

Get started with mailFence + spamFence

Pref	Hostname	IP Address
10	gw1.security.comendo.com	208.43.252
20	gw2.security.comendo.com	89.104.217
30	gw3.security.comendo.com	89.104.217

dns lookup ns lookup mx
Reported by ns1.hosting2.dk on Thursday, June 24, 2010

Comendo requests your DNS provider, on your behalf and with your permission, to point your domain(s) MX records at Comendo mailFence + spamFence clusters...

<input type="checkbox"/>	0	RE: Vedr.: FW: Multitelecons til Kirk...
<input type="checkbox"/>	4	Get that Higher Income you deserve for a...
<input type="checkbox"/>	0	ft
<input type="checkbox"/>	0	FR1@tenlog) is back up
<input type="checkbox"/>	0	RE: F-Secure
<input type="checkbox"/>	0	FR1@tenlog) is down
<input type="checkbox"/>	0	router's router config diff
<input type="checkbox"/>	0	vet
<input type="checkbox"/>	0	Re: [BFWA.77572.572] RE: Problem i Secur...
<input type="checkbox"/>	0	Vedr.: FW: Multitelecons til Kirk Vdr...
<input type="checkbox"/>	0	EURUSRV2(2@tenlog) is down

Once your MX records are pointing at Comendo mailFence + spamFence clusters, all e-mails are delivered to Comendo and displayed in the Comendo Security Center web-interface...



The mailFence + spamFence clusters filter all malicious and unsolicited E-mails, and then delivers the expected/ solicited e-mails...

Intro

This guide is in 3 parts

Part 1, "How scanning works", compares an e-mail environment without Comendo Security Services, with an e-mail environment using Comendo mailFence + spamFence.

Part 2, "Checklist", guides you through the necessary steps to setup Comendo mailFence + spamFence for your domain(s). Read this section to get started immediately.

Part 3, "Best Practices", provides information of how to use Comendo mailFence + spamFence correctly, and what to do in certain scenarios involving errors, failures or alike.

If you have any questions or concerns (not only in regard to this guide), please do not hesitate to contact our support at +971 444 65793 or co@comendo.com.

Content

Part 1: How scanning works.....	4
Normal setup.....	4
Comendo setup.....	5
Part 2: Checklist.....	6
Check your MX.....	7
Check your incoming server.....	8
Check your mailflow.....	10
Check your IP-restrictions.....	11
Help us help you.....	12
Part 3: Best Practice.....	13
Stateful firewall.....	14
What happened to my e-mail.....	15
White- and Blacklisting.....	19
Odd behavior.....	20
Contact information.....	21

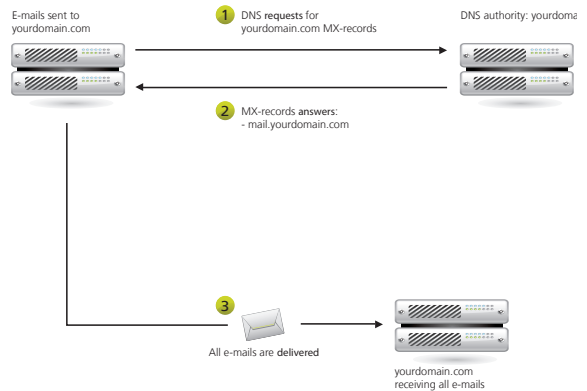
1 How scanning works

Normal setup

When an e-mail is sent from one mailserver to another mailserver through the internet, the following 3 steps apply:

1. The sending mailserver asks the responsible DNS server for the receiving domain (ie. yourdomain.com) where to deliver the e-mail. This information is kept in the MX records by the responsible DNS server.
2. The responsible DNS server sends the MX record information back to the sending server. The sending server now knows where on the internet it is supposed to deliver e-mails for yourdomain.com, which ie. could be mail.yourdomain.com.
3. The sending server finally delivers the mail to the MX records of that domain, which ie. could be mail.yourdomain.com

An MX record simply contains one or more destinations of a mailserver for any given domain.



1 How scanning works

Comendo setup

When an e-mail is sent from one mailserver to another mailserver that is protected by Comendo mailFence+spamFence, the following 4 steps apply:

1. The sending mailserver asks the responsible DNS server for the receiving domain (ie. yourdomain.com) where to deliver the e-mail. Only this time the MX record information points at Comendo mailFence+spamFence clusters.
2. The responsible DNS server for the receiving domain, ie. yourdomain.com, sends the MX record information back to the sending mailserver.

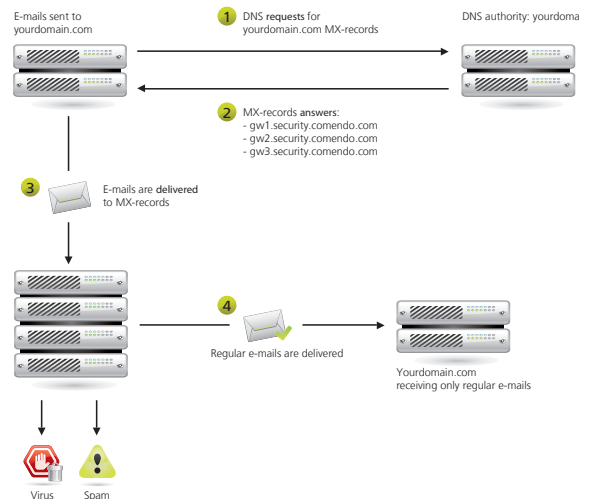
The MX records now contains the following Comendo mailFence+spamFence cluster addresses:

gw1.security.comendo.com
gw2.security.comendo.com
gw3.security.comendo.com

3. The sending server now delivers the mail to the MX records of that domain: Comendo
4. A Comendo mailFence+spamFence cluster receives the e-mail in question. At first the e-mail is checked for spam, and if classified as spam, the e-mail is quarantined.

If the e-mail is not classified as spam, the mail is then checked for known viruses, and if any virus found - the mail will not be quarantined but deleted.

If the e-mail has no viruses or is not classified as spam, the mail will finally be delivered to your mailserver which ie. could be mail.yourdomain.com



2 Checklist

If we take a look at the drawing in section 1 of this guide, we see what basic needs to be in place, and in which order:

1. MX records must contain Comendo addresses.
2. Comendo must know the address of your server.
3. Your firewall and mailserver must allow connections from Comendo IP-ranges.

This section contains troubleshooting instructions for your new Comendo mailFence + spamFence solution.

Keep in mind, that you can always contact Comendo support at +971 444 65793 or find help in our online helpdesk.

> <http://helpdesk.comendo.com>

Knowledgebase

Comendo mx records and ip range

portal.kb.public.top :: English : Mailscan :

Users with the following MX-records on their domain, can in their fire

Mx records:

- domain.tld. IN MX 10 gw1.security.comendo.com.
- domain.tld. IN MX 20 gw2.security.comendo.com.
- domain.tld. IN MX 30 gw3.security.comendo.com.

Our ip range:

- 89.104.216.0 Netmask: 255.255.255.0 (89.104.216.0-89.104.216.255)
- 89.104.217.0 Netmask: 255.255.255.0 (89.104.217.0-89.104.217.255)

2 Checklist

Check your MX

As mentioned in section 1 of this guide, a MX record is simply a “spread sheet” containing information. This sheet is part of a DNS zone, which is being managed by a given DNS server.

This DNS server can be your own inhouse server, or it can be a service you have bought elsewhere, which is common for small to medium-sized businesses.

If you are in doubt about who is hosting your DNS zone, do not forget that you can allways contact Comendo support at +971 444 65793.

Comendo support can assist to find your DNS provider, and also to contact them and ask for the MX record change on your behalf.

Changing an MX record usually takes about 12-24 hours.

You can allways check you MX records at:

> <http://www.mxtoolbox.com>

If you manage your own MX records, you should then change your MX record(s) to those shown in the picture above:

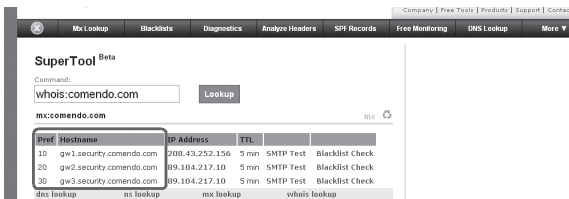
10	gw1.security.comendo.com
20	gw2.security.comendo.com
30	gw3.security.comendo.com

If your DNS hosting company has provided you with a webinterface / control panel, the DNS hosting company most likely expects you to change your MX records on your own.

If you need help with that, call Comendo support. We can either ask your DNS hosting company to make the changes, or we might be able to perform the changes for you, if we get your login to that control panel.

Information about Comendo MX records and IP-ranges and a more technical guide to troubleshooting incoming e-mails are available at the Comendo helpdesk:

> <http://helpdesk.comendo.com>



The screenshot shows the SuperTool Beta web interface. At the top, there is a navigation bar with links for 'Company', 'New Tools', 'Products', 'Support', and 'Contact'. Below this, there is a menu with options: 'MX Lookup', 'Blacklists', 'Diagnostics', 'Analyze Headers', 'SPF Records', 'Free Monitoring', 'DNS Lookup', and 'More'. The main content area displays the results of a 'whois:comendo.com' lookup. The command input field shows 'whois:comendo.com' and a 'Lookup' button. Below the command, the domain 'mx.comendo.com' is listed. A table of MX records is shown with columns for 'Pref', 'Hostname', 'IP Address', 'TTL', 'SMTP Test', and 'Blacklist Check'. The table contains three rows of data. At the bottom of the screenshot, there are several small icons and labels: 'dns lookup', 'mx lookup', and 'whois lookup'.

Pref	Hostname	IP Address	TTL	SMTP Test	Blacklist Check
10	gw1.security.comendo.com	208.43.252.156	5 mn	SMTP Test	Blacklist Check
20	gw2.security.comendo.com	89.104.217.10	5 mn	SMTP Test	Blacklist Check
30	gw3.security.comendo.com	89.104.217.10	5 mn	SMTP Test	Blacklist Check

2 Checklist

Check your incoming server

Assuming the MX records now points at Comendo all your e-mails are then received, scanned and filtered by Comendo.

Everything else than spam and malicious e-mails will now be delivered to your mailserver. In order for Comendo to deliver these e-mails, Comendo must know the address of your mailserver.

Go to your Comendo Security Center

> <https://security.comendo.com>

Then browse through the menus as follows;

mailFence/spamFence -> Settings -> Account.

In this section you will find a field called "Incoming server".

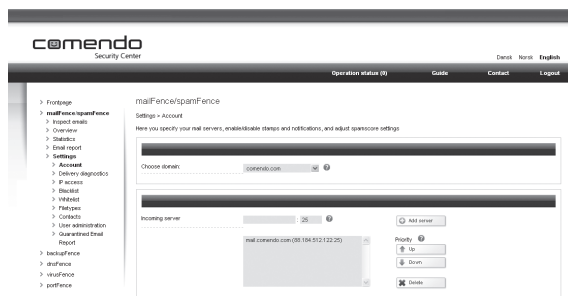
The address (IP address / hostname) of your mailserver must be in this list, and this will be the mailserver to which Comendo delivers the scanned e-mails.

Check the servername to ensure it is correct. If the current server is not correct, delete the address from the list and type in the correct address in the field above the server list.

It is possible to have more than one mailserver on the list.

Comendo will then try and deliver all e-mails to the first address listed, and if the connection fails to this server, Comendo will try and deliver e-mails to the next server and so on.

All changes made in this part of the Comendo Security Center takes up to 30 minutes to apply.



Once you confirmed the address of your mailserver is correctly typed into the "Incoming server" list go to the following menu:

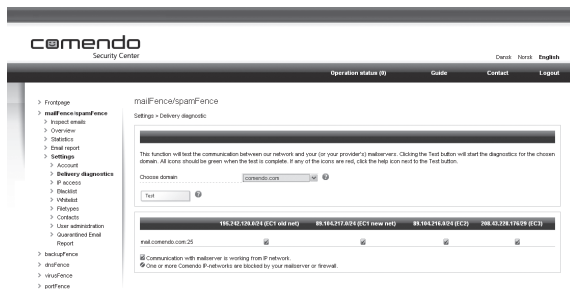
mailFence/spamFence -> Settings -> Delivery diagnostics

In here you will see your domain in the drop-down menu and you can now click "Test".

This test creates a telnet connection from each of the 4 Comendo mailscanning clusters towards your mailserver, and this is indicated by either a red or green icon

2 Checklist

below each cluster, stating whether a connection failed or succeeded.



If the result is four green icons, there are no problems for Comendo to deliver your e-mails.

If one or more tests are red, Comendo cannot deliver e-mails to your mailserver from these clusters.

This can either be a restriction in your firewall or a restriction on your mailserver.

In this matter, you must allow connections in your firewall and on your mailserver from the following IP-ranges:

89.104.216.0/24	Netmask: 255.255.255.0
89.104.217.0/24	Netmask: 255.255.255.0
195.242.120.0/24	Netmask: 255.255.255.0
208.43.228.176/29	Netmask: 255.255.255.248

You can also find them on the Delivery diagnostics page when you click the "test" button.

Information about Comendo MX records and IP-ranges and a more technical guide to troubleshooting incoming e-mails are available at the Comendo helpdesk:

> <http://helpdesk.comendo.com>

Please note that if you have your mailserver hosted by another company, and if you do not manage the mailserver or firewall your self the company hosting these services must check if the mentioned IP-ranges is allowed in your firewall and on your mailserver.

2 Checklist

Check your mailflow

Assuming your domains' MX records are now pointing at Comendo and your mailserver accepts connections from the earlier mentioned IP-ranges, you can now use the Comendo Security Center webinterface to check your mailflow.

In the Security Center click on:

mailFence/spamFence -> Inspect e-mails

You should now get a screen similar to this:

The screenshot shows the Comendo Security Center interface. The main content area is titled 'mailFence/spamFence' and 'Inspect e-mails'. It includes a search bar with fields for 'Domain', 'Date', 'Time (HH:MM)', 'Spam score', 'Search on email address', and 'Search on subject'. Below the search bar is a table of email inspection results. The table has columns for 'Type', 'Score', 'Subject', 'From', 'To', and 'Time &'. The results list various email types such as 'Virus', 'Spam', and 'Phishing' with their respective scores and subjects.

Type	Score	Subject	From	To	Time &
0	RE Virus - FVX_Multibolensia (1)AV		homer.k@ip...	homer.k@ip...	2010-09-24 15:07
4	Cellular spider scanner you share for a...		homer.k@ip...	homer.k@ip...	2010-09-24 15:05
0	if		charles@stet...	charles@stet...	2010-09-24 15:03
0	FH@Bnkspj is back up		ic@comendb.com	homer.k@ip...	2010-09-24 15:02
0	RE F-Serve		ic@comendb.com	homer.k@ip...	2010-09-24 15:02
0	FH@Bnkspj is down		ic@comendb.com	homer.k@ip...	2010-09-24 15:01
0	realtime center config file		homer.k@ip...	ic@comendb.com	2010-09-24 15:00
0	vet		charles@stet...	charles@stet...	2010-09-24 15:00
0	Re: [HWS] 27252-072:RE: Problem Secur...		support@secu...	charles@stet...	2010-09-24 14:59
0	Virus - FVX_Multibolensia (1)AV		homer.k@ip...	homer.k@ip...	2010-09-24 14:58
0	EUPOSPV2@Bnkspj is down		ic@comendb.com	homer.k@ip...	2010-09-24 14:58
0	FH@Bnkspj is back up		ic@comendb.com	homer.k@ip...	2010-09-24 14:58
0	EUPOSPV2@Bnkspj is down		ic@comendb.com	homer.k@ip...	2010-09-24 14:58
0	www.burtonvector.com(Bnkspj) is down		ic@comendb.com	homer.k@ip...	2010-09-24 14:58
0	webtest		charles@stet...	charles@stet...	2010-09-24 14:58
0	RE: Phishing Service Request #251234 ba...		bruce.chr@en...	bruce.chr@en...	2010-09-24 14:57
0	SPAM		homer.k@ip...	ic@comendb.com	2010-09-24 14:56
0	Virus - Comendo - SWX		ic@comendb.com	homer.k@ip...	2010-09-24 14:55

Click on an e-mail in the list to read your mailserver's response.

If your e-mail flow contains a lot of e-mails marked with red question marks, your mailserver is not accepting connections from the earlier mentioned IP-ranges.

If your e-mail flow contains lots of e-mails marked with grey hourglasses, your e-mail server is either not responding, responding very slowly, or lacks sufficient system resources to accept the e-mails in question.

There are many different responses depending on which mailserver you are using and which version, why there might be errors that are not mentioned within this guide.

If you have any concerns or questions, contact support.

2 Checklist

Check your IP-restrictions

As mentioned earlier; when a sending mailserver sends an e-mail to another server, the sending mailserver usually makes a DNS request to the receiving domains' DNS authority, to get the address of the receiving mailserver.

What if a spammer tries to send spam directly to your mailservers' IP-address dodging Comendo mailFence + spamFence?

You can set up your firewall and mailserver to only receive e-mails from our IP-ranges.

Please note that if you have your firewall or mailserver hosted by an another company and if you do not manage these yourself you may not be able to make these restrictions in the firewall or on the mailserver.

If everything works fine

Assuming everything works fine; your e-mail flow is OK, and your mailserver is receiving the wanted amount of e-mails, you can now setup your firewall and mailserver to deny connections anything else than the following four IP-ranges, which are the same as earlier;

89.104.216.0/24	Netmask: 255.255.255.0
89.104.217.0/24	Netmask: 255.255.255.0
195.242.120.0/24	Netmask: 255.255.255.0
208.43.228.176/29	Netmask: 255.255.255.248

You can always find the IP-ranges in the Security Center -> Delivery Diagnostics section, by clicking the "test" button

Information about Comendo MX records and IP-ranges is also available at the Comendo helpdesk:

> <http://helpdesk.comendo.com>

2 Checklist

Help us help you

At this point your new mailFence + spamFence product should be running.

Comendo is now scanning all your e-mails, filter unsolicited mails as spam and quarantines those, deletes e-mails containing viruses, and delivers the expected amount of e-mails to your server.

What else is there to check?

Maybe you have some suggestions for improvements, bugs to report or maybe ideas for a new feature?

Does your business receive important e-mails from domains that are known for sending a lot of spam like hotmail?

Maybe you do a lot of business in Asia which is not known for having the best reputation in regard to spam?

Keep an eye on your mailflow during the upcoming days and see if you notice any e-mails that Comendo considers being spam but you know is not.

No one knows your daily e-mails better than you do.

Call us! Let us know!

We will do everything we can to ensure you have the best possible experience with Comendo mailFence + spamFence.

Comendo Security Support:

Phone: +971 444 65793

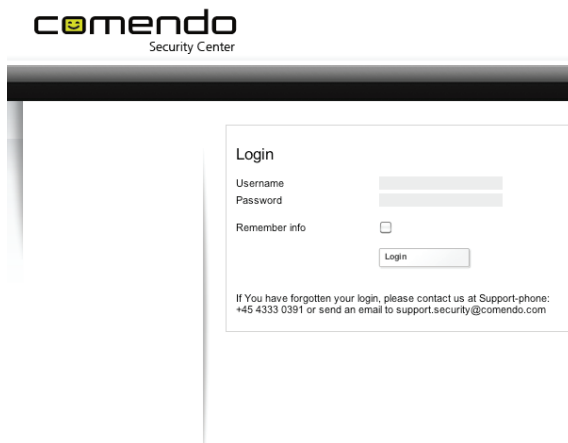
E-mail: co@comendo.com

3 Best Practice

In section 1 of this guide we go through how a normal mailflow works and in contrast how a mailflow with Comendo mailFence + spamFence works.

In section 2 we provide you with a checklist of which most important parts to pay attention to regarding the setup of mailFence + spamFence.

In this section we will look at how e-mails are handled within the Security Center and how you can troubleshoot these to identify or locate a problem.



3 Best Practice

Stateful firewall

If you have a stateful firewall and are experiencing problems with e-mail delivery, you should disable Stateful Packet Inspection (SPI) or 'SMTP inspection'.

Read more about Stateful Firewalls at Wikipedia, the free encyclopedia on the internet.

> <http://en.wikipedia.org>



The screenshot shows the Wikipedia article for 'Stateful firewall'. At the top left is the Wikipedia logo with the text 'WIKIPEDIA The Free Encyclopedia'. Below it are navigation links: 'Main page', 'Contents', 'Featured content', 'Current events', and 'Random article'. There are three main sections: 'Interaction' (with sub-links like 'About Wikipedia', 'Community portal', 'Recent changes', 'Contact Wikipedia', 'Donate to Wikipedia', 'Help'), 'Toolbox', and 'Print/export'. A 'Languages' section lists 'Deutsch' and 'Piemontèis'. The main content area has the title 'Stateful firewall' and the subtitle 'From Wikipedia, the free encyclopedia'. The text begins with 'In computing, a **stateful firewall** (any firewall th... legitimate packets for different types of connect...'. Below the text is a 'Contents' table of contents with links to '1 History', '2 Description', '3 Application-level filters', '4 Pitfalls' (with sub-links '4.1 Incompatibilities' and '4.2 Vulnerabilities'), '5 See also', and '6 References'. The 'History' section is partially visible at the bottom, starting with 'Credit to the inventor of the stateful firewall is us...' and 'Before the advent of stateful firewalls, a *statele*...'.

3 Best Practice

What happened to my e-mail

You can view and search your mailflow in the Security Center by clicking on:

mailFence/spamFence > Inspect e-mails.

When you want to know what happened to an e-mail, go to this menu and then search for the e-mail.

The symbol to the left of the e-mail gives an indication of how it has been handled by Comendo. Click on the e-mail for more details.

Comendo by default logs all your e-mails for 14 days unless other agreements have been made. Furthermore spam e-mails that are quarantined can be released within this timeframe.

Everything older than 14 days is deleted and cannot be retrieved.

If the e-mail you are looking for is not located in the Security Center, Comendo most likely did not receive the e-mail or the e-mail is older than 14 days and therefore it no longer exists in the log.

If Comendo rejects an e-mail before trying to deliver it to your server, the sender of that e-mail has received a reject message from Comendo stating why this message was not accepted.

This happens in few scenarios which could be as following:

- The senders IP-address is blacklisted as a known spammer.

Find more information about blacklisted e-mails at Wikipedia, the free encyclopedia on the internet.

> <http://en.wikipedia.org>

- The sender does not meet the requirements/ RFC standards that has been defined by IETF.

For more information about IETF visit

> <http://www.ietf.org>

For more information about RFC visit

> <http://www.ietf.org/rfc.html>






Some specific RFC's for using SMTP on the internet can be found here:



> <http://www.ietf.org/rfc/rfc2821.txt>

> <http://www.ietf.org/rfc/rfc2822.txt>

3 Best Practice

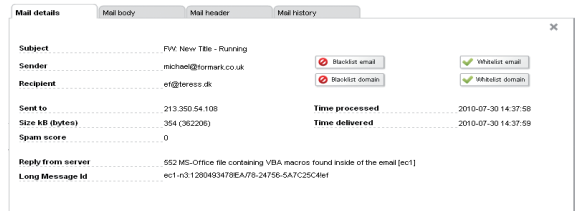
When you find the e-mail look at the symbol to the left to get an indication of what sort of mail it is.

-  This is a normal e-mail. It has been delivered to your e-mail server.
-  This e-mail is quarantined as spam. If you want to received the e-mail, you can click on it to open the information window, and then click on the "Release" button at the bottom to the right.
-  This e-mail contained a virus. It has been deleted from our systems. We cannot send it to you.
-  We are unable to send this e-mail to you at the moment. We will try to resend this e-mail over the next 7 days before we give up. If your server is down, we automatically keep your e-mail safe until your server is back online (if within 7 days).
-  This e-mail was rejected by your server. It has been deleted from our systems. We cannot send it to you. Our systems have sent an automatic reply (a "bounce message") about this to the sender.





-  The sender of e-mail is blacklisted and the e-mail is quarantined. If you want to receive the e-mail, you can click on it to open the information window, and then click on the "Release" button at the bottom to the right.
-  The sender of this e-mail is whitelisted. No e-mails from this sender will ever be quarantined as spam. It has been delivered to your e-mail server.

In all the above cases you can click on the e-mail for more information.

By clicking on an e-mail a pop-up will appear, displaying detailed information about this specific e-mail.



The screenshot shows a pop-up window titled "Mail details" with tabs for "Mail body", "Mail header", and "Mail history". The "Mail header" tab is active, displaying the following information:

Subject	FW: New Tbe - Running		
Sender	michael@formark.co.uk	 Blacklist email	 Whitelist email
Recipient	e@freesk.dk	 Blacklist domain	 Whitelist domain
Sent to	213.350.54.108	Time processed	2010-07-30 14:37:58
Size KB (bytes)	354 (362206)	Time delivered	2010-07-30 14:37:59
Spam score	0		
Reply from server	502 MS-Office file containing VBA macros found inside of the email[ec1]		
Long Message Id	ec1-c031280493479EA79-24756-5A7C25C4ef		

3 Best Practice

The following details are available:

- Subject of the e-mail
- Sender e-mail address
- Recipient e-mail address
- The mailserv Comendo delivered the e-mail to or tried to deliver to.
- The size of the entire e-mail (incl. attachments, text, pictures, signatures etc.)
- Time and date the e-mail was recived by Comendo.
- Time and date the e-mail was delivered to your server.
- The by Comendo assigned spamscore (0 for not spam).
- The reply from your mailserv (failed, accepted, delayed, queued etc.)

Of special interest is "Reply from server". This is how your mailserv responded when Comendo delivered (or tried to deliver) the e-mail to your server.

In regard to this, the following can be worth noticing: A mailserv allways responds with an SMTP code, which typically is:

- 2xx
The e-mail was accepted for delivery.
- 4xx
The e-mail is temporarily rejected by the mailserv and Comendo will try and deliver the e-mail later.
- 5xx
The e-mail was permanently rejected by the mailserv and the e-mail will not be delivered.

Specific examples of the 3 scenarios:

```
250 2.6.0  
<7FECAEAE-151B-4E36-8707-F68C684959A1@me.com> Queued mail for delivery
```

The mailserv accepted the e-mail and queued it internally for delivery. (This is a typical Microsoft Exchange response)

```
452 4.3.1  
Insufficient system resources
```

The mailserv is too busy to accept the e-mail or it is lacking ressources such as disk space, memory or maybe even CPU power.

3 Best Practice

550 5.1.1

User unknown

In this situation the mailserv has no mailbox for that recipient and therefore rejects the e-mail permanently.

If an e-mail is rejected by your mailserv or if Comendo for some reason can not deliver the e-mail to your mailserv, this information can give you a hint of where the problem might be.

Body, header and history

In the pop-up you will also find some tabs in the top of the window.

“E-mail body” can be used to see what is inside an e-mail. This is only possible for e-mails that has been quarantined as spam.

The purpose of this is to see if the content is malicious or not, before the e-mail is released to the final recipient.

“E-mail header” contains information about the origins of the e-mail. This is only available for quarantined spam e-mails.

The purposes are many, but mostly to identify where the e-mail actually came from originally.

“E-mail history” contains delivery information.

The purpose of this, is to see if an e-mail has been tried delivered several times and therefore is delayed, or maybe to check different responses from your mailserv in relation to troubleshooting.

3 Best Practice

White- and Blacklisting

E-mails that are spam quarantined by Comendo might not be considered as spam by you or the recipient within your organisation.

Whitelist

To make sure that you are always receiving all the right e-mails, you can whitelist a specific sender address or you can whitelist the entire sender domain. This is done in the menu by clicking on:

mailFence/spamFence -> Settings -> Whitelist.

This allows an e-mail to be delivered to you even though Comendo considers it being spam.

Considerations are advised when using the whitelist:

Most spam is what we call "spoofed e-mails". Spoofed e-mails are e-mails with a fake sender address which typically is your domain. Then e-mails look like they come from your own domain.

In this regard, it is not recommended to whitelist your entire domain. Most often when a user sends an e-mail to another user on the same domain the e-mail is not passing the internet. Therefore there is no reason to whitelist your own domain.

Another consideration to be made is about known public free mailservices such as hotmail.com, gmail.com, aol.com, yahoo.com etc.

Lots of spam looks like it is coming from these mail-services but in most cases these are spoofed addresses as well. Whitelisting the entire hotmail.com domain will result in you receiving lots of spam.

If you need to whitelist some hotmail.com address it is recommended to whitelist the specific e-mail address such as donald.duck@hotmail.com and not @hotmail.com.

Blacklist

Using the blacklist has the opposite effect. A blacklisted sender will not be able to deliver e-mails to you.

The blacklist is used to prevent receiving specific e-mails like newsmails or other unwanted e-mails. By blacklisting the e-mail address or the entire sender domain the user will no longer receive the unwanted e-mails.

If a new type of spam attack occurs the filter will quickly adapt to this and in a very short time be able to filter these new types of spam as well.

It may be helpful in a beginning of a new type of spam attack to blacklist the spammer until the filter has fully adapted to this new spam. This scenario is though very rare.

3 Best Practice

Odd behavior

It could happen that some e-mails are delivered more than once. It could happen that some e-mails are queued although other e-mails are delivered without a problem. What should you do when you experience such odd behaviour?

Start troubleshooting by using the Security Center. Click on:

mailFence/spamFence -> Settings -> Delivery diagnostics

Use the test to check if your firewall and mailserver is accepting e-mails from the Comendo mailFence + spamFence IP-ranges.

Check your mailflow for errors and check you mailserver response if any e-mails have errors in the Security Center.

Alternatively you can check the e-mail header to track down eventual problems. This does however require more advanced knowledge of e-mails.

Read more about e-mail headers at Wikipedia, the free encyclopedia on the internet.

> <http://en.wikipedia.org>

Do not hesitate to contact support for help or questions.

3 Best Practice

Contact information

Your organisations contact information is available in the Security Center. Click on:

mailFence/spamFence -> Settings -> Contacts

Keep your contact information up to date, especially your contact e-mail.

We use your contact information when we send you privileged information. When updating your contact information, you should consider the following situations:

If the contact person is on holiday who should we contact instead? Add that contact.

If your server is down should we send privileged information to an alternative e-mail address? Add that address.

Consider using a group e-mail as contact address such as `comendo.contact@yourdomain.com`.

Comendo Security Support

Phone: +971 444 65793

E-mail: co@comendo.com