Connect smarter. Anywhere.

# SkyFile Mail v10
# Virus & Spam filter

June 2018
Ref: Version 10

# Table of contents

## 1. INTRODUCTION

Our messaging services SkyFile Mail and SkyFile C include all the features needed to eliminate viruses and spam on the bases of typical properties (Blocked HELO, greylisting etc.). This is very important, as the number of spam/viruses is rising constantly. Viruses and spam represent more than 70% of the global email traffic.

SkyFile Mail and SkyFile C also recognise mutating viruses: These are self-changing viruses which appear with permanently changing different attachment names and sizes, subject lines, etc. Even a possible return mail from the land-side server will be blocked to protect SkyFile Mail's customers against paying for this unwanted mail.

Filtering spam is not an easy job, and not an exact science either. Spam detection in the SkyFile Server is a multi-stage process and it includes heuristic mechanisms as well as handmade word-filtering. Detection and scoring algorithms are the result of years of spam analysis and are also frequently adapted to new spam waves.

The SMTP server can reject emails in real-time during the delivery process so that the sender immediately knows that the delivery failed. Often more than 50% of all emails are rejected during the SMTP dialogue.

After a mail is received by the SMTP server, the mail gateway decodes the components and checks each of them. The filtering process used by Marlink is based on a score of different parameters.

The mail is blocked with a return mail if the score sum is overpassing a certain limit defined by Marlink's Team.

## 2. WHAT IS A "COMPUTER VIRUS"?

A computer virus is a type of malicious software program (malware) that, when executed, replicates itself by modifying other computer programs and inserting its own code. When this replication succeeds, the affected areas are then said to be "infected" with a computer virus.

## 3. WHAT IS SPAM?

Email spam, also known as junk email, is a type of electronic spam where unsolicited messages are sent by email.

Many email spam messages are commercial in nature but may also contain disguised links that appear to be for familiar websites but in fact, lead to phishing websites or sites that are hosting malware. Spam email may also include malware as scripts or other executable file attachments, also named "trojans"

## 4. CUSTOMISED FILTERS

In addition to the above described general filters, SkyFile Mail provides individual filters like black & white lists, subject keywords or size-limits (global or per sender) to gain additional individual security. It enables each customer to define exactly who can send what sort of emails to the SkyFile Mail or SkyFile C account. Both options can be configured by the customer himself, thus customers can create the maximum protection for their own email accounts!

Furthermore, a “Black & white list virus control” has been incorporated into SkyFile Mail (and SkyFile C). This fairly new feature allows you to receive a rejection notification if a shore-to-ship email has been filtered by the SkyFile server.

Thanks to our “P360” web-portal, a shipping-company or a partner can easily manage and control the filter in place on a vessel or a fleet.

SkyFile Mail Premium users benefit from a service of Quarantine. Mail usually rejected by the system are put in quarantine. They are visible and manageable via “P360”. Authorised people can easily reject/remove the mail from the system or force the delivery to the ship.

## 5. SKYFILE ANTI VIRUS

In addition, Marlink provides an efficient anti-virus system/software based on SOPHOS technology. This company provide anti-virus systems to big companies around the world. Thanks to the SOPHOS Labs, our customers benefit from high expertise and extensive experience in combating viruses. Their experts are permanently working on making the systems more secure and better protected.

SkyFile Anti-Virus delivers, via email, daily updates to their subscribers making a vessel at deep sea protected as if it was connected to a corporate network. The anti-virus engine is updated regularly with our Over the Air (OTA) update service. Therefore, no need for going on-board to perform manual updates of the system. OTA update is available for monthly and yearly engine updates.

## 6. RECOMMENDATIONS FOR SENDERS

Terrestrial senders wishing to deliver emails to SkyFile customers should be aware of the following rules:

- Never activate a mail forwarding from another server to a SkyFile Account. This breaks most of the anti-spam mechanisms since the original sender data like IP address or HELO are no longer visible to the SkyFile server
- To avoid being blacklisted, dial-up customers should always send mails through their provider’s SMTP smart-host which typically has a static IP address
- Mail servers should strictly respect the Internet standards as defined in RFC documents. For instance, they must send a valid domain name behind the HELO command, and mail should be retried properly to avoid problems with “Greylisting”
- White-listed email addresses or domain-names get a lower score in case of spam-detection. Marlink strongly recommends using the filtering processes available in P360. White-listing an email-address or a domain-name is always beneficial for the users as it reduces the risk of blockage

## 7. WHAT IS “GREYLISTING” METHOD?

Greylisting is a method of defending email users against spam. A mail transfer agent (MTA) using greylisting will “temporarily reject” any email from a sender it does not recognize. If the mail is legitimate, the originating server will try again after a short delay, and if sufficient time has elapsed, the email will be accepted.

The main advantage from the users' point of view is that greylisting requires no additional configuration from their end. If the server utilizing greylisting is configured appropriately, the end user will only notice a delay on the first message from a given sender, so long as the sending email server is identified as belonging to the same whitelisted group as earlier messages.

If mail from the same sender is repeatedly greylisted it may be worth contacting the mail system administrator with detailed headers of delayed mail.

Marlink and the SkyFile Development Team developed, maintained and controlled all these rules for the security and the peace of the SkyFile users. However, from time to time, the system happens to create false positive (emails blocked while they should have been transferred). As indicated at the beginning of this document, filtering spam is not an exact science. It can happen and, although it might be annoying, it is a normal behaviour.

Marlink is always listening to the SkyFile' users and tries to rectify, change or adapt the rules when it is necessary and possible.

## 8. WHAT TO DO IN CASE OF MAILS QUARANTINED?

When an email is filtered, blocked by the system and quarantined, the sender and also the shipping-company, owner of the account receives a notification. The sender understands that the email has been blocked and quarantined. He also knows that it is not necessary to send the mail again. The shipping company, receives a notification saying that a mail has been quarantined and that it can be easily either deleted or delivered anyway to the recipient (the ship).

Therefore, the decision is given to the shipping-company. Via P360, the user can consult the list of quarantine emails for the fleet or for each single email accounts. From that point, the user decides if the mail is suspicious or dangerous (in that case the email might be deleted), or if the mail is good and secure (in that case the email might be delivered to the vessel anyway by a simple click)

Users considering that the email has been filtered by mistake (false positive) can contact Marlink's Service Desk. The security team will study the case and make changes if possible and/or necessary.

## 9. CONCLUSION

Currently there are about 100,000 different viruses and these are increasing every day with even more sophisticated methods. Consequently, we cannot guarantee a 100% blockage of viruses and spams, but as we've got intelligent and flexible algorithms, we are always technically in advance! To eliminate new threats that appear on the web, our anti-spam anti-virus algorithms are constantly adapted.

## 10. NEED SUPPORT?

If you have any questions, please contact your Key Account Manager or Marlink Service Desk:

| | |
|---|---|
| Email**:** | servicedesk@marlink.com |
| EMEA: | +33 (0)1 70 48 98 98 |
| Americas: | +1 (310) 616-5594 |
| | +1 855 769 39 59 (toll free) |
| Asia Pacific: | +65 64 29 83 11 |