

Spamhaus SBL

[What is the SBL?](#)

[Who uses the SBL?](#)

[How do I use the SBL?](#)

[How much spam will the SBL block for me?](#)

[Can the SBL block legitimate email?](#)

[Can the SBL be used to block more than just spam?](#)

[How often is the SBL zone updated?](#)

[How do I test my SBL setup?](#)

[How do I keep my network's IP blocks out of the SBL?](#)

[When will Spamhaus remove my IP\(s\) from the SBL?](#)

[How often are listings re-checked?](#)

What is the SBL?

The Spamhaus Block List (SBL) is a realtime database of IP addresses of spam-sources, including known spammers, spam gangs, spam operations and spam support services. SBL listings are made according to policies outlined in [Rationale & Listing Criteria](#).

The database is kept updated every day, around the clock, by Spamhaus Project team members around the world.

Who uses the SBL?

The SBL is used by many of the world's Internet backbones, large tier-1 providers and ISPs in almost every county, including a number of large U.S. and European government and military networks, and some of the best giant free email providers. Most large SBL subscribers, universities and corporations (which include major banks, aerospace and electronics) have hourly SBL Data Feeds. The combined SBL user base (mailboxes protected by the SBL) now exceeds 600 Million internet user mailboxes*.

Companies marketing anti-spam software and hardware gateways have also incorporated an SBL feed into their products where it helps protect their customers by identifying worldwide spam sources.

* as of February 2007 the SBL user base exceeded 644,997,000 internet user mailboxes.

How do I use the SBL?

The Spamhaus Block List ("SBL") is in a format intended to be used by the mailservers of corporations or ISPs. End users should ask their email

provider if they use the SBL, and if not, ask them to implement it. If this is not possible, end users should look for spam filtering software that is able to use "DNSBL" systems (sometimes called "Blacklist DNS Servers" or "RBL servers"). Most will have the SBL (or ZEN, or the older SBL-XBL) as a default or available as an option. Use of the SBL in query mode is free for users with normal mail server traffic (but ISPs and corporate networks with heavy email traffic will need to use our [Data Feed](#) service).

The SBL can be used by almost all modern mail servers, by setting your mail server's anti-spam DNSBL feature (sometimes called "Blacklist DNS Servers" or "RBL servers") to query sbl.spamhaus.org.

For information on how to configure your mail server to use sbl.spamhaus.org please refer to your mail server documentation/manuals or ask your mail server developer. With so many different mail servers in use we can not offer technical help with setting up the SBL.

We recommend you use sbl.spamhaus.org together with xbl.spamhaus.org and pbl.spamhaus.org, as the SBL and XBL/PBL block [different spam sources](#). To save you having to query three separate DNSBL zones there is a special combined "ZEN" zone, zen.spamhaus.org, which contains the complete SBL, XBL and PBL data. We recommend you use this combined zone, by simply setting your mail server's DNSBL check to query zen.spamhaus.org only. For more information on this, please read our [How to use the SBL](#) page.

We ask, but do not require, that all ISPs using our BL zones inform customers of the fact you run spam filters (simply because it is the correct thing to do). Use of known-to-be-effective spam blocklists is normally seen as a service advantage and strong sales point. All SBL, XBL and PBL users are welcome to use the "email protected by" SBL, XBL and PBL web badges on sites.

How much spam will the SBL block for me?

This depends on a number of factors; how many domains you host, how many email addresses in those domains have been harvested by spammers, pulled out by dictionary attacks, etc.

Current numbers show the SBL can stop, on average, about 15-25% of incoming spam at SMTP connection time, and over 90% of spam in message body URI checks.

The SBL is meant to be used in conjunction with other Blocklists. The SBL targets spammers who host on, or spam from, a fixed location.

Additional systems such as the [Spamhaus XBL \(Exploits Block List\)](#) and the [Spamhaus PBL \(Policy Block List\)](#) should be used to block spam from spammers who use criminal methods to spam. These target spammers

using open botnet-proxies - PCs they have infected with viruses. The combination of all three is available in our [Spamhaus Zen](#) zone.

See the [Spam Filtering Guide](#) page with charts and details on how the Blocklists function.

Can the SBL block legitimate email?

The SBL's primary objective is to avoid 'false positives' while blocking as much spam as possible. Indeed because SBL false positives are extremely rare, there is little visible controversy regarding the SBL yet we are one of the Internet's biggest spam blocking systems.

It is important to note that, unlike most commercial ISP-level spam filter solutions, in its most used form, the SBL does not "absorb and trash" incoming email - instead it has a vital delivery fail-safe mechanism: By design, no matter how rare they may be, any false positive rejected by mail servers using the SBL follows correct RFC defined SMTP mail delivery procedure and is returned ("bounced") to the immediate Sender with the explanation of why the message could not be delivered and what the Sender should do about it. One of our main objectives is to help keep valid, non-spam email from being lost, or mixed in with hundreds of spam messages where they can be overlooked or automatically trashed as many systems will do.

However, like any system used to filter email, the SBL has the potential to block items of legitimate email if for example they are sent from an IP under the control of a spammer or via IPs belonging to a Spam Service. The chances of any legitimate email coming from such IPs are very slim, but need to be acknowledged.

In order to terminate some persistent spam operations the SBL team occasionally needs to escalate a listing and it is in the application of an escalation that 'collateral damage' can occur. Once a known spam operation is blocked, the SBL team then attempts to open dialogue with the ISP providing service to the spammer and assists the ISP with collating evidence to terminate the spammer. In rare instances the ISP turns out to be knowingly assisting the spam operation for profit. In these cases the SBL Team may deem the ISP itself to be the 'Spam Support Service' and may escalate by listing the ISPs corporate resources (such as corporate mail servers), determined on a case-by-case basis to focus action on the ISPs executives and always with the primary objective of avoiding blocking legitimate customers.

Can the SBL be used to block more than just spam?

Yes. One can deny access to Apache webserver based websites from SBL listed IP addresses. An Apache tool called [mod_access_rbl](#) does the job. It is designed for Apache 1.3 - but a patch for the 2.x versions has been created

(as has a newer 2.x only system called [mod_dnsbl_lookup](#)). A website that covers it, and exactly how to set up a system like this is located at *Got Root?* in an article called "[How to use RBL's to protect apache from compromised and infected systems.](#)"

Do provide a way for denied users to see why they have been denied. Also, note that this is the SBL **not** the [XBL](#) or [PBL](#). The XBL contains dynamic IP addresses, meaning the user you would be blocking is probably not going to be the user with the exploited computer. The PBL just contains large ranges that should not send SMTP. Please do not block innocent users.

On moderate-traffic websites, we really recommend a proper DNS caching system be used, on high traffic sites one must implement our [Spamhaus DNSBL Data Feed Service](#).

How often is the SBL zone updated?

The SBL DNS zone is rebuilt and reloaded every 30 minutes, 24/7, to ensure that new spam problems are swiftly blocked and that fixed problems are swiftly removed. For high redundancy there are over 40 public SBL mirrors located in many nations around the world. Each SBL mirror is independently run as a free service to the Internet community and all respond in realtime to public queries of [sbl.spamhaus.org](#). SBL DNS mirrors are located in: Argentina, Belgium, China, Denmark, France, Germany, Greece, Italy, the Netherlands, Russia, Singapore, Spain, South Africa, Venezuela, the UK and USA.



How do I test my SBL setup?

Once you have set up your mail server to use [sbl.spamhaus.org](#) (or the preferred [zen.spamhaus.org](#)), you can test to see if the SBL blocking is working by sending an email (any email) to: nelson-sbl-test@crynwr.com

(you must send the email from the mail server which you wish to test). The [Crynwr](#) system robot will answer you to tell you if your server is correctly blocking SBL-listed IP addresses or not.

How do I keep my network's IP blocks out of the SBL?

Or "How do I keep my spammers off my network?"

- Enforce a strong [Acceptable Use Policy](#) (AUP).
- Read *postmaster@* and *abuse@* mailboxes every day, and act on reports!
- Maintain accurate and active contact information in "whois" records.
- Check out new clients at <http://www.spamhaus.org/rokso/>.
- Check out new clients at <http://groups.google.com/>.
- Be sure that your [role accounts & feedback loops](#) are working properly, which includes:
 - * Working *postmaster@* and *abuse@* mailboxes ([RFC2822](#), [RFC2142](#)).
 - * IP ranges registered with [AOL FBL](#), [SpamCop](#) and [others](#).
 - * Domains registered with [The Network Abuse Clearinghouse](#) (abuse.net).

When will Spamhaus remove my IP(s) from the SBL?

There are a few issues ISPs need to take care of before confirming that an SBL-listed spammer has been removed. Once the spammer is removed, the ISP should request removal by sending a removal request to the SBL removal queue (click the "contact the SBL Team" mailto link on the bottom of each SBL listing page). While specifics of each listing vary, basically the spam problem must be completely stopped. Here are some of the steps for a general case of a spammer's dedicated account:

- the server needs to be taken down or disconnected (except if it concerns a virtual or shared server);
- any PTR entries need to be cleared or set back to its default setting;
- any DNS entries served by the ISP's main DNS servers for the SBL-listed customer should be cleared;
- the ISP's MX server should no longer accept mail for the SBL-listed customer;
- if the IP addresses were SWiP'd or in rWhois, they should be removed or a request for removal to the RIR should have been made.

How often are listings re-checked?

We only re-check a listing when contacted, there is no automatic re-checking of listings. However to prevent 'stale' listings from remaining on the SBL each record has a "time to live" setting after which it is automatically deleted from the SBL. The default "time to live" for a listing is 6 months, however some listings (such as listings for major spam-in-progress) are set to short periods such as 48 hours. Problem areas and

known professional 'hard-core' spam operations with netblocks SWiP'd to them by ARIN/RIPE/APNIC/etc may have their record's "time to live" set to years. The system automatically sweeps (deletes) listings when the 'time to live' has expired.