalition, extreme advocates of free speech. However, we believe that speech is more free if the recipients hear what they choose to hear, rather than what spammers want them to hear.

An electronic mailbox, which is jammed to overflowing with spam, may not even have room for desirable, consensual communications. But even if there are no resource constraints on a mailbox, the ability of the average Internet citizen to sift through mountains of spam, after paying to receive it is limited. How free is speech between two consenting parties if thousands of third parties are deliberately shouting messages at the first two?

As for censorship, we don't care what two consenting people say in the privacy of their own channel. We don't care if people want to send each other traffic often considered inappropriate or boring (such as pornography or football scores). What we are trying to prevent is paying; in money, resources and our own time, to receive and process traffic that is nonconsensual in nature. We do not accept unsolicited mass email, regardless of its subject matter.

### **Historical Context of Spam**

Advertising, when done well, is expensive, and if it succeeds it is because it actually does offer some kind of value to the people who respond to it. Spam is another in a long line of methods of transferring advertising costs to recipients. Most of us get a lot of junk paper mail every day, and most of us throw most of it away without outrage. But what if it arrived with postage due, and with no way to refuse delivery or refuse payment? If you can envision that, then you are well on your way to understanding why we do in fact experience outrage when we receive unsolicited mass email, i.e., *spam*.

## **Reasons for Listing an IP Address on the RBL**

In this section we describe some of the reasons an IP address may get listed on the MAPS RBL, as well as some of our efforts to help prevent these types of abuse from taking place.

### **Listing Due to Spam Origination**

The original focus of the MAPS RBL when it began operations in mid-1996 was on identifying the sources of dedicated, professional spammers. Over time, the success of the MAPS RBL forced abusers to resort to other channels for distributing spam such as third party relaying and direct-to-MX contacts.

These countermeasures to our defenses, as well as newly emerging sources of abuse have made it necessary to modify our own strategies in response. We will describe the MAPS RBL strategies in its earliest days before discussing the more recent and more insidious forms of email abuse MAPS is attempting to control.

When a professional spammer gets a leased line, we find out about it when they start spamming us, and we track down every network object they own and we blackhole all or nearly all of them: mail servers, web servers, name servers, terminal servers, usenet servers -- everything. If a professional spammer owns it, we don't want it talking to us, no matter what the protocol.

When an ISP sells dialup or leased line connectivity to a spammer, we try really hard to get them to cancel the contract and strengthen their AUP against future spammers. If they plead inability to break the contract (which is very common), but they are willing to tell us exactly which netblocks have been allocated to the spammers, we will blackhole only the spammer subnetblocks.

### **Listing Due to Use of Unconfirmed Mailing Lists**

More recently, legitimate and respected businesses have stumbled into the spamming business. It is even more important to address Unsolicited Bulk Email (UBE) from the Fortune 500 than it is to challenge UBE promoting multi-level marketing schemes.

When well-respected companies begin using UBE as part of their direct marketing campaigns, it is almost always the result of the mistaken attempt to apply direct mail and telephone marketing principles to email. MAPS is a fervent advocate of the commercial use of email, but we also insist that such use begins from the principle that *all communications must be consensual*.

In practice, this means that businesses should never presume to shift the costs of their advertising onto their customers until they have been given explicit permission to do so. Would any respectable marketer even dream of using collect phone calls or postage due mailings to reach potential customers?

Marketers wishing to use email should consider the foregoing question carefully when preparing their campaigns. Advertising based on permission marketing principles have proven to be extremely successful. Opt-in is a win-win strategy for both marketers and consumers.

On the other hand, marketers who wish to insist on a so-called opt-out strategy -- in which they take it upon themselves to send as much promotional material as they want to someone's inbox until asked to stop -- are eligible for listing on the MAPS RBL (more recently the MAPS Non-confirming Mailing List - NML<sup>SM</sup>). The opt-out approach violates our fundamental principle: *all communications must be consensual*.

This fundamental principle is sometimes violated by mailing lists with inadequate confirmation or verification steps. Mailing lists lacking a subscription confirmation step can be used to send unsolicited mass email to unwilling recipients. A mailing list should include only those who have explicitly indicated an interest in receiving messages from the list.

Prudent mailing list management mandates verification of all subscription requests before mailings commence. Many well-meaning list managers have found themselves in the spamming business when they don't confirm subscriptions. Please review MAPS' Application Note: Guidelines for proper mailing list management, for additional expectations and best current practices.

### **Listing Due to Spam Relaying**

Currently, the most common reason for a host or network being in the MAPS RBL is that it was used by a spammer as a mail relay. We call this *third party relay spamming* since the owner of the mail relay is neither a spammer nor a spamee. They unwittingly provide a conduit between a spammer and some number (usually a very high number, tens or hundreds of thousands) of spam victims. Because this activity represents unauthorized use of a server by a third party, the press has taken to calling it *server hijacking*.

These third party relay operators are themselves victims of spam, but not in the usual sense since their personal inboxes are unaffected. Once a spam has completed the relay, operators have no trace left of it other than: log files, angry complaints from spam victims, and disrupted connectivity due to having been put into the MAPS RBL.

Open relays may be entered immediately onto the MAPS RBL to stop spam-in-progress. Depending on the severity of the relay, we may contact the site's listed authoritative contact, or at least the postmaster@ and abuse@ addresses for the listed site. At this point, we feel that most people that intend to secure their sites against unauthorized use have done so, and the remainder have no short-term intention to prevent the abuse of their systems.

MAPS also provides the Relay Spam Stopper (RSS<sup>®</sup>) -- a list including *only* unsecured relays which have been used to distribute spam. The MAPS RSS has different nomination requirements than the MAPS RBL. Please see the MAPS RSS section of the MAPS web site for further information.

Once a site is on the MAPS RBL or MAPS RSS for open relay, it will remain on the list until the site administrators contact us and let us know that it is secure. When we are contacted, a staff member will confirm that the listed site is no longer relaying spam. If it is not relaying, the site will be unlisted, usually within a few minutes of the email or phone call.

### **Listing Due to Open Proxy**

Like open relays, open proxy servers which have been used in the transmission of spam may be entered immediately onto the RBL until they are properly secured. Again, the owner of the open proxy is neither a spammer nor a spamee. They are however, providing a means for the transmission of spam (and often other unauthorized traffic) by a third party. In the majority of the cases, the only record of the true origination of the mail is in the proxy server's logs - any email or other traffic

received from the open proxy will appear to have originated there. In a lot of cases, spam via open proxies is indistinguishable from Direct to MX spam.

MAPS also provides the Open Proxy Stopper (OPS<sup>SM</sup>) -- a list including *only* unsecured proxies which have been used to distribute spam. The MAPS OPS has different nomination requirements than the MAPS RBL. Please see the MAPS OPS section of the MAPS web site for further information.

### **Listing Due to Spam Support Services**

In addition to those domains that originate or relay spam, organizations providing spam support services are eligible for listing in the MAPS RBL. "Spam support services" includes:

- I. providing any service which uses internet resources to support spamming activity, including, but not limited to:
  - (i) hosting web pages which are promoted by spam;
  - (ii) providing email drop boxes or auto responders which are promoted by spam;
  - (iii) providing resources such as DNS services, banner ads, hit counters, script processing and form handling services to sites promoted by spam;
  - (iv) news to mail gateways;
  - (v) fax to email services;
  - (vi) voicemail to email services;
  - (vii) providing credit card processing or other online payment collection services for goods and services promoted by spam;
  - (viii) providing adult verification services to sites promoted by spam;
  - (ix) email to pager services.
- II. providing software or services for distributing spam;
- III. hosting web pages or otherwise providing connectivity to those who provide software or services for distributing spam;
- IV. providing software or services to acquire email addresses by any means other than verified opt-in methods, e.g., email appending, harvesting addresses from web pages, newsgroup articles, and online directories, or mining addresses using "dictionary attacks" or automated processes for the purpose of deriving email addresses without the knowledge and consent of the owners of those email addresses;

- V. providing access to, or distribution of lists of email addresses obtained by any means other than verified opt-in.
- VI. continuing to provide service or access to customers providing spam support services after such activity has been brought to the access provider's attention.

Not a month goes by without some listee of the MAPS RBL sending us mail, asking for advice and/or assistance, because they do not allow spam to emanate from their networks. All they're doing, they usually say, is providing online payment processing services or an email drop box or a web page for spammers. *Why*, they ask, *are they being blackholed even though they are not sending us any spam?*

Well you see, spammers know that they will lose their accounts and/or links if they use those accounts or links for spamming. So they don't. They order an account from a large online service provider and spam like crazy using that account, until a few hours later when that account is terminated for cause. They usually end up paying nothing for these accounts. We call this whack-a-mole spamming after the popular arcade amusement game by that name.

We work with every online service provider who asks for assistance to help them validate users before letting them have access (spammers were reusing the same credit card numbers but with different names from day to day), to help them stop spam from escaping their borders (limiting each user to one outbound email message per minute, of five recipients or less, works well), and generally helping them see the seriousness of their situation.

But this is not by itself sufficient. So when we are spammed, we look at the various contact information given in the text of the spam. Our reasoning is, it would make no sense to have sent us this *whack a mole spam* if the contact address (maybe email, maybe web, maybe both) was nonfunctional. And if it becomes widely known that selling email or web services only to have them advertised in the text of spam is a great way to lose connectivity, then spammers will not be able to hide behind legitimate service providers and we'll smoke them out into the open, which means into using their own (blackholable) links.

*This tactic has worked* and we will therefore keep doing it. Our very strong advice to all web and email providers is: *require your users to sign a contract stating that they will not use email or web addresses from your systems as contact points for spam*. In fact you could go further, as many providers do, and require (as a term of your contract) that your customers *do not engage in the practice of spam in any part of their business*. There is plenty of money to be made in the ISP business, you do not need to take every customer in order to prosper, and spammers will cost you a lot more money in the long run than they will ever pay you.

A site being advertised as a target on multiple spam messages may be placed on the MAPS RBL. If we are contacted, a staff member will confirm that the listed site publishes and *enforces* a strict usage policy with respect to email abuse, and has a

current and answered abuse@ account. Meeting these qualifications usually gets the site unlisted. Known spam factories require more detailed qualifications before they are unlisted.

### **Listing Due to Netblock Inheritance**

A network or host that has been added to the MAPS RBL becomes a sort of a *dead spot* in the address space. Things which are assigned that address can't reach a big part of the network, and as a result they experience a very much smaller *internet experience* than hosts and networks which are not listed in the MAPS RBL. The wonderful result of this is that spammers have to move on, at considerable pain and expense, to new, not-yet-blackholed, parts of the address space.

The nonwonderful final result of this is that the next person to be assigned the spammer's old address space will get the same rotten connectivity that the spammer got. Every once in a while somebody contacts us and tells us that they think this is happening to them, and while we always check to be sure we aren't being spoofed, so far it has always been an actual inheritance of an old spammer netblock by a new non-spammer user or organization.

When it is brought to our attention that an IP address is no longer under the control of a spammer, we will work with the new user to remove the address as quickly as possible. Loss of connectivity hurts us all. Spam hurts us all even more.

### **RBL Nomination Process**

IP addresses that have been nominated to the MAPS RBL go through a thorough review process before they are added to the list. Submissions are obtained from role accounts, trusted submitters and 3rd parties.

- 1) Investigation - all submitted spam samples are reviewed for accuracy and completeness to determine:
  - a) whether the email is actually spam
  - b) the true origin IP address(es) of the spam emails
  - c) what parties are responsible for the IP in question, and how they can be contacted to take action to stop the spam
- 2) Notification – attempts are made to contact the responsible parties outlining:
  - a) what IP or IPs are being considered for addition to the RBL
  - b) reason for listing

- c) spam samples to illustrate that there is indeed a problem that requires action be taken.

Any responses, including auto-replies and bouncebacks, are recorded for the investigation, and responded to appropriately. This is to ensure that a 'good-faith' effort to notify the responsible parties has been made before a listing goes live, and that they have a chance to respond to the listing.

- 3) Nomination - If no response is received, or the responsible parties are unwilling or unable to rectify the problem, a nomination to the RBL is made. The Investigator creates a nomination documenting the entire Investigation and Notification process. Once the nomination is reviewed and the information in the nomination is verified, an IP address is added to the MAPS RBL

### **RBL Removal Process**

When a request for removal from the MAPS RBL is received, a dialogue will be started with the requestor to determine:

1. if the requestor is an appropriate contact to request removal, such as an abuse representative or server administrator, as opposed to a casual or end user
2. why action was not taken before the listing went live in the RBL
3. what action has been taken to resolve the problem and what further actions have been or will be taken to ensure that the problem will not occur in the future
4. if necessary, ask about abuse handling policies, acceptable use policies, any problems encountered in the notification, etc.

These interactions are documented and a recommendation will be made for the listing (removal, probation, maintain listing). Once a remove request has been submitted, we work quickly to determine if the necessary steps have been taken to assure that there will be no more spam problems in the future. An IP address can be unlisted very soon after a request is made.