Impersonation Protection (Whaling & Phishing Highlight)

×NOTE: In versions prior to 4.7 this menu was named “Whaling and Phishing Highlight”, starting from 4.7 it is named “Impersonation Protection”

Phishing Highlight

Phishing Attacks look like a genuine email message from someone that looks like a trusted sender, like your bank for example, which contain a link to click on to take you to the web site where you will be asked to type in personal information such as your account number or credit card details, or any other personal information.

Common frauds are already blocked by Libraesva ESG as spam or phishing messages, this check helps you alerting your users with ‘unsafe’ links. These links are those where the real address of the link in the message is not the same as the text that appears to be the link; or are simply numeric links, very hard to understand.

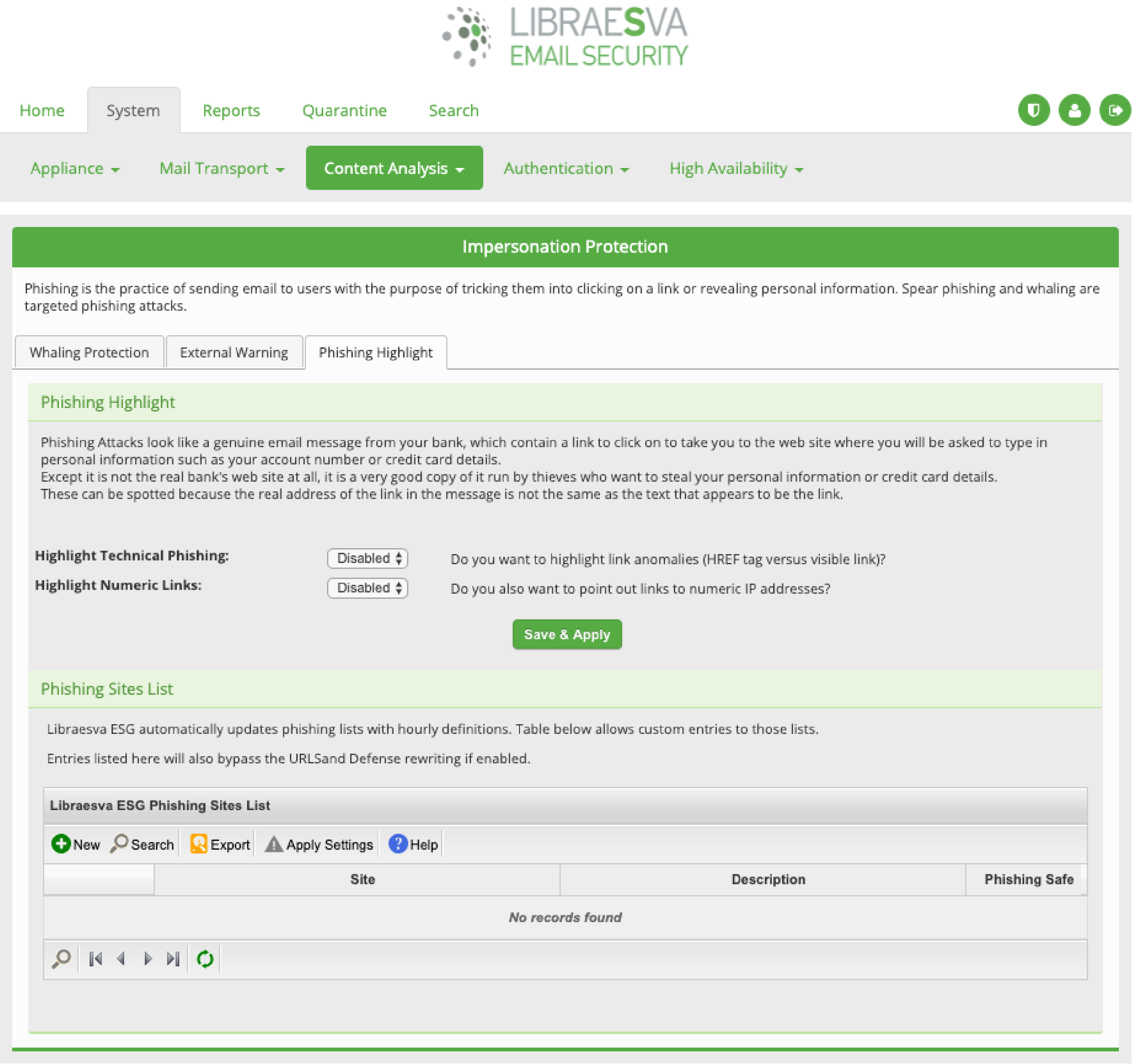
You have two options here:

- Enable or disable ‘unsafe’ link checks (Find phishing frauds)
- Enable or disable Numeric links highlight

When these settings are enabled and Libraesva ESG finds an unsafe link, will simply prepend a red string alerting the user about the following link.

Libraesva ESG keeps a regular updated list of known Bad Phishing sites and Safe Phishing sites, but for obvious reasons these lists cannot be comprehensive of all cases. For this reason it is possible add custom entries to avoid inline Phishing Warnings for safe sites, like for example intranet websites. Or you can explicit add Bad Phishing Sites.

Please take note that for standard port 80 and 443 there’s no need to specify port, otherwise the correct syntax is <ip>:<port> (e.g. 1.1.1.1:8080)



Impersonation Protection

Phishing is the practice of sending email to users with the purpose of tricking them into clicking on a link or revealing personal information. Spear phishing and whaling are targeted phishing attacks.

Phishing Highlight

Phishing Attacks look like a genuine email message from your bank, which contain a link to click on to take you to the web site where you will be asked to type in personal information such as your account number or credit card details.
Except it is not the real bank's web site at all, it is a very good copy of it run by thieves who want to steal your personal information or credit card details.
These can be spotted because the real address of the link in the message is not the same as the text that appears to be the link.

Highlight Technical Phishing: Disabled — Do you want to highlight link anomalies (HREF tag versus visible link)?

Highlight Numeric Links: Disabled — Do you also want to point out links to numeric IP addresses?

Phishing Sites List

Libraesva ESG automatically updates phishing lists with hourly definitions. Table below allows custom entries to those lists.

Entries listed here will also bypass the URLSand Defense rewriting if enabled.

Libraesva ESG Phishing Sites List

	Site	Description	Phishing Safe
		No records found	

×**NOTE:** You can customize the inline warning string from menù *System->Logo and Messages Customization*.

Impersonation Protection (Whaling Protection)

Whaling is a type of phishing fraud that targets high-profile end users such as C-level corporate executives, politicians and celebrities.

You can configure this feature by assigning one or more email addresses that belong to an User. In this way, through a series of controls, if an attacker tries to impersonate a CEO or a manager, Esva blocks the mail as “Whaling Fraud.”

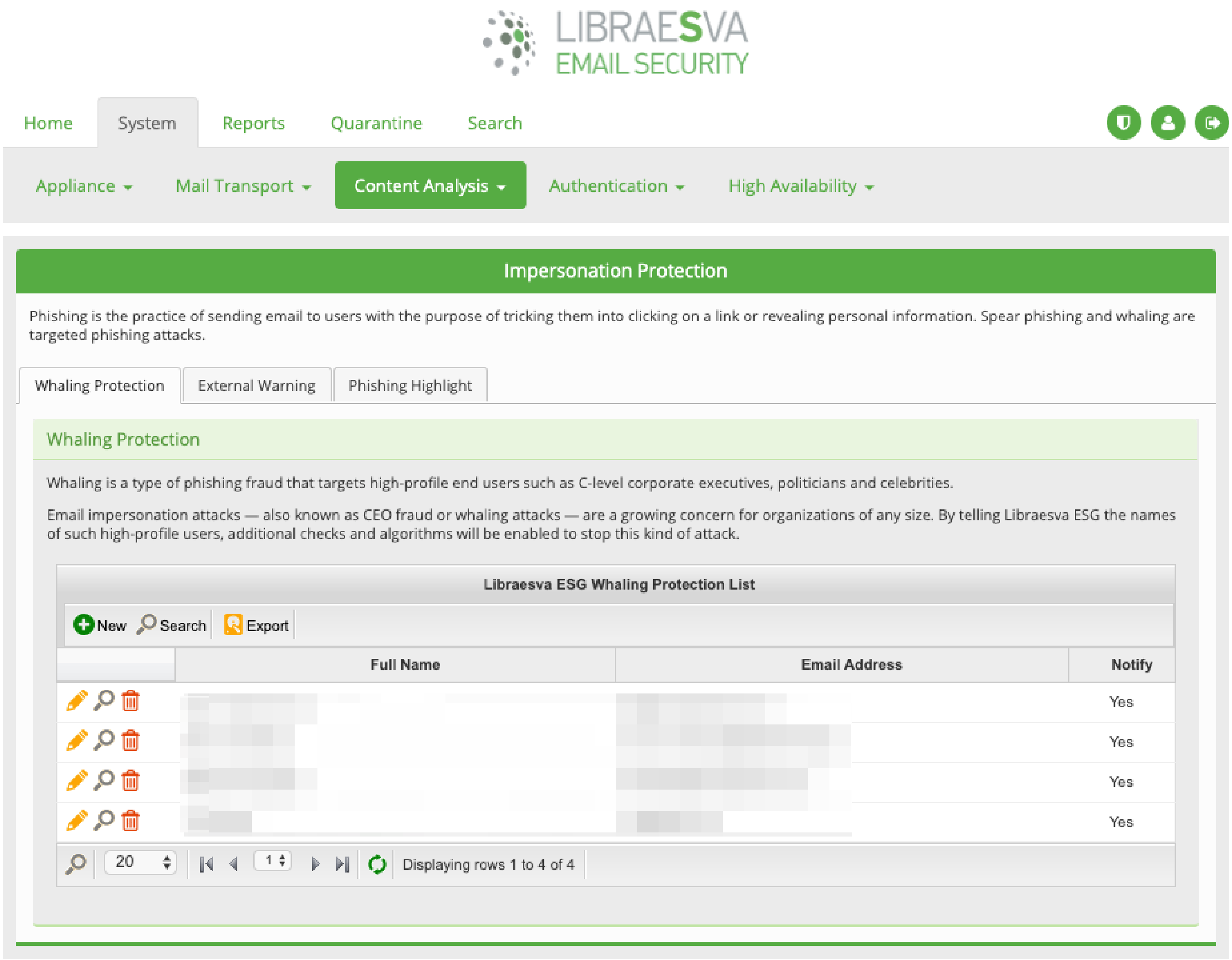
You can also configure an email notification to the recipient target of the Whaling attempt.

The impersonation protection engine analyzes email directed to the domains of the C-level persons configured in this table. The domains are derived form the entered email addresses and from the domains of all the email aliases of these users (if available).

This is important especially in an ISP/MSP setup: each “whale” entered in this table is such only in regard to its domain(s).

Example:
entering *first.last@domain1.com* causes the engine to analyze email directed to domain1.com for impersonation attempts of this person. If this email address has some email aliases on other domains also email directed to those domains is analyzed.

If you wan to domain2.com to be also protected by impersonation attempts on this person, just enter a new entry with the same name and an email address like this: *first.last@domain2.com*. Now also email directed to domain2.com will be checked for impersonation attempts on this person. It does not matter if this last email address does not actually exist.



Impersonation Protection

Phishing is the practice of sending email to users with the purpose of tricking them into clicking on a link or revealing personal information. Spear phishing and whaling are targeted phishing attacks.

Whaling Protection

Whaling is a type of phishing fraud that targets high-profile end users such as C-level corporate executives, politicians and celebrities.

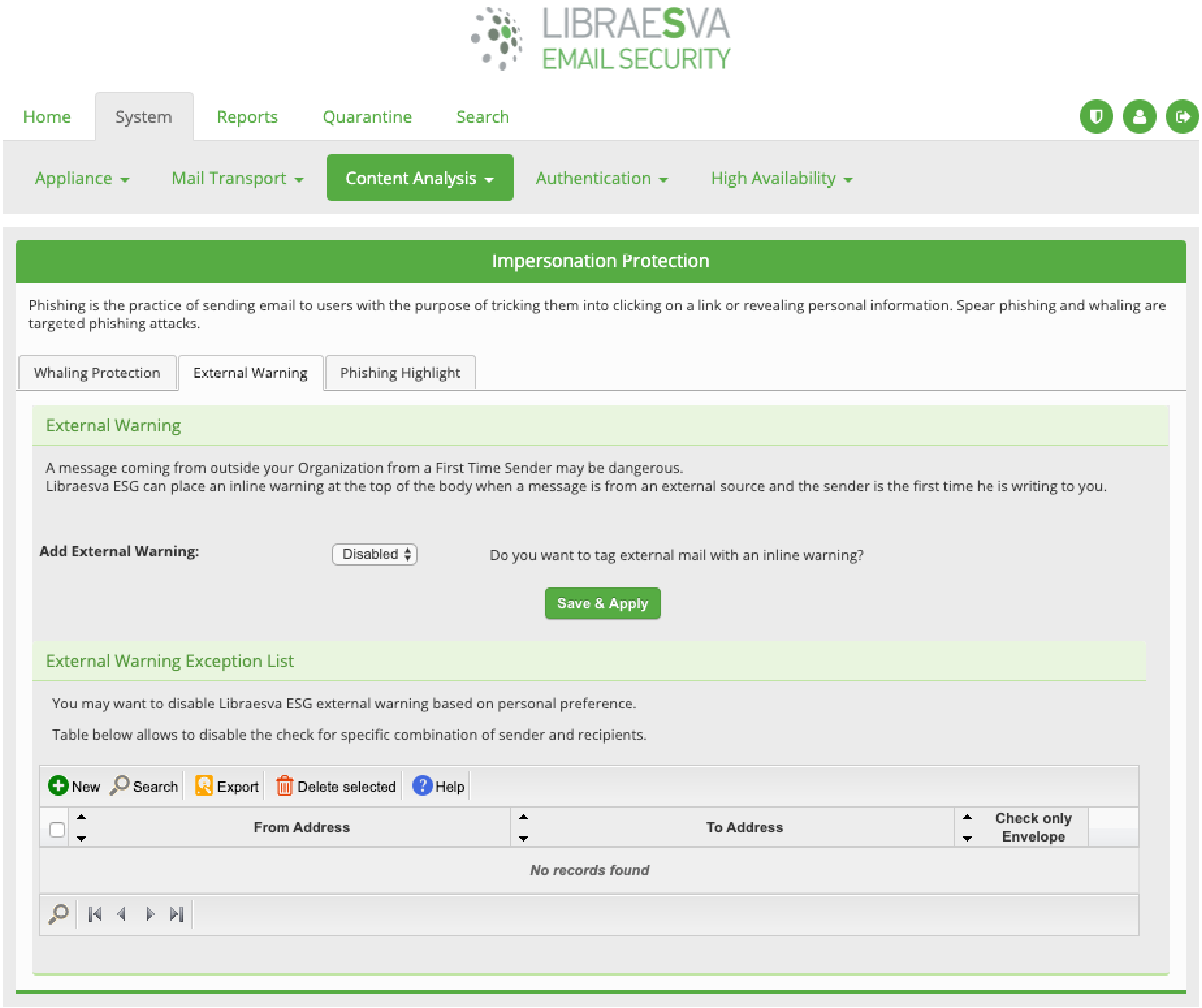
Email impersonation attacks — also known as CEO fraud or whaling attacks — are a growing concern for organizations of any size. By telling Libraesva ESG the names of such high-profile users, additional checks and algorithms will be enabled to stop this kind of attack.

Libraesva ESG Whaling Protection List

Full Name	Email Address	Notify
[redacted]	[redacted]	Yes
[redacted]	[redacted]	Yes
[redacted]	[redacted]	Yes
[redacted]	[redacted]	Yes

Displaying rows 1 to 4 of 4

External Warning



Impersonation Protection

Phishing is the practice of sending email to users with the purpose of tricking them into clicking on a link or revealing personal information. Spear phishing and whaling are targeted phishing attacks.

External Warning

A message coming from outside your Organization from a First Time Sender may be dangerous.
Libraesva ESG can place an inline warning at the top of the body when a message is from an external source and the sender is the first time he is writing to you.

Add External Warning: Disabled — Do you want to tag external mail with an inline warning?

External Warning Exception List

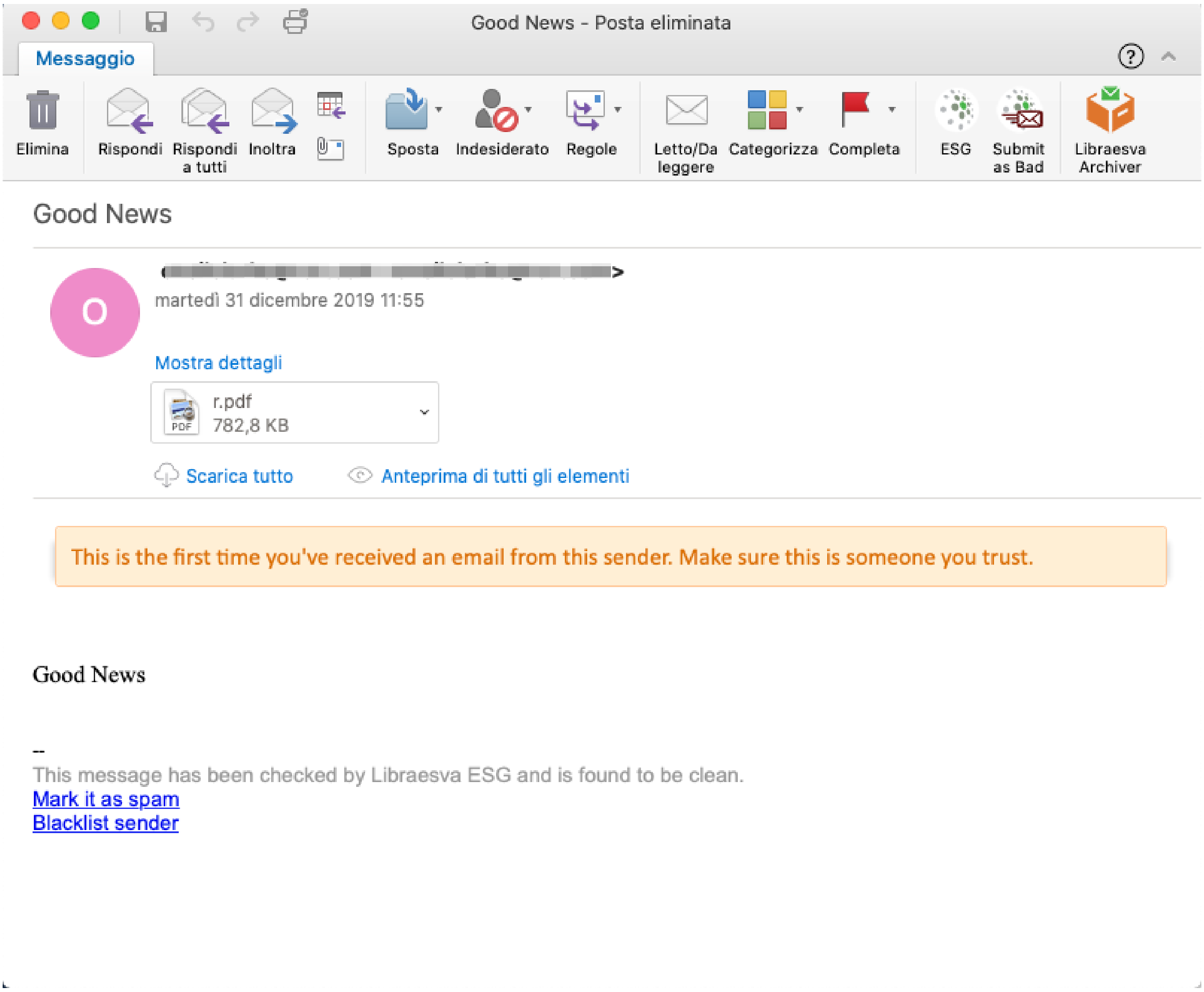
You may want to disable Libraesva ESG external warning based on personal preference.

Table below allows to disable the check for specific combination of sender and recipients.

□	From Address	To Address	Check only Envelope
		No records found	

A message coming from outside your Organization from a First Time Sender may be dangerous.
Libraesva ESG can place an inline warning at the top of the body when a message is from an external source and the sender is the first time he is writing to you.

Following an example of warning:



Good News

O [redacted]>
martedì 31 dicembre 2019 11:55

r.pdf
782,8 KB

This is the first time you've received an email from this sender. Make sure this is someone you trust.

Good News

--
This message has been checked by Libraesva ESG and is found to be clean.
Mark it as spam
Blacklist sender

Like other scanning options, you can add exceptions to its highlighting.