Situation

With Proofpoint Essentials in use, users still receive spam messages.

Solution

• Configuration changes to spam items
• Configuration changes to spam filtering
• Review filters and approved senders
• Report as false negative

Proofpoint Essentials Spam scanning

Proofpoint Essentials is powered by Proofpoint’s MLX machine learning technology. This solution examines and filters millions of possible spam attributes in every email including message envelope headers and structure, email images, email sender reputation as well as unstructured content in the message body to prevent spam emails, attachment-based spam (including PDF and image-based spam), while automatically filtering and adapting to new spam attacks as they appear. However, there will be cases where mail, considered to be SPAM by the user, is delivered. These are often newsletters or “bulk-mail”.

However, spam email comes in many forms, and attackers do not stop changing their methodology, and will continue to send spam to try to by-pass filters. When spam email makes it past our filtering, this indicates that the message does not contain any markers in our current definition set. Please see below for the false negative reporting process.

Spam feature items to review

The spam features are located at Security Settings > Email > Spam Settings.

1. Log into the Proofpoint Essentials user interface.
2. Search for the customer in the search bar.
3. Click on Company name to open.

These are the settings to note:

• Quarantine email suspected of being phish
• Quarantine bulk email
• Spam stamp & forward
• Inbound domain spoofing protection

Quarantine email suspected of being phish

Proofpoint Essentials will mark suspected phishing messages with a phish tag. These may not score high enough for
spam and may not get quarantined in some cases. However, if this feature is enabled, it will quarantine the message tagged as *phish*. In the *Log Details*, it will indicate a *Phish* tag has been applied.

---

### Quarantine bulk email

Bulk email (newsletters in most cases) is not considered spam in the traditional sense. These messages are opt in, meaning you had at one time opted in for them. Proofpoint Essentials will mark recognizable newsletters with a *bulk* tag, which can be seen in the *Log Details*. These types of messages may not score high for spam. However, setting this feature will quarantine messages tagged as *bulk*.

---

### Spam stamp & forward

This *Spam Stamp & Forward* option tags a message as spam, but still forwards it to the mail server. By allowing this feature, this allows spam emails that are borderline spam to go through to the mail server.

**Support Recommendation**

Support recommends not using this feature. If you do, make sure the tag is known across the company to ensure they know this message is possible spam.

---

### False Negative Reports

Please note that delivered messages that users want to report as false negative may not be feasible. Support recommends turning off this feature, as most of these would likely be caught without it enabled.

---

### Inbound domain spoofing protection

This feature is very straightforward. It is for domain scanning only. All your domains you list in your *Domains* tab will be scanned as part of this feature. If an inbound message with your domain in the *SENDER* or *FROM* field is in it, this feature would quarantine the message.

**Support Recommendation**

Support recommends this feature to be turned on for all users. If a customer is using an outside service that uses your domain, you can create a custom filter to allow this particular message through.

---

### Spam filter setting to review

From the same area in the *Spam* section in the user interface, you can find the *Spam Sensitivity* slider. The default *Spam Sensitivity* is set to 7.

- The lowest the slider can be set is: 2
- The highest the slider can be set is: 22

Please note:
• The lower the sensitivity is set, we quarantine more spam email.
• The higher the sensitivity is set, we will deliver more messages that could be spam to the mail server.

**Sensitivity Settings**

Setting of 2: will block more spam email from going to the mail server

Setting of 22: will allow more spam email to mail server

---

**Review filters and approved senders**

When spam emails make it to the mail server, the first thing to check are the logs. Please ensure you are familiar with reviewing mail logs to review the details of the message.

**Permalinks**

If you are wanting help with support, please ensure you provide a permalink. Please check here to review how to get a permalink.

**Triggering Filter**

When you review the details of the message, the key item is if there is a **Filtered: Allow** entry as a **Status**. In the details, you can find what caused this by the **Triggering Filter**. This section is brief description of what the item is. Click on the actual item that triggered will open the direct filter in a new tab. It will either be an approved sender or an actual filter that allowed the message.

- **Approved Sender** - The end-user or company entered the domain or email address into the **Allow** list.
- **Filter** - The end-user or company created a rule that meets the criteria to allow the message through.

**Global versus End-user**

When the **triggering filter** is clicked, it will open the tab directly to the appropriate window. It could be for the company level or the specific end-user.

In either case, the message was not spam scored properly, as the customer or end-user has indicated to let these messages pass without scoring.

---

**Report false negatives**

From the **Log Details** if a message came through as **Category Clean**, then a false negative report should be done on this, i.e. reporting as spam. Our current definition set does not have anything in place that matches anything in the message and it will score high enough and it will pass through our filtering.

Please follow our standard [false negative reporting process](#) when opening a ticket. This is an effective method that helps you to help Proofpoint update spam definitions accordingly so we can block these or a similar iterations of these threats.