Email Protection
Proofpoint End-User Quarantine for TitleWorkPlace
April 2017
Overview

The Proofpoint Messaging Security Gateway enforces anti-spam, anti-virus, and content policies for our TitleWorkPlace email accounts. All incoming email is inspected by the cloud hosted Proofpoint Secure Messaging Gateway before it enters our organization.

For messages determined to be safe but classified as spam, Proofpoint delivers to your personal Spam Quarantine. The quarantine web application can be accessed here: https://001a8d02.pphosted.com:10020.

You will receive an email message referred to as an “End User Digest” each morning at 7:00 CT when you have received new spam within the previous 24 hours. This message will include a list of all newly received spam and includes links to perform similar functions as the web application directly from the email message. By Default, the End User Digest will not be delivered if you have not received any new spam within the last 24 hours.

Releasing Messages from Quarantine – Web Application

The following illustration provides an example of the End User Web Application. There are two ways to launch the Web Application:

- Enter the URL provided above to open in a web browser.
  - Use your TitleWorkPlace username and password.
  - Note: Users who access TitleWorkPlace via Agency Secure must use method #2 below instead.

- Click the Manage My Account link in the email digest (shown on the next page).
  - You are automatically signed in.

When opened, the console defaults to the Quarantine tab in the left pane and presents you with a view of all your spam messages that were blocked. Selecting Lists allows you to add senders to your personal Safe Senders and Blocked Senders lists. Note that adding addresses to the Safe Senders list will only override spam filters, messages from these senders will still be blocked if they contain viruses and other malicious content.

Selecting Profile allows you to change the following user preferences:

- **Send Digest** – you can opt to receive digest messages every morning even when empty if you choose.
- **Preferred Language** – language can be changed to desired preference.
- **Spam Detection** – allows you to select between varying degrees of spam control with these settings.
  - Relaxed filter
  - Moderate filter
  - Aggressive filter
Message commands are available along the top of the console window. They are:

- **Find** – allows you to locate specific content within the quarantine.
- **Release** – releases the messages you have selected to your mailbox using the appropriate checkbox.
- **Not Spam** – reports to Proofpoint that the blocked message is legitimate, known as a ‘false-positive’ so that future filtering logic is improved.
- **Allow Sender** – adds the senders of selected messages to your Safe Senders list. Note: When you add a domain name (e.g., yahoo.com) to the Safe Senders list, all email addresses from that domain will be considered ‘safe’. You should restrict the safe list to specific senders by entering their full email addresses (ex. john.doe@yahoo.com).
- **Options** – provides additional functions including:
  - **Request Digest** – emails you an up-to-date digest message.
  - **Refresh** – displays any newly received spam that arrived after you logged in to the web application.
  - **Delete All** – clears all messages from your spam quarantine.

### Releasing Messages from Quarantine – End User Digest

The below illustration is an example of the End User Digest message.

Like the Web Application, the email Digest displays messages that have been classified as spam. These messages are still stored in your personal Quarantine; the Digest only provides a way to manage your quarantine from email.

Note, if the links in the Digest have expired, you will be prompted to log in to the Web Application to release a message. Within the digest message, you’re presented with a few options along the top row that are unique to the digest.

- Selecting **Request New End User Digest** will email you a new digest, to include any newly quarantined mail since delivery of the last digest.
- Selecting **Request Safe/Blocked Senders** will email you a list of addresses you currently have included on your Safe and Blocked Senders lists.
- Selecting **Manage My Account** will simply open the web application should you need update your Blocked Senders lists or your preferences.
Message commands are available as links next to each message. From the digest, you will select the desired link next to the appropriate message. You will not select check boxes for messages to process like with the web application. These links are as follows:

- Selecting **Release** will cause the message to be delivered to your mailbox.
- Selecting **Release and Allow Sender** will also deliver the message, but will also add the sender to your Safe Senders list.
- Selecting **Not Spam** will report the message as a false-positive to Proofpoint so that future messages with these characteristics will not be scored as spam.