How to avoid forged e-mails?

The From header of an e-mail, which you view in the header of e-mails can be anything, it doesn't even need to be a valid e-mail address and it can be different from the actual sender of the message.

For that reason, it's possible that you will receive forged e-mails as if they were sent from/to your account or from some other account in your domain to you. Usually, such emails, many times hoaxes or phishing attempts, are correctly caught as spam.

Let's start off enabling a rule that tries to catch e-mails sent from and to your account. So for example, From test@emailarray.com and To test@emailarray.com.

- Go to

  https://cp.emailarray.com
- Log in using your full e-mail address (user@domain.com) and current password.

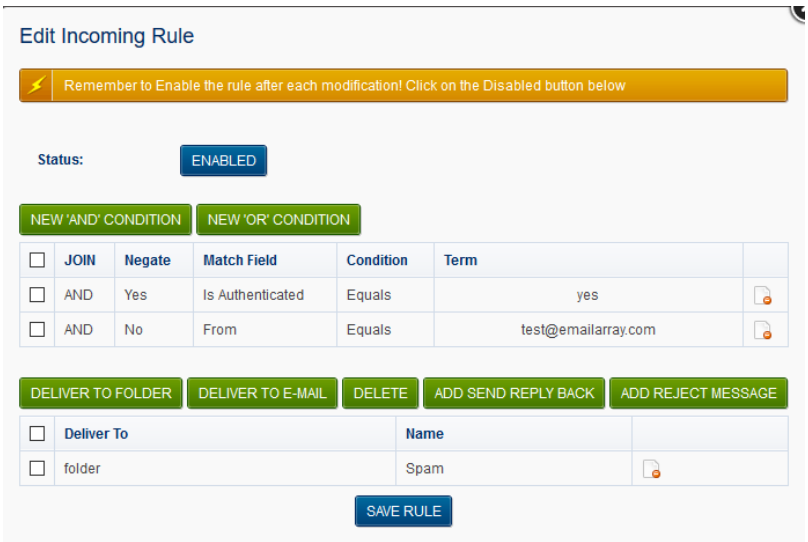
Alternatively, you can login to the user control panel using the respective link while logged to Webmail.

After logging in and click on **Filtering**, on the top bar.

Change the **Detect Forged From** pull-down menu to **Yes** and click on **Update settings**.

Afterwords, click on **Home** in the top bar, followed by the **Delivery Rules** icon.

You will notice a new rule entitled "DetectForgedFrom". Click on the **pencil icon** next to it, to edit it. This is what it looks like:



What the rule does is check if the user did NOT authenticate using our SMTP (notice that the Negate column for the first condition is set to Yes) and uses your address as a FROM address and in

such cases, it moves such e-mails to your spam folder.

This rule can currently be created only on the user level, however, if you decide to implement it for all your users, contact us, and we will enable it automatically for everyone.

One possibility is to change the folder where such e-mails are sent to. This will let you tweak the rule in an easier way. First of all, create a folder in WebMail or an e-mail client using IMAP, such as "Forged". Then, simply click on the **minus sign icon** next to the Spam folder action (shown above), click on **Deliver to folder** button and choose your "Forged" folder.

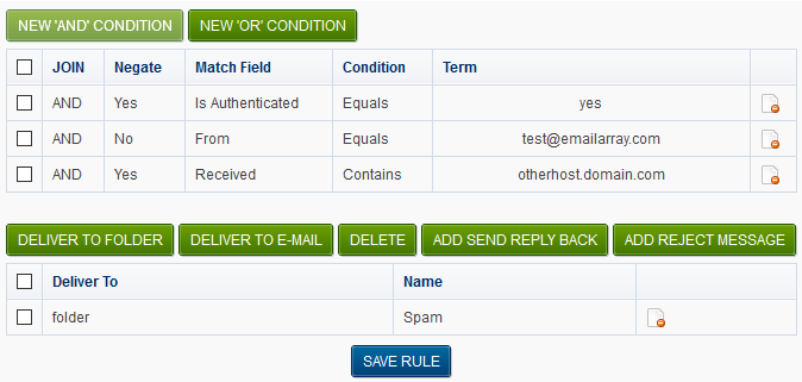
Notice that there's another rule entiled "SpamDelivery", responsible for moving spams to your spam folder and it comes before the Forged From rule. For that reason, forged e-mails detected as spam will be moved to your spam folder. If you decide to create a separate folder, such as the suggested "Forged folder", consider clicking on the **up arrow** next to the Forged From rule and moving this rule above the SpamDelivery rule. This way, all forged e-mails will be sent to your "Forged" folder, avoiding clutter in your spam folder.

Besides catching forged e-mails, this rule may catch legitimate messages that were send as being you, from some other SMTP server. For example, some website form or application that sends emails using your e-mail address in the From header.

You can tweak the rule by denying such cases, so the filter does not catch such cases.

For example, let's say you receive legitimate e-mails that come From your email and to your e-mail address, sent from a remote server called otherhost.domain.com, which is the hostname of the system that sends our server the e-mail, shown in the e-mail header. What we do is click on **New And Condition**. This new condition should have the **Match field** menu set to **Received** and **Negate Match** set to **Yes**. In the **term** field, type in otherhost.domain.com and click on **Add Condition**. Notice that rule is not set to Disabled. Click on the **Disabled** button to enable the rule and click on **Save rule**. What we did, is inform the system to NOT run the rule for e-mails that come from otherhost.domain.com.

This is how the rule now looks:



Let's consider one last scenario. Consider that you want to avoid forged e-mails coming from ANY account of your domain, not just your own account.

In such case, click on the **minus sign icon** next to the FROM condition and add a **New And Condition** of the **type FROM** and for **Term**, type in **your domain**, in this case "emailarray.com" (without quotes).

It might give you a bit of work to fine tune the rule so that it is near perfect, but many customers and companies consider it a good idea.

Revision #3
Created 21 August 2024 17:24:33 by Support
Updated 22 August 2024 16:54:07 by Support