Introduction

The purpose of this memo is to explain how the email that originates from outside this organization is processed, and to describe the tools that you can use to manage your personal spam quarantine. This memo does not apply to internal email messages.

To protect this organization from virus attacks and to protect you from receiving hundreds of spam messages, all incoming email is filtered by the Proofpoint Messaging Security Gateway – an anti-spam and anti-virus product. Proofpoint MLX™ is an advanced machine learning filtering technique used to ensure that no valid mail is improperly filtered. For more information about the Proofpoint Messaging Security Gateway and MLX, you can visit Proofpoint's web site at *www.proofpoint.com*.

We can also use the Proofpoint Protection Server to filter outgoing mail to deter the distribution of trade secrets or intellectual property or to filter for specific words that may indicate inappropriate content, including pornography or obscene and racist words.

How does email filtering work?

All incoming (and outgoing) email is filtered by the Proofpoint Protection Server. Depending upon Proofpoint Protection Server rules and policies, messages that contain a virus, or spam, or inappropriate content can either be deleted or "scored." In the case of spam, the message score indicates the probability that the message is spam – so a message scoring 100 would have 100% chance of being spam (definite spam) and a message scoring 0 would have 0% chance of being spam (legitimate correspondence). Messages scoring high enough to probably be spam are quarantined, and messages scoring below 50 are sent directly to your inbox.

What is the Quarantine?

The *Quarantine* is a location on a server where email messages that are suspected to be spam are stored temporarily so that they can be reviewed and retrieved if necessary. System administrators have the ability to search for messages on a user's behalf. You may also review and take action on your own quarantined email through the use of the End User Digest. Messages that are not

released from the Quarantine are automatically deleted after a designated period of time.

What is an End User Digest?

If email messages addressed to you were sent to the Quarantine, you will receive an email notification, called an *End User Digest* (or Digest), in your mailbox. The Digest provides you with a list of the messages addressed to you that are stored in the Quarantine. You can look at the message subject headers to determine their content and decide what actions you want to apply to the messages.

You may also receive an empty Digest, which is simply an email message indicating that you have no messages in the Quarantine. You may want to receive a Digest even if it doesn't contain any messages, so you can continue to manage certain aspects of your email. The system administrator decides whether or not users should receive an empty Digest.

What is the Welcome Message?

The Welcome Message is an email message that informs you that an account has been created for you. It includes a temporary password and a **Manage My Account** link. Click the link to launch a browser, and use your temporary password to access your Proofpoint account. (See the section *What is the Web Application?*) You will be asked to change your temporary password the next time you log in to your account.

How do I use the Digest?

The Digest will provide you with a list of all of the spam that has been quarantined for your account since you received the last Digest update. You will see a list of messages and columns that indicate the subject, sender, and time received for each email.

> **Note:** Your administrator controls how long the links in the Digest will work until they expire. For example, if you click a link in the email Digest to release a message from the Quarantine, and the link has expired, you will be prompted to log in to the Web Application to release the message. (See the section *What is the Web Application?*)

You will have three separate links available to you to complete an action on each email message:

- Release – releases the message from the Quarantine to your normal email inbox.

- Safelist – releases the message from the Quarantine to your inbox and adds the sender to your personal Safe Senders list. All future email from this sender will not be checked for spam.
- Report – reports that the message was a false positive (that is, it should not have been classified as spam). In this case, further training is done to ensure that similar messages are not caught as spam in the future.

Other links in the Digest provide additional functionality. These links are not related to individual quarantined messages. The following links provide additional Digest management:

- Request New End User Digest – immediately generates a new Digest with up-to-the-minute information about quarantined messages. *Note: this Digest will contain a list of all messages currently in the Quarantine, not just those received since the last scheduled Digest update.*
- Request Safe/Blocked Senders list – sends you a list of all entries currently on your personal Safe and Blocked Senders List.
- Manage My Account – allows you to change account preferences, as well as actively manage your Safe Senders and Blocked Senders lists using a web interface.

What other features are available to manage my account?

The Manage My Account link gives access to a separate web interface that will allow you to manage your Safe Senders and Blocked Senders lists, change the preferred language interface for your Digest, and adjust Digest preferences.

To access these features, click the Manage My Account link in the Digest. A separate browser window pops up on your screen and your personalized account management page will load in this window. You do not need to authenticate to your account management page because a secure code is generated in your personalized Digest that ensures that only you have access to change your settings.

You have the following options to choose from in your account management page. Click the name of the option in the left navigation pane:

- Profile – controls Digest settings and language preferences.
- Lists – provides tools to manage personal Safe Senders and Blocked Senders lists.

Profile option to manage my account

The Profile option displays a My Settings view and the Save, Request Digest, and Refresh links.

Links:

- Save – saves your settings each time you make any changes.
- Request Digest – sends you an updated Digest.
- Refresh – refreshes the view.

My Settings:

- Send digest with new messages – this is the default setting. You will only receive a Digest when you have new messages in the Quarantine.
- Send digest even when I have no new messages – this choice will send you a Digest whether or not you have new messages in the Quarantine. If there are no new messages, you will receive an empty Digest.
- Preferred Language – you can select a language from the drop-down list. This is the language that displays in your Digest and in your Manage My Account browser window.
- What type of spam detection do you want? – you can select a spam policy from the listed choices. The policies determine how you want your email filtered for spam.

Lists option to manage my account

The Lists option displays the Safe Senders List and Blocked Senders List views where you can manage your personal lists of safe senders and blocked senders. The spam detection technology provided by Proofpoint's adaptive machine-learning engine is highly accurate and you are not required to add entries to your Safe Senders or Blocked Senders lists. This feature is available to you if want to create your own personal lists.

Click Safe Senders List or Blocked Senders List in the left navigation pane to choose the list you want to manage.

Links:

- New – provides a text field so you can add an email address or domain to your list.
- Edit – lets you make changes to an address already on your list. You need to first select (click the check box) for the address you want to change.
- Delete – deletes the selected address from the list.

- Select All – selects all of the addresses on the list.
- Unselect All – un-selects all of the selected addresses on the list.
- Request Digest – sends you an updated Digest.
- Refresh – refreshes the view.

Safe Senders List:

> Email sent from addresses or domains on the Safe Senders List will not be filtered for spam, but will be filtered for viruses.

Blocked Senders List:

> Email sent from addresses or domains on the Blocked Senders List will automatically be discarded so that you will not receive future emails from them. *Note: if a spam message does make it through to your inbox, you should not add that email address to your Blocked Senders List since spammers rarely use the same email address twice.*

Why do I get a warning message when I click on links in the Digest?

It is normal to see an "Invalid Certificate" warning when clicking on the links in the Digest. You can safely accept the certificate warning and continue.

If the Digest links have expired, you will be prompted to log in to the Web Application to manage messages in the Quarantine.

How do I delete my messages in the Quarantine?

There is no need to delete your messages in the Quarantine.

If you do not release a message from the Quarantine, it will automatically be deleted after four weeks. If you look at the messages in your Digest and determine that all of them are spam, you do not need to do anything. The messages will automatically be deleted from the Quarantine.

What is a Safe Senders and Blocked Senders list?

There are two types of Safe Senders lists: the *Organization Safe Senders List* and your personal *Safe Senders List.* Both are simply lists of legitimate senders of email. The email administrator controls the Organization Safe Senders List, which applies to everyone in the organization. You control your personal *Safe Senders List* to which you can add the addresses of people, organizations, and mailing lists from which you *do* want to receive mail.

If a sender's address is included in the Safe Senders List, the Proofpoint Protection Server does not filter the message for spam. (However, it still filters the message for a virus or inappropriate content.)

There is also an *Organization Blocked Senders List* and a personal *Blocked Senders List*. These lists contain addresses of people, organizations, and mailing lists from which you do *not* want to receive “junk email.”

What is a false positive?

A *false positive* is an email incorrectly identified as spam. If an email message is scored as spam and sent to the Quarantine, but it really is a legitimate message from a legitimate sender, you can report it as a false positive (Not Spam).

In the future, messages that have the same characteristics as the message you reported will not be placed in the Quarantine for containing spam.

What is a false negative?

A *false negative* is an email incorrectly identified as *not* spam. An email message that is incorrectly delivered to your mail box because it was not identified as spam can be reported as a false negative.

Spammers are very clever and are always seeking ways to trick products like the Proofpoint Protection Server into delivering spam to your mailbox. Proofpoint sends frequent updates to our organization in an attempt to stay one step ahead of the spammers.

What is a spam policy?

Spam policies determine how the spam sent to you will be processed. For example, your spam could be deleted or quarantined. You can only select your own spam policy if you are allowed to Manage My Account.

What is the Audit Messages section that appears in the Digest?

The *Audit Messages* section that appears in your Digest indicates that you are a member of any group designated to audit messages. The messages listed under the Audit Messages section are all the messages that have been delivered to your mail box. If you determine that some of the messages that were delivered are actually spam (false negatives) you can report these messages to Proofpoint by clicking the "Report Spam" link next to the message.

Members of the Spam Reporting Group help improve the spam identification process by reporting false negatives to Proofpoint for further analysis.

What is the Web Application?

The Web Application allows you to view your quarantined messages and manage your account using a web browser. Instead of waiting for a Digest in your inbox, you can log in any time to your account and release messages from the Quarantine, manage your profile settings, or manage your Safe Senders and Blocked Senders list.

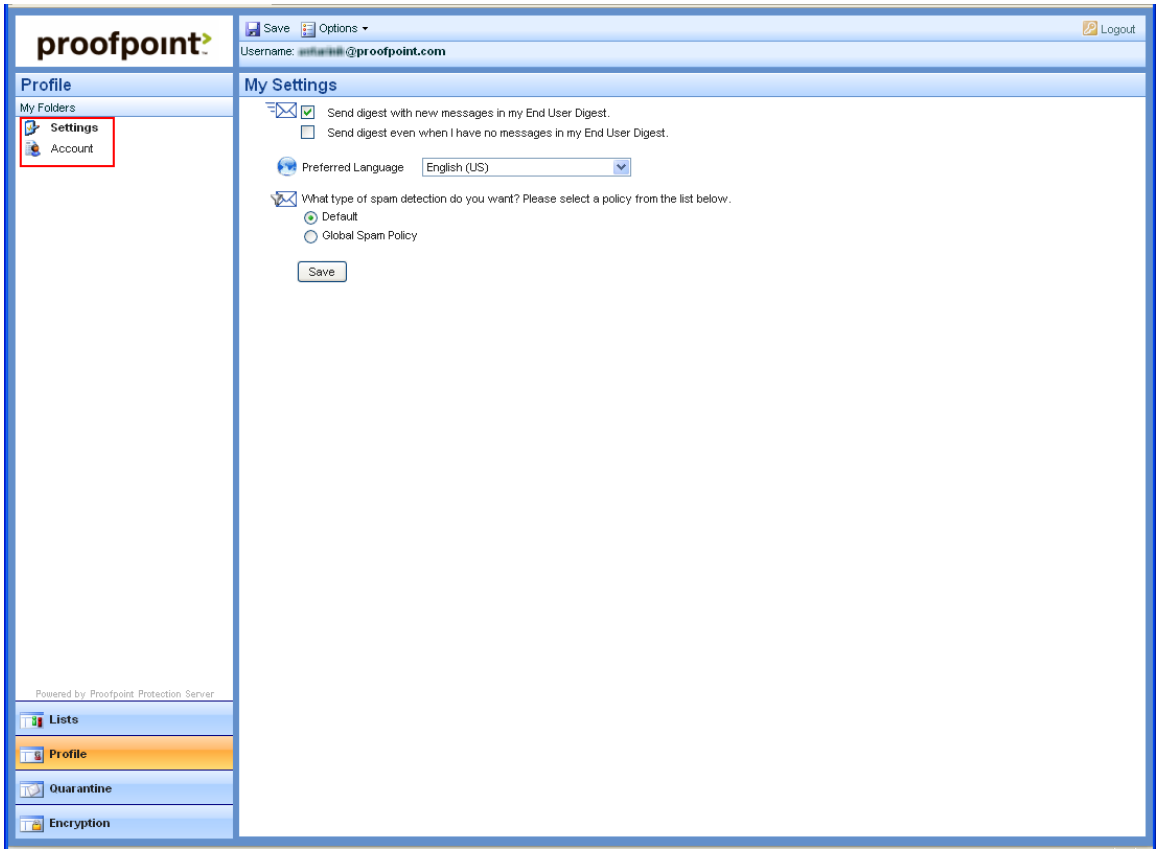
At SMC we included Proofpoint in our Okta website. You can access your Proofpoint web application by adding the Proofpoint application to your Okta Applications:

No password is required to log you in!

If you see messages about certificates pop up, just click OK to continue.

Your view to the Web Application

The first view you see is My Profile, where you can change My Settings and manage your Account. On the My Settings page, you can make choices for your preferred language, whether or not you want to receive an empty Digest, and which spam policy you want applied to your email messages.

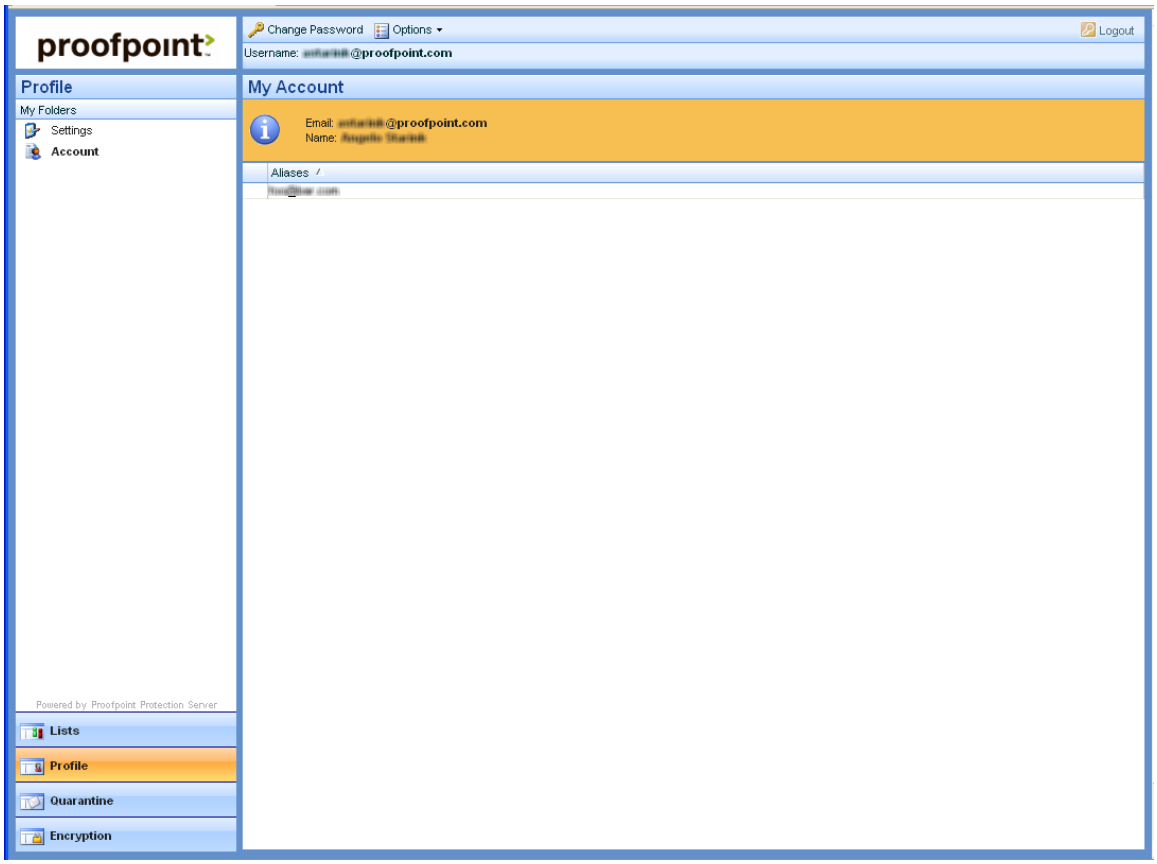


The left side displays links for each of the tasks you can complete in the browser:

- Profile – You can change your preferences on the Settings page and view your email aliases on the Account page.
- Lists – Safe Senders and Blocked Senders lists.
- Quarantine – contains a list of your messages in the Quarantine.

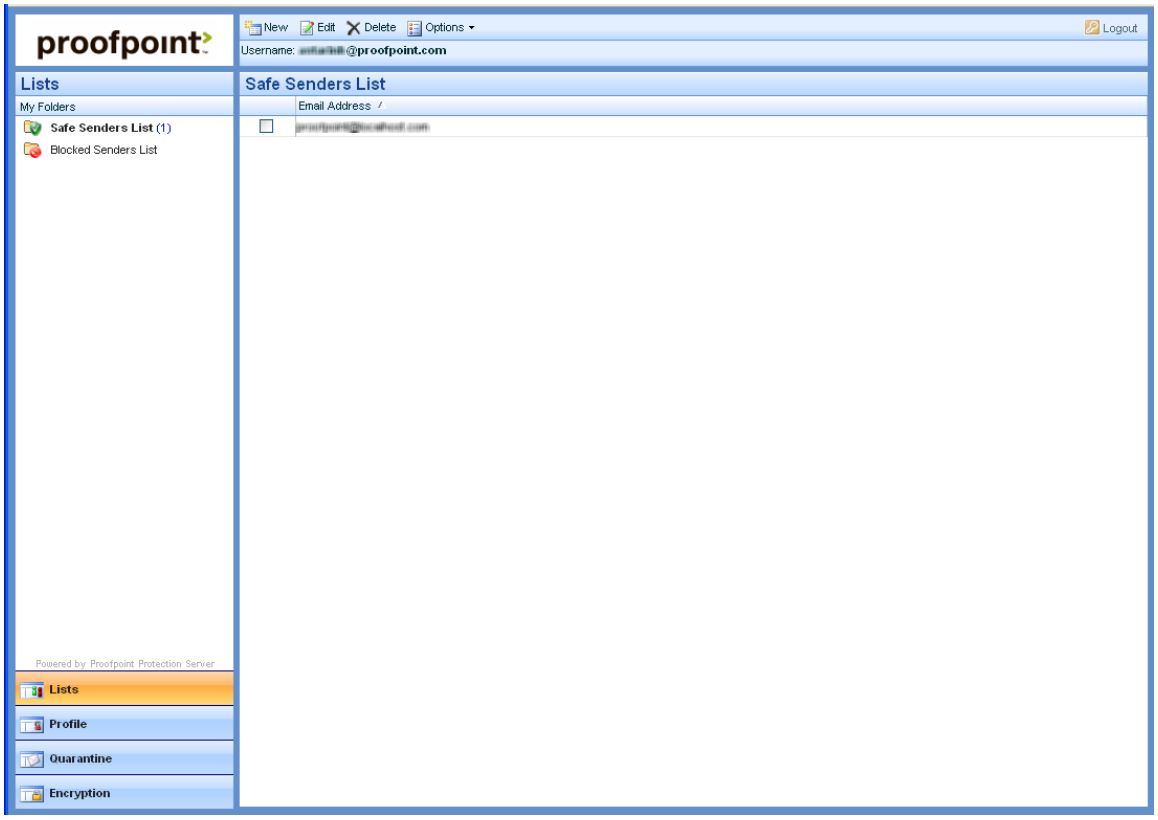
Account

Click Account under Profile on the left side to view your email aliases. You cannot make any changes to this page.



Lists

Click Lists on the left side to view your Safe Senders and Blocked Senders lists.



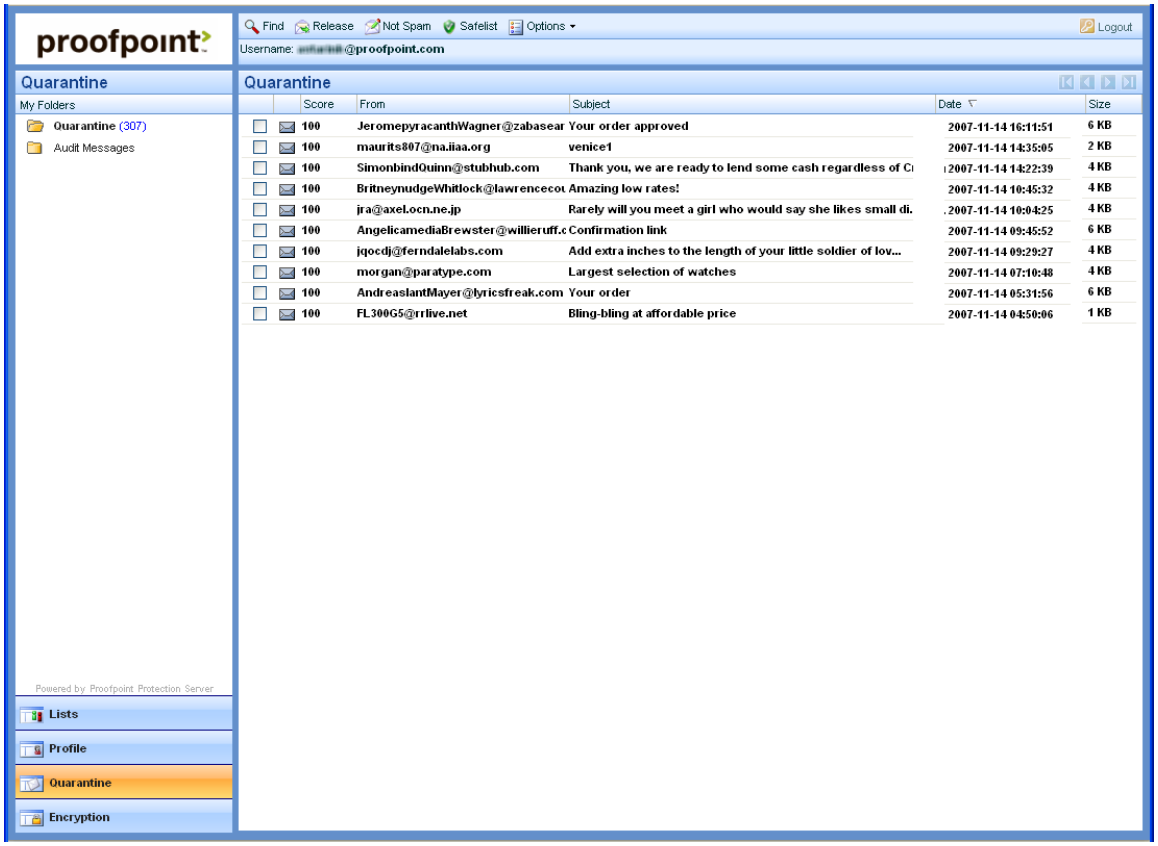
To add a Safe Sender to your list:

1. Click Safe Senders List on the left side.
2. Click New on the top of the page.
3. Enter an email address into the field.
4. Click Save.

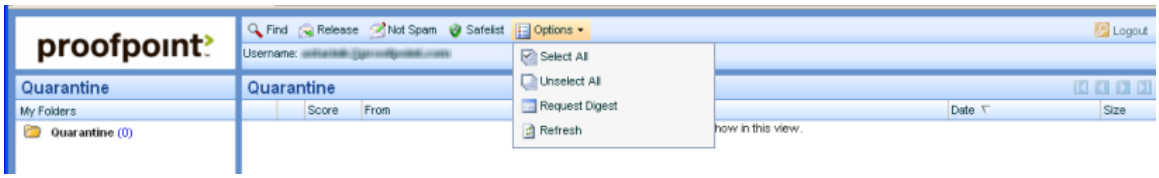
Follow the same procedure to add entries to your Blocked Senders list.

Quarantine

Click Quarantine on the left side to view your messages in the Quarantine. This page displays messages addressed to you that were classified as spam and are sitting in the Quarantine.



You can apply several actions to the messages on this page. To select one or more messages, select the check box next to the message before you apply the action.



- Logout – logs you out of your Proofpoint profile and closes your session.
- Select All – selects all of the messages so that you can apply the action to all of the displayed messages. (For example, you may have 100

messages in the Quarantine, but only 20 are displayed. The action applies to the displayed messages.)
- Unselect All – unselects all of the selected messages.
- Request Digest – sends an updated Digest to your email inbox.
- Find – displays the fields to search for a specific message using search criteria such as who sent the message, the subject line, or the age of the message.

- Refresh – refreshes the view on the page. For example, if any new messages have been added to the Quarantine while you had the browser open, they will be added to the list.
- Delete – deletes the selected messages from the Quarantine.
- Safelist – adds the sender of the selected message to your Safe Senders list.
- Not Spam – reports the message as a false-positive, and in the future, messages like this one will not be classified as spam.
- Release – releases the message to your inbox.

Audit

Not everyone will have messages in the Audit view. Your system administrator decides who will be auditing messages. Auditing messages sends information back to your system administrators so that they can improve the email filtering process for your organization.

Two additional actions are available in the Audit view:

- Report Spam – this is a message that was not classified as spam, but it is indeed spam. It is a false negative. Future messages with these characteristics will be classified as spam.
- Report Phish – this is a message that was sent by someone trying to (illegally) collect information about you. Typically, email messages like this one ask for credit card information or bank account information.

How do I reset my password?

At SMC your Proofpoint user account is linked through Okta so no password is needed!!! This does mean you have to sign into Okta or authenticate through it to get into Proofpoint.