How to Avoid Being Blacklisted

What Are Blacklists?

A **blacklist** usually refers to a list of e-mail or IP addresses known to send spam e-mails or some other type of unsolicited messages. Such lists are currently used by mail servers for filtering incoming e-mails and blocking the ones listed, in order to improve mail security and integrity. The blacklist is also the opposite of what is called a **whitelist**.

The Basics

First of all, being blacklisted does not mean that you have committed some kind of offense or illegal action. Blacklists have multiple purposes, including the denial of SMTP direct access for dial-up and DSL users, which mostly engage dynamically assigned IP addresses. Users are forced this way to send their mail through their provider's mail servers, which are properly configured.

Blacklists may also define what is considered to be an abuse, sometimes in a debatable manner, as no strict rules are set regarding this matter. Some of them include NDR and other auto-responses in their policy in order to prevent NDR attacks and other similar problems. During normal operations, as the RFC states, any server is forced to accept NDR messages.

Other lists aim to limit the networks assigned to certain countries. In such cases, a provider can use a policy and not accept any emails sent from or through those countries.

The Details

There are a few steps you should take to in order to prevent being blacklisted. The most important ones are closely related to securing your mail server and making sure no third-party can use it to send e-mails in an unsecured fashion:

- Do not allow unsolicited ads and other bulk e-mails to be sent from your server, by the hosted accounts;
- Do not run pro spam services like: spam websites, drop mail boxes for replies to spam e-mail ads, DNS for junk mailers, payment processing services for the products advertised in spam messages, junk mail tools (like lists of e-mail addresses);
- Make sure all your hosts are as secure as possible;
- Make sure you do not have any spam bots on your systems;
- Make sure your mail server is not an open relay;
- Make sure your proxy server is not an open proxy;
- Check that the **abuse@yourdomain.tld** and **postmaster@yourdomain.tld** addresses exist and that they are functional;

- Make sure the information provided in the domain registration service (whois) is updated and complete;
- Make sure all your mail servers accept **mail from: <>** delivery notifications (NDR);
- Don't use an ISP that has a bad reputation when it comes to spam. Doing so may get you blacklisted just because your IP address is part of their allotted subnet;
- Make sure your DNS is properly set up and that you are complying with the RFC rules regarding service configuration;
- Make sure your mail server does not send poorly-formatted messages;
- Deploy Domain Keys and SPF for outgoing messages;
- Use secured connections (SSL/TLS) as much as possible;
- Do not allow unauthenticated users to send e-mails neither locally nor remotely.

When you feel that your server is correctly configured and spam-safe, you can use one of the open relay testing and DNS testing tools available on the Internet to make sure everything is working as it should. If any errors are then reported, they should be fixed before taking any server into production.

Also, never forget that there are distributed lists that do not provide any method of removal from the database. In such cases it is best to prevent being added in the first place.

References

For information about how to get removed from blacklists, please check this article as well: What to Do if You Are Blacklisted.