Bounce spam protection (DSNs/NDRs)

Author:
Webservio Inc.

Created On: 11 Feb 2013 7:33 PM

"Bounce spam" can be an annoying problem. The email SMTP protocol is a very simple protocol that was defined in 1982. Spam was not yet a problem and to keep things as simple as possible, no security measures were implemented in the protocol itself. The result of this is that there is no verification whatsoever that the "From:" address in an email message actually belongs to the sender.
To try and avoid spamfilters, spammers will typically use random email addresses as fake senders. This way they can avoid any simple spamfilter that blacklists based on the sender email address. It is important however that the email address they use as a sender does exist, since spamfilters can apply a "sender verification check" to ensure that the sending address itself exists.

SpamExperts applies advanced methods to identify and block "bounce-spam".

What causes Bounce

Properly setup mailservers will not cause bounce spam and directly reject the message with a 5xx error code when the spammer tries to deliver it. Unfortunately there are many legitimate mailservers that are incorrectly setup, however. The spammer tries to deliver a spam message with your email address in the from to an unknown address, the bad mailserver accepts the messages for delivery, it then finds out that the destination user does not exist, and it will send a bounce email to your email address because it (wrongly!) believes you are the originating sender. Because these bounces do not come from spamming servers, but from legitimate servers, they are very hard to block by any spamfilters.

Catchall domains

If you have configured your email system to accept all email sent to any address @yourdomain, this is called a "catchall domain". The main advantage for you is that you won't have to create a separate mailbox for each address that should work. The problem however is that if spammers detect that your mailserver claims to accept email for any address, they can easily generate random email address and end with @yourdomain to generate millions of different "valid" email addresses! It's therefore highly recommended to disable the email catchall to avoid spammers from abusing your domain to generate fake senders for their spam messages.

BATV signing

A special "trick" to avoid bounce spam is to sign every outgoing email with a special Bounce Address Tag Validation code. If a bounce is generated from a destination server, the incoming filter will check if it was originally signed. Only if the message was originally signed, the bounce is accepted. If the message was not signed when it was send out, the bounce is not accepted. SpamWeeder Premium Outbound option supports BATV signing for its outgoing email products.