SSBG IT Solutions

Ph: (8621) 5404-3999 Fax: (8621) 5404-7759
Email: Sales1@SSBG.com.cn www.SSBG.com.cn

How to Avoid Email Server Blacklisting

By Samuel C Ritter
Senior Consultant, SSBG IT Solutions

The best way to avoid being blocked is to run a clean mail system from the beginning. It is kind of like quicksand that way. If you allow a server administrator to avoid the best practices models from the beginning, then it is much more difficult to dig your way out of the hole it creates.

Due to the number of requests for this type of information, I have put together the following Best Practices Guideline used by SSBG Sr Technicians, and as part of our on-going technical training program. Please note that since email systems worldwide are always developing and changing, these guidelines will of course have to be updated and adjusted regularly to be effective over time.

The basic rules are as follows:

---

1) No Mail relay of any kind on your mail server - and setup an abuse@domain.com address for each of the domains you are hosting, so you will know when someone is trying to contact you regarding a spam problem from your server.

2) Require SMTP authentication for both SENDING and receiving mail via your mail server.

3) Do not run other server applications on your designated email server (creates holes that can possibly be exploited by spammers).

4) Use a professional level Email server software (preferably legal with continuous quarterly updates to keep you ahead of the spammer exploits).

5) Old software or non-professional grade software is much easier to compromise.

6) Understand and make use of PTR DNS records.

7) Correctly configure and maintain DNS records for your domains (including MX and A record associations).

8) Do not host your mail server on anything other than a static IP address.

9) Use a properly configured and managed firewall system (hardware is preferred) to protect your server from outside intrusion or exploitation.

10) Limit users on your system to no more that 15-20 simultaneous recipients of a single email message.

11) Do not try to use your mail server as a marketing tool or list server - Building a list server separately, on a different IP address would be advised - and make sure it is also securely managed to prevent outside abuse.

Of course, even the best managed systems sometimes find there way onto a blacklist or blocklist of some sort, and in fact several poorly run blacklists based in the US block all traffic from places like China indiscriminately. When this occurs, you are faced with the problem of getting your IP/system off of that list as quickly as possible. I have listed below the basic steps for handling this kind of situation.

Follow these Steps:

Ph: (8621) 5404-3999 Fax: (8621) 5404-7759
Email: Sales1@SSBG.com.cn www.SSBG.com.cn

1) Check your server logs, and try to find the details concerning the blocked transactions.

2) Contact the Sysadmin for the location or company that is blocking you.

3) If they are using a spam filter, you will need to find out what kind of filter they are using, or the blacklist reference they are using, and then try to figure out why your mail is being rejected.

4) If you find your mail is being rejected because it is listed as a spam source with Spamhaus, Spamcop or one of the other international blacklists, then I suggest you visit the appropriate website and take the necessary steps to request removal. This process can take several weeks in some cases as they will respond to your request by telling you why you were blocked, and then schedule a time later on to re-test your IP and server before they will release your address from the blacklist.

5) You will have to continue submitting and negotiating with each blacklist individually to get your IP address clear once again, once you have been added to a blacklist, as they will often pick up results from each other in order to make their systems more responsive.

Here are some of the more common blacklists used currently by companies for spam filtering:
Fiveten – www.blackholes.five-ten-sg.com
SpamHaus – www.spamhaus.org
YBL – www.ybl.megacity.org
SpamCop – www.spamcop.net

Each of these sites contain information about how spam filtering and blacklists work, and will even offer detailed information and resources concerning how to avoid getting on their lists, and what you can do to be removed from these lists.