Subject: spam from my domain!
Posted by Anonymous on Wed, 07 Mar 2007 15:11:48 GMT
View Forum Message <> Reply to Message

Hi there,
we recieved some spam from fake email adress of our domain!
how can I block them?
any help is appriciated!

star-pak

Subject: Re: spam from my domain!
Posted by support on Thu, 08 Mar 2007 11:11:09 GMT
View Forum Message <> Reply to Message

> we recieved some spam from fake email adress of our domain!
> how can I block them?
> any help is appriciated!

If you are sure that you never receive legitimate emails from your own domain,
you can put it on the blacklist.

Subject: Re: spam from my domain!
Posted by Anonymous on Thu, 08 Mar 2007 13:34:22 GMT
View Forum Message <> Reply to Message

Thanks!

Subject: Re: spam from my domain!
Posted by fuchur on Mon, 12 Jan 2009 09:23:17 GMT
View Forum Message <> Reply to Message

Hello,

we have the same problem that we receive mails from our own domain. In our case we receive legitimate e-mails from our domain so it's not possible to put our domain on the blacklist. Isn't there another possibility to block these spams?

Thank's in advance
and Best Regards,
fuchur

Subject: Re: spam from my domain!
Posted by support on Tue, 13 Jan 2009 09:38:11 GMT
View Forum Message <> Reply to Message

> we have the same problem that we receive mails from our own
> domain. In our case we receive legitimate e-mails from our
> domain so it's not possible to put our domain on the blacklist.
> Isn't there another possibility to block these spams?

If you don't filter local mail (mail within your organization) and outgoing mail with NoSpamToday!, you can blacklist your domain.

Configure all mail clients to submit outgoing mail messages to your mail server directly!

Subject: Re: spam from my domain!
Posted by MBSA on Wed, 04 Mar 2009 15:17:05 GMT
View Forum Message <> Reply to Message

I have a similar problem. We have a lot of domains registred and if a spam gets through, is usually one with a spoofed (one of our own...) sender address.
I have configured SPF records for those domains. So if the SA engine checks the SPF, the spoofed mails should be stopped. But unfortunatly they do not. How can I increase the score for a failed SPF-check so SA labels those mails as spam ?

Thank you
M

Subject: Re: spam from my domain!
Posted by support on Fri, 06 Mar 2009 11:24:16 GMT
View Forum Message <> Reply to Message

> I have a similar problem. We have a lot of domains registred
> and if a spam gets through, is usually one with a spoofed (one
> of our own...) sender address.
> I have configured SPF records for those domains. So if the SA
> engine checks the SPF, the spoofed mails should be stopped. But
> unfortunatly they do not. How can I increase the score for a
> failed SPF-check so SA labels those mails as spam ?

How about adding *@yourdomain.com to the blacklist in this case ?

Subject: Re: spam from my domain!
Posted by James Wilkinson on Mon, 09 Mar 2009 13:38:26 GMT
View Forum Message <> Reply to Message

A bunch of rules like this should do the trick:

```
header __LOCAL_ENV_FROM_EXAMPLE EnvelopeFrom =~ /\@example\.com$/
meta LOCAL_EXAMPLE_SPF_FAIL         __LOCAL_ENV_FROM_EXAMPLE && SPF_FAIL
describe LOCAL_EXAMPLE_SPF_FAIL    Not from example.com (SPF fail)
score LOCAL_EXAMPLE_SPF_FAIL       3.0
```

Put that lot in local.cf, run sa-lint.bat (make sure there are no errors after the sa\spamassassin.cf line) and restart NoSpamToday.

Note 1: change example.com to whichever domain you want to check. Technically, you should put a backslash("\") in front of each dot, but leaving them out is unlikely to cause problems. (You do need a backslash in front of "@"s.) You could use more advanced regexps to put all the domains into one rule, but it's simpler having one set of rules per domain.

Note 2: you'll have to have one set of rule names per example: only one definition of a particular rule name will be used. So if you have alpha.example.com and beta.example.com, go for names like __LOCAL_ENV_FROM_ALPHA and __LOCAL_ENV_FROM_BETA

Note 3: This checks EnvelopeFrom, not From, which is what SPF checks anyway. There are occasions when non-spam email (for example, mail sent from a website at the request of one of your users to another of your users) will have a From address at your domain. These should have an EnvelopeFrom domain of the website, but occasionally, wanted email will still incorrectly have an EnvelopeFrom of your domain. For that reason, I wouldn't score this rule much over 3.0: matching spam is very likely to hit enough rules to stop it, but wanted email still has a chance of getting through.