safentrix

The World's ~~First~~ Best Free Email Security Service

User Guide

www.safentrix.com

Contents

Introduction

SAFENTRIX is a hosted Email security solution keeping Virus, SPAM and Phishers off your network, while ensuring that genuine emails can always reach the users. System administrators can easily setup SAFENTRIX for use with their domains in three easy steps.

SPAM protection is an on-going process with thousands of new category of SPAM being generated every day. While SAFENTRIX guarantees 99%+ SPAM effectiveness, it is still possible that small amount of emails are

- Wrongly classified as genuine when in fact they are SPAM
- Wrongly classified as SPAM when they are in fact genuine.

There are also times when SAFENTRIX blacklists an email server because it has sent SPAM. In this case, SAFENTRIX will reject any email from this blacklisted server. Once the administrator of the blacklisted email server fixes the SPAM issues, SAFENTRIX will need to start accepting emails from the mail server again.

SAFENTRIX provides automated processes to correct the above situations. This guide presents detailed steps on what is to be done in each of the above case so that normal functioning is restored.

Reporting SPAM

If a SAFENTRIX user receives a SPAM, it can be reported by forwarding the email to spam@safentrix.com. The SPAM feedback processor gets these emails, processes them and if it finds that it is indeed SPAM, changes the rule base as required.

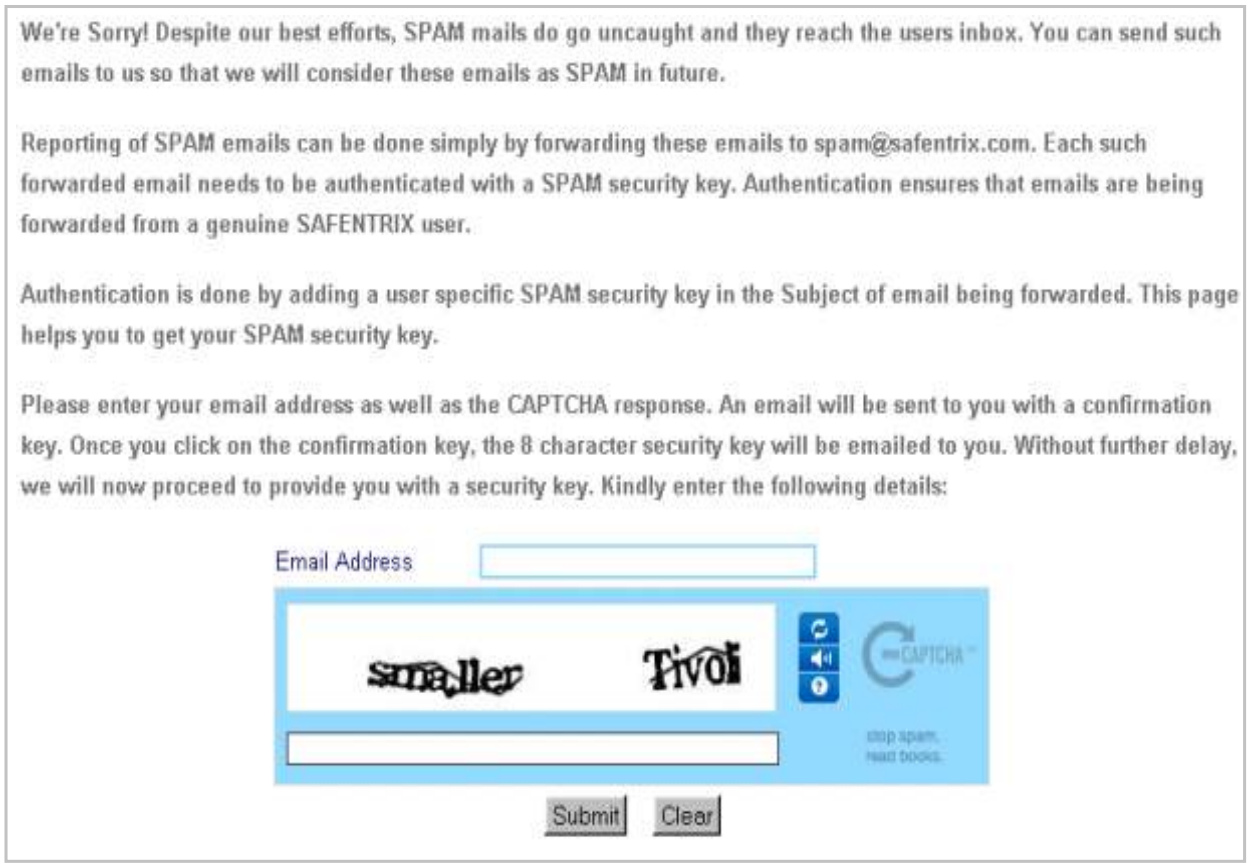
Once the rule base is changed, users would not receive such emails in future, as the system will classify them as SPAM and reject them.

SAFENTRIX SPAM feedback processor accepts emails only from genuine SAFENTRIX users. It ignores emails from any other senders. To ensure that user's SPAM feedback is processed (and not ignored), the user needs to get a SPAM Security key from SAFENTRIX portal.

Please note that the SPAM Security key is unique for each user and each user who wants to report SPAM should get their own Security key.

Getting Spam Security Key

To get user SPAM security key, visit http://www.safentrix.com/reportspam/getkey.php. That will display the following page:



Enter user's email address in the “Email Address” field and enter the correct CAPTCHA response.

If this email ID represents a valid SAFENTRIX user, an email will be sent to user's Email address and the following dialog will appear:

The user will receive an email as follows:

Once the email is received, user can confirm the request for Security key by clicking on the link included in Email. If the confirmation is successful, the SPAM Security key will be sent to your mail box. A sample email is given below:

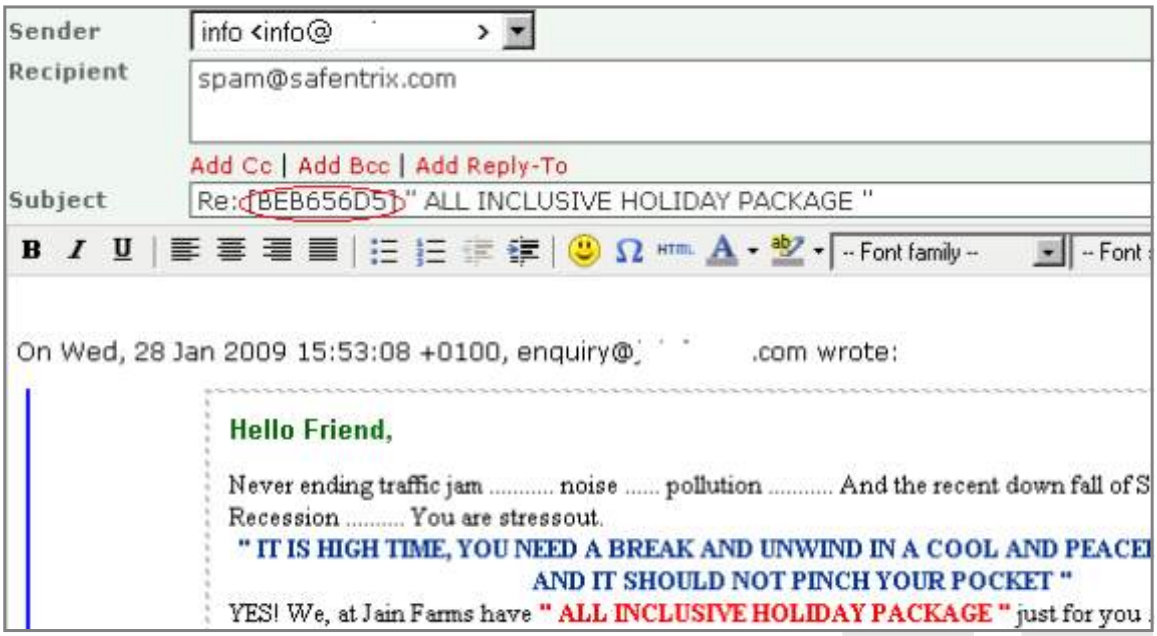
Forwarding SPAM

Once user gets a SPAM Security key from SAFENTRIX site, SPAM emails can be forwarded to spam@safentrix.com.

It is preferred that SPAM emails are forwarded using “Forward as Attachment” option. If the user's email client does not provide such an option, the SPAM email can be forwarded using the plain “Forward” option.

When forwarding add SPAM Security Key anywhere in the “Subject” line enclosed within “[ ]”. For example, if your SPAM security key is “BEB656D5”, add “[BEB656D5]” somewhere in the Subject of the SPAM email being forwarded.

An example of a SPAM being forwarded with SPAM Security key is given below:



In the above example, the included SPAM Security key is marked with a red Oval. Users must add their Security key similarly before forwarding SPAM emails.

Reporting False Positives

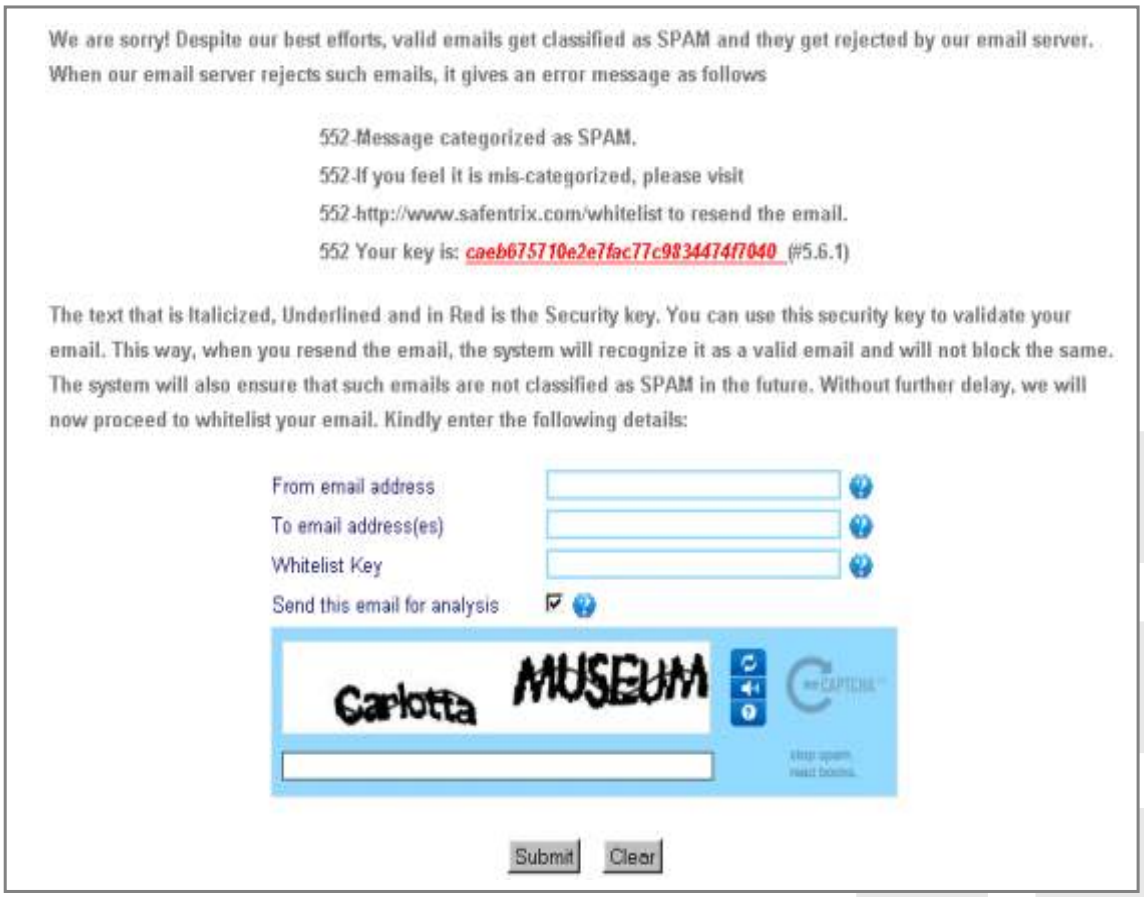
False positives are emails that are wrongly classified as SPAM by SAFENTRIX and rejected. SAFENTRIX rule base ensures near zero false positives. However, there are rare instances when genuine emails are classified as SPAM.In these cases, SAFENTRIX will reject the email and sender will get a notification as follows:

552-Message categorized as SPAM.
552-If you feel it is mis-categorized, please visit
552-http://www.safentrix.com/whitelist to resend the email.
552 Your key is: *caeb675710e2e7fac77c98344474f7040* (#5.6.1)

The sender can visit the page http://www.safentrix.com/whitelist, white list this email and resend the email. This time, the system will recognize this to be a valid email and deliver it to recipient.

Each rejected email will contain an unique Key (which is given in Red, underlined and Italicized above).

To whitelist the Email, goto http://www.safentrix.com/whitelist. That will bring up the following page:



Enter the details asked for, including

1. From address in the email (Sender's email address)
2. Email addresses to which the email was sent. If the email was sent to multiple email addresses, enter all the email addresses, separated by commas.
3. White list key. This will be present in the rejection message.
4. Correct CAPTCHA response.

Once all the details are entered, SAFENTRIX will whitelist the email. Sender can resend the email and it will reach the recipient without any delays. SAFENTRIX may also modify its rule base to not consider such emails as SPAM in future.

De-Blacklisting Email Server

SAFENTRIX maintains a proprietary Real time Blacklist (RBL). IP Addresses of email servers that

1. Send SPAM to a SAFENTRIX user
2. Send email to SAFENTRIX SPAM trap email address, or
3. Send email to SAFENTRIX Honey pot servers,

are added to the RBL. Once an address is listed in SAFENTRIX RBL, SAFENTRIX rejects all emails from these servers, irrespective of content.

While this is a good system, there are times when a “good” email server is Hijacked to send SPAMs. In this case, it is possible that even genuine emails from this server are rejected. This section explains the steps to be taken so that the email server is removed from the blacklist and normal mail traffic resumes.

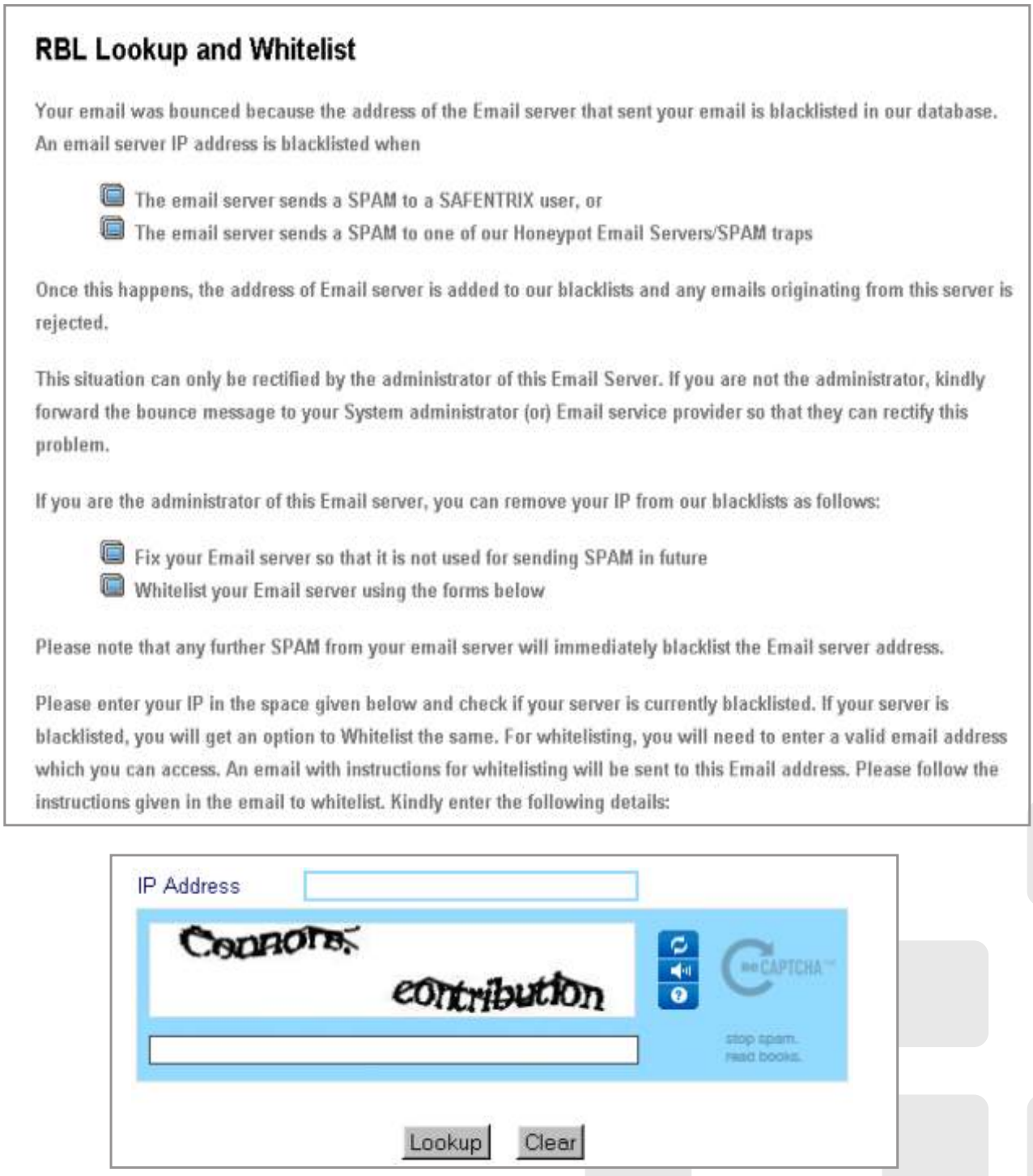
Kindly note that these steps can only be performed by the System administrator of Blacklisted email server. This means that if you are a sender whose Email was rejected due to blacklisting, please forward the bounce message to

1. Your organization's Email administrator, or
2. Support desk of your Email service provider.

If you are the administrator of the Email server that has been blacklisted, you may follow the steps below:

1. Please fix the problems that enabled your server to be used for SPAM.
   Goto http://www.safentrix.com/rbl

That will display the following page:



The first step is to find if your Email server IP is still blacklisted. To find out

1. Enter your Email server IP address in the “IP Address” edit field.
2. Enter the correct CAPTCHA response.

SAFENTRIX will check if the given address is blacklisted and if it is not blacklisted, give a message as follows:

In the above case, there is nothing further to be done.

If your Email server is blacklisted, you will receive a message as follows:

In the above case, SAFENTRIX will give an option to Whitelist (as in the following dialog):

You will need to

1. Enter a valid email address in the “Email Address” field.

Once this is done, you will get an Email with instructions for White listing in the specified email address. A sample email is show below:

Confirm the White listing by clicking on the Email link from the Email server. This is required to ensure that White list requests can be done only by the Email server administrator.

Once the White list request is confirmed, SAFENTRIX removes the email server address from its RBL and normal mail traffic resumes.

Please note that any future SPAM emails to SAFENTRIX will immediately add the server address to RBL.