Adept

Managed ICT Services & Solutions

SAIX Blacklisting

In Internet terminology, Blacklisting is a generic name for a list of e-mail addresses or IP addresses that are originating with known spammers. Individuals and enterprises can use blacklists to filter out unwanted e-mails, as most e-mail applications today have filtering capabilities. SAIX is the largest IP/Internet backbone that connects the country to the rest of the world. Users connecting with ADSL on the SAIX network, will by default be relaying mail via the SAIX SMTP outgoing mail servers.

Since their network carries a large amount of users, they have to ensure strict enforcement of spam policies. Should one of their servers get listed for spam, it will affect 1000s if not 10s-of-thousands of users at a time. It has recently become a more common occurrence to experience mail issues as a result of blacklisting. This is partially attributed to the raised standards of handling of mass mail abusers in efforts to prevent spam.

1. Possible reasons for being blacklisted

    a. Open-relay/Proxy server blacklists are based on open ports through which unauthorized network traffic is allowed to flow. The open-relay/proxy lists are the most definite and widely used since they are based on the presumption that a "spammer" found you and likely had relayed a high volume of SPAM through your Message Transfer Agent (MTA), causing your MTA's IP address to be reported to the list by recipients of that SPAM message

    b. Another method blacklist sites use to produce listings is that of "guilt by association". A blacklist site will list much larger blocks of IP addresses than those owned by the suspected abuser. For example, if you are provided with an IP address and the "spammer" owns an address that is close in range to yours and the spammer gets listed on this type of blacklist, your IP block might be listed as well. Usually the reasoning behind this practice is that, by punishing innocent parties, the blacklist-er is putting more pressure on the ISP to disconnect the suspected spammer's Internet access. SAIX can only take action against a customer in violation of their AUP and direct evidence must be provided to substantiate the violation (email headers or other evidence of abuse). A blacklist site's evaluation of someone as a "known spammer" or having a "history of spam" is NOT acceptable evidence of violation of our AUP, and does not warrant the termination of service.

    c. Forms of Spyware viruses are also able to attach themselves to computers and use the device as a host for distributing Spam without the users' knowledge. This is commonly the problem as users do not realize their computer has been infected until it is too late.

Email support@adept.co.za
Tel +27 (0)21 888 6500
Fax +27 (0)21 888 6600

2nd Floor DataVoice House, 16 Elektron Avenue
Techno Park, Stellenbosch, 8301
www.adept.co.za

Adept Internet (Pty) Ltd.
Directors: J. Pietersen, G. le Grange
Reg. 1984/001310/07

2. How to tell if you are SAIX blacklisted

    a. When attempting to send emails, you may receive bounce messages back that will relate to the SAIX system.

SAIX blacklist bounce message examples:

- <AUD-SRV.AudiInternational.local #5.7.1 smtp;554 5.7.1 Service unavailable; Sender address [example@domain.co.za] blocked using rhsbl.saix.net; RHSBL03 See <http://www.saix.net/smtp/rhsbl-faq.html>
- 554 5.7.1 <info@example.com>: Sender address rejected: Yahoo TOS - SAIX Ref:S942 - Blacklisted for SPAM
- <xxxxx@domain.co.za> (smtp.saix.net: 554 5.7.1 <servername.domain.local>:Helo Command rejected: AOL TOS - SAIX Ref:H434 - Blacklisted for Spam Trojan)

    b. To test your port traffic:

- Open up the Command prompt
- Type nslookup example.com.rhsbl.saix.net
- If it points to 127.0.0.4, your domain is listed

    c. There are also sites that perform lookups on the various RBL sites to check if your details are listed

- Mxtoolbox is an example of such a site: http://www.mxtoolbox.com/blacklists.aspx

    d. Verify with your ISP that you are indeed blacklisted

3. What to do if you suspect being blacklisted

This partially depends on the category your blacklisting falls into, but the safest first step to take is to contact your Internet Service Provider. Should that be Adept, you can call us on 0861100557.

- Your settings will be checked to see what Outgoing Sever Settings you have for your email account
- It's a good idea to send a copy of the bounce message, via an alternative email solution (e.g. Gmail)
- Your entire network needs to be scanned with up-to-date antivirus and antispyware software
- After that's complete, we can log a request with SAIX for de-listing

4. What category are you blacklisted for?

Bounce messages will contain a code similar to "RHSBLxx" in the error. Here is a brief definition of the different codes:

- RHSBL00 - Administrator test listing
- RHSBL01 - America Online Terms of Service (AOL TOS) Complaints
- RHSBL02 - Domain caused a SpamCop complaint or listing
- RHSBL03 - Domain was found to send high volumes of mail in a 24 hour period
- RHSBL04 - Miscellaneous RBL listings
- RHSBL05 - Domain caused a SORBS complaint or listing; see www.sorbs.net
- RHSBL06 - Yahoo Terms of Service (Yahoo TOS) Complaints; see http://www.saix.net/smtp/rhsbl-faq.html

Remember that if you are not sure whether a bounce messages is linked to being blacklisted, you can send a copy of the bounce message, including the headers, to support@adept.co.za asking for analysis.