

Email: Rejection notices

Last Updated Tuesday, 19 June 2007

I am trying to send an email to someone on your service. When I send I get a rejection notice and they never receive the email.

When an email is rejected by our server it is accompanied with the reason for the rejection. WebNexus/SCR only rejects email for a few reasons aside from the standard "user does not exist" rejections. Unless you are the network administrator for your mail server then you should forward your rejections to the administrator. However if you are the network administrator please read below for ways to resolve the issues.

Blacklisted:

The first of these rejections is blacklisting. WebNexus/SCR uses SpamHaus and SpamCop to block known spammers from our network. These rejections are usually accompanied with a URL that will take you to the site that has you blacklisted so you can resolve the issue. If you are on a blacklist it is usually because you have spam coming from your network or your ISP does and hasn't resolved the issue in a timely manner. These rejections will have text similar to this.

554 Service unavailable; Client host [0.0.0.0] blocked using bl.spamcop.net; Blocked - see <http://www.spamcop.net/bl.shtml?0.0.0.0>

or

554 Service unavailable; Client host [0.0.0.0] blocked using sbl-xbl.spamhaus.org; <http://www.spamhaus.org/query/bl?ip=0.0.0.0>

The only way to resolve this issue is to follow the URL in the rejection and resolve the issue with the blacklist. Once that is resolved your mail will start flowing to our servers without a problem.

Reverse DNS or hostname lookup

The other form that WebNexus/SCR uses is reverse DNS lookup. To sum this up, our server will ask the server who controls the names of IP address that is communicating with it. If there isn't a fully qualified domain name (FQDN) record for the IP in question our server will reject the email with the following text

450 Client host rejected: cannot find your hostname, [0.0.0.0]

There really is only 1 way to fix this problem. Your DNS server(s) must be properly configured to answer rDNS queries. Unfortunately how to do that is beyond the scope of this FAQ but you can find information and links to tools that will assist you in correcting any misconfigurations you may have.

http://en.wikipedia.org/wiki/Reverse_dns

Note: These methods are used to force ISPs to comply with RFC standards as well as to keep their networks free of viruses and spam. 90% of spam is sent from virus infected computers and poorly configured networks. Due to the effectiveness of these methods and what they imply we will not "white list" any provider who is found to be within these categories. You will need to correctly configure your network or resolve the issue that has caused your equipment to be blacklisted. It will take far less time to correct the issue than to ask every single ISP that is practicing these methods to white list each domain.