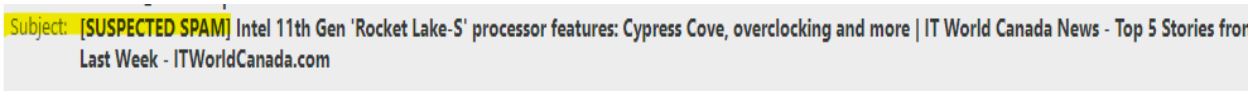
Cisco Email Security - What's New?

The Cisco Email Security Appliance (ESA) uses a variety of mechanisms to filter spam and fight malicious attacks. The goal of the solution is to filter out positively identified spam, and quarantine or discard email sent from untrusted or potentially hostile locations. Antivirus scanning is applied to emails and attachments from all servers to remove known malware. It also performs checks on the sender based on their reputation and to verify they are legitimate senders. With the increased filtering, more messages may be identified as SPAM.

With the new software, there are some new features end users need to be aware of.

How Spam Mail is Handled

If an email is flagged as suspected SPAM it delivers the message to the mailbox, and prepends the subject line with **[Suspected SPAM]** as shown below:



If the email is positively identified SPAM it will go to the SPAM quarantine and prepend the subject line with **[SPAM].** Items that have inappropriate content (contains profanity or suggestive content) will be flagged to the quarantine and tagged with **[FLAGGED: INAPPROPRIATE]** in the subject heading.

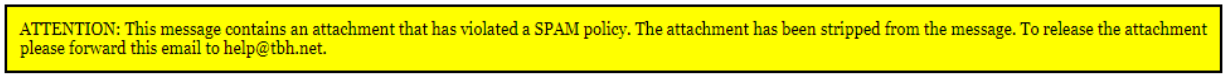
Reminder: Items are kept in SPAM Quarantine for 14 days.

Please review the document How to Access & Manage your SPAM Quarantine found on the iNtranet to administer your quarantine.

Any messages containing virus or malware messages will be dropped from the system and will not be delivered.

Attachments

Emails with attachments that violate the content policies will be sent to your quarantine. User can release the messages, however the attachment will be stripped from the message upon delivery to the mailbox with the following disclaimer:



To have these attachments released, contact the Help Desk.

External email Disclaimer

As with our previous version, a disclaimer will appear on all external emails coming into the TBH email system. The addition of this disclaimer is part of our ongoing cybersecurity initiative in an effort to combat spam and phishing emails.

This disclaimer message is a subtle reminder to always **use caution when opening emails from unknown or external senders.** Be wary of any e-mails that appear to come from our organization but have this disclaimer attached, or external messages asking to change your password or login to a website. Report those messages as Spam or Phishing.

> CAUTION: This email originated from outside the organization. Do not click links or open attachments unless you validate the sender and know the content is safe. Please forward this email to help@tbh.net if you believe this email is suspicious.

Graymail

Graymail messages are messages that do not fit the definition of spam, for example, newsletters, mailing list subscriptions, social media notifications, and so on. These messages were of use at some point in time, but have subsequently diminished in value to the point where the end user no longer wants to receive them.

The difference between graymail and spam is that the end user intentionally provided an email address at some point (for example, the end user subscribed to a newsletter on an e-commerce website or provided contact details to an organization during a conference) as opposed to spam, messages that the end user did not sign up for.

Cisco ESA provides an integrated graymail scanning engine and a cloud-based Unsubscribe Service.

The graymail management solution allows the organization to:

- Identify graymail using the integrated graymail engine and apply appropriate policy controls.
- Provide an easy mechanism for end users to unsubscribe from unwanted messages using Unsubscribe Service.

How does Graymail Work?

When an email comes into the system:

1. The email security appliance checks if the message is spam, virus or malware positive.
2. If it passes the check (negative), it next checks if the email is graymail.
3. If it flagged as graymail, it will add a banner with unsubscribe button to the message. Also, the Email Security appliance rewrites the existing unsubscribe links in the message body so any malicious links within the email are verified. The Unsubscribe banner will show in the

4

End-User Safelist

If an end users has configured a Safelist for their own email accounts, graymail messages from a sender in the safelist will **not** be scanned by the graymail scanning engine. To manage your safelist, **please review the document How to Access & Manage your SPAM Quarantine found on the iNtranet.**