proofpoint.

Security Awareness PhishAlarm Configuration

Admin Action Required

Microsoft is transitioning away from legacy Exchange tokens, which will impact the functionality of the PhishAlarm Add-in. Administrators must accept new permissions to ensure continued access and functionality. See PhishAlarm Add-in Permissions for more information

Posted Dec 5 2024

PhishAlarm Configuration

PhishAlarm® is an Add-in for Microsoft Exchange that allows users to easily report suspicious email without being encumbered to remember an ever-changing abuse box address or the correct format (headers and email bodies) to forward suspicious emails. PhishAlarm displays a button in the supported email client which, when clicked, will forward the email to defined email addresses. Typically, these email addresses are either an abuse box or members of your organization's incident response and security team.

PhishAlarm Add-in is provided as a manifest URL for Microsoft Exchange. It can be configured and customized to meet the needs and branding of your company. You can decide how you want the PhishAlarm button to look and act, which notification messages display to the user based on the type of email reported, what you want the messages to say, and what you want done with the email after it's reported.

Depending on how you configure PhishAlarm, the suspected email can be deleted or moved to a junk folder. It can also be forwarded to a pre-defined list of email addresses for further analysis. PhishAlarm can be configured to recognize and route different categories of emails to the appropriate team or individual. For example, the system can recognize emails sent from Proofpoint's Security Education Platform and route them to the appropriate individuals within the organization. Similarly, if any simulated mock-phishing emails are reported, they can be forwarded to the Security Awareness team, whereas other reported emails are sent to the Threat Response team.

Here are four categories of emails that you will be able to configure in PhishAlarm:

Simulated Phish	Emails sent from a Phishing Simulation campaign.
Potential Phish	Emails that are not any of the other categories (Simulated phish, Safelist email, or Proofpo
Safelist	Emails that are designated as safe and adhere to a set of rules configured on the Safelist t

Proofpoint Training	Email notifications sent from the Proofpoint Platform including Training Assignment and Re

Microsoft Exchange Supported and Features Supported Per Client

Below are details about how PhishAlarm integrates with Microsoft Exchange as well as a list of features.

Email Client	**PhishAlarm for Exchange** *Add-in deployed via XM*
Outlook 2010 for Windows	—
Outlook 2013 for Windows	Y
Outlook 2016 for Windows	Y
Outlook 2019 for Windows	Y
Outlook 2016 and 2019 for Mac (Exchange 2013, 2016, and 2019; Office 365)	Y
Outlook on the Web: • Outlook Web App (Office 365) • Outlook Web Access (Exchange 2013, 2016, and 2019) • Outlook.com	Y
Outlook for iOS and Android[2]	Y

[1] *PhishAlarm for Exchange must adhere to browser requirements depending on the version of Outlook and operating system in use. Please refer to this Microsoft Docs article for more information:* [Browsers used by Office Web add-ins.]()

[2] *Supported only in Office 365. Mobile add-ins are not supported on the U.S. Government Community Cloud (GCC) or onpremise Microsoft Exchange Servers.*

Features Support Per Email Client

The following feature matrix notes the capabilities supported when PhishAlarm is installed within specific email clients.

● = Supported by Exchange ○ = Not Supported by Exchange

Feature	PhishAlarm For Exchange
Forward to specified email recipients	●
Delete email after report	●
Move email to Junk folder after report	●
Capture header	●
Capture body	●
Capture attachments	●
Prompt Message	●
Language support for notifications	●
Automatic software updates[1]	●
Safelist Emails	●
Custom Icon and Text	●
Report from Shared Inbox	○
Report Messages from Multiple Accounts	○

Deployed Centrally	●
Preserve Original Header and Body	Attached/Inline

1 Updates to business logic are automatic, but an update of the XML manifest is still required for PhishAlarm For Exchange.

CONFIGURING PHISHALARM

Before the PhishAlarm add-in can be used, you must configure four areas:

- **Appearance** – The look of the PhishAlarm button as it appears in the email client. Refer to Configuring the PhishAlarm Add-in Button for Exchange for more information.

- **End-user notifications and email handling** – The notification, or feedback, message the end user sees after reporting a phish and what you want PhishAlarm to do with the email within the email client after it’s reported. Refer to Configuring End-user Communication for more information.

- **Email forwarding** – The forwarding options for each type of reported email, such as forwarding to a security operation center (SOC). Refer to Configuring Reported Email Forwarding Options for more information.

- **Safelisted emails** – The email addresses designated as safe by your organization. Refer to Configuring Safelist Emails for more information.

Configuring the PhishAlarm Add-in Button for Exchange

PhishAlarm can be configured for your organization’s environment and the email client version of Microsoft Exchange that you’re using. You can choose from multiple button layouts and customize various button label text and languages to create a look and feel that supports your corporate brand and your global employee base.

Note: For the PhishAlarm add-in button to work for a user, the individual’s email address **must** be uploaded to the Security Education Platform through the User Management option. Only licensed users can report emails using the PhishAlarm button.

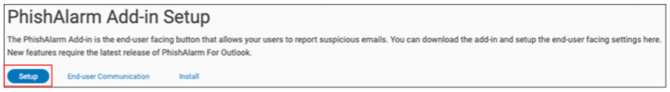
Setup

Use the steps below to configure how the PhishAlarm button will appear to your end users.

1. Sign into the Security Education Platform.

2. Click **PhishAlarm > Add-in Setup**.

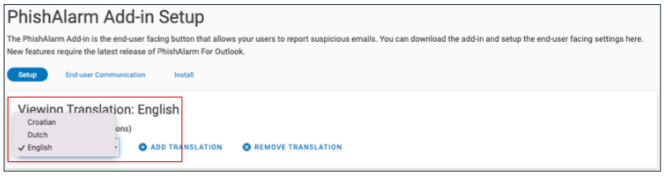
3. Click the **Setup** tab.



PhishAlarm Add-in Setup

The PhishAlarm Add-in is the end-user facing button that allows your users to report suspicious emails. You can download the add-in and setup the end-user facing settings here.
New features require the latest release of PhishAlarm For Outlook.

4. In the **Viewing Translation** section, select the language from the **Translation set** list for the PhishAlarm add-in button that is going to be configured. You can customize the information in multiple languages to address the localization needs of your end users by repeating these steps below for each language needed.



PhishAlarm Add-in Setup

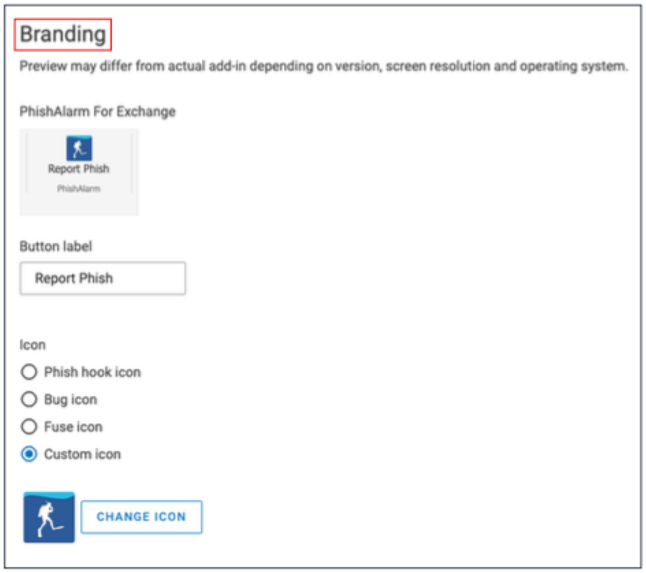
The PhishAlarm Add-in is the end-user facing button that allows your users to report suspicious emails. You can download the add-in and setup the end-user facing settings here.
New features require the latest release of PhishAlarm For Outlook.

Viewing Translation: English

Note: If you need to add languages to the **Translation** set list, click **+ ADD TRANSLATION**, select the language from the list, and click **ADD**. If you want to remove a language from the list, click **x REMOVE TRANSLATION**, click **DELETE** next to the language(s) to be removed, and click **CLOSE**.

5. The **Branding** section applies to the add-in PhishAlarm for Exchange. In this section, you will configure the text and icon image on the PhishAlarm button itself.

Across the top of the section, you will see preview examples of how the PhishAlarm button will look. These previews automatically update when features and options are changed on the page so that you can see how the buttons will look.



Branding

Preview may differ from actual add-in depending on version, screen resolution and operating system.

PhishAlarm For Exchange

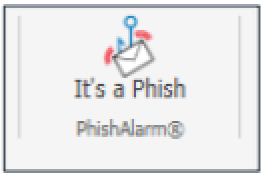
Button label: Report Phish

Icon

○ Phish hook icon
○ Bug icon
○ Fuse icon
● Custom icon

Note: Depending on the version, screen size, and operating system being used by each end user, the preview examples may differ from how they display for each user.

6. Use the **Button label** field to customize the text that is displayed on the actual PhishAlarm button. By default, this field will display the wording, **Report Phish**, in the language selected in the previous step. You can customize the text to meet your needs or keep the default text. For example, if you enter “It’s a Phish” in the field, the button will look like this:



Using PhishAlarm For Exchange, the manifest must be reloaded before the button label change is visible. Obtaining the Exchange Manifest URL Link for more information.

7. Select the **Icon** that you want to appear on the PhishAlarm button. You can choose a standard fishhook or bug icon, or you can upload a custom icon of your own, with file size limitation of 128 x 128 px.

Phish Hook Icon	This option displays a fishhook hooking a closed envelope.
Bug Icon	This option displays a bug on an open envelope.
Phish Hook Icon	This option displays a blue fishhook hooking a blue closed envelope.
Bug Icon	This option lets you upload an icon of your own. The graphic file must be a . pixels. You can drag and drop the file or click **Browse** to locate it and click **C** displays below the option for review.

8. Click **SAVE CHANGES** to keep the settings entered on the page.

9. Repeat these steps for each language that you need to configure for the PhishAlarm button.

End-user Communication Configuration

End-user communications are the feedback messages that display for users after they report an email using the PhishAlarm button. There are multiple end-user messages that may display, all of which are customizable. You can define:

- Which message displays depending on the type of email the user reported.

- How the notification message is delivered to the user, such as by pop-up message or an email.

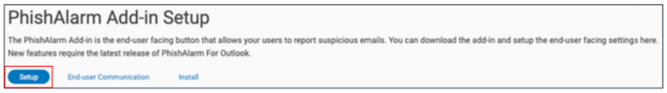
- What will happen to the email after it is reported, such as deleting it from the user’s Inbox or moving it to a junk folder.

Use the steps below to configure each type of end-user communication.

1. Sign into the Security Education Platform.

2. Click **PhishAlarm > Add-in Setup**.

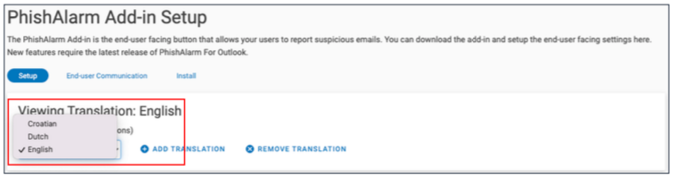
3. Click the **End-user Communication** tab.



PhishAlarm Add-in Setup

The PhishAlarm Add-in is the end-user facing button that allows your users to report suspicious emails. You can download the add-in and setup the end-user facing settings here. New features require the latest release of PhishAlarm For Outlook.

4. In the **Viewing Translation** section, select the language from the **Translation set** list for the PhishAlarm add-in button that are going to configure. You can customize the information in multiple languages to address the localization needs of your end users by repeating these steps below for each language needed.



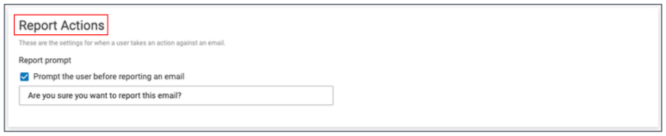
PhishAlarm Add-in Setup

The PhishAlarm Add-in is the end-user facing button that allows your users to report suspicious emails. You can download the add-in and setup the end-user facing settings here. New features require the latest release of PhishAlarm For Outlook.

Viewing Translation: English

Note: If you need to add languages to the **Translation set** list, click **+ADD TRANSLATION**, select the language from the list, and click **ADD**. If you want to remove a language from the list, click **x REMOVE TRANSLATION**, click **DELETE** next to the language(s) to be removed, and click **CLOSE**.

5. In the **Report Actions** section are settings for when a user takes an action against an email by clicking the PhishAlarm button.



Report Actions

These are the settings for when a user takes an action against an email.

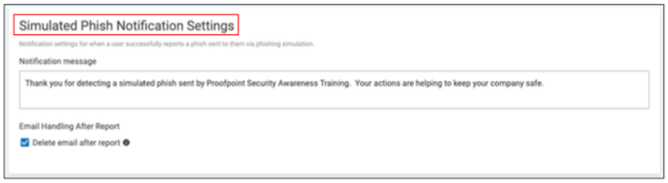
Report prompt

☑ Prompt the user before reporting an email

Are you sure you want to report this email?

Prompt the User Before Reporting an Email	• Select the checkbox to displays a "Yes or No" confirmation message to the user after th button is clicked. There's an option to customize text in the text box or keep the default "Are to report this email?" text. • A clear checkbox to not display a confirmation message at all to the end user.
Notification Type	Select how you want the confirmation message to display to the end user.

6. In the **Simulated Phish Notification Settings** section, define the message text that displays when a user *successfully* reports a simulated phish sent from a phishing simulation campaign and how to handle the email after it is reported.



Simulated Phish Notification Settings

Notification settings for when a user successfully reports a phish sent to them via phishing simulation.

Notification message

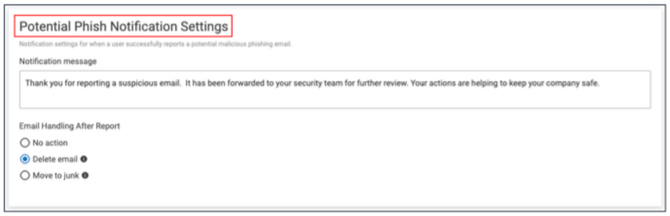
Thank you for detecting a simulated phish sent by Proofpoint Security Awareness Training. Your actions are helping to keep your company safe.

Email Handling After Report

☑ Delete email after report

Notification Message	Enter the text that will appear in the notification pop up message to the end user who *succe* simulated phish sent from a phishing simulation campaign or keep the default text displaye
Email Handling After Report	Select the **Delete email after report** checkbox if you want the reported email automatically user's Delete folder after it is reported for deleting in accordance with the company policies

7. In the **Potential Phish Notification Settings** section, define the confirmation message text that displays when a user reports a potential malicious phishing email campaign and how to handle the email after it is reported. These are emails that do not fall into any of these other categories: simulated phish, Safelist email, or Proofpoint training email.



Potential Phish Notification Settings

Notification settings for when a user successfully reports a potential malicious phishing email.

Notification message

Thank you for reporting a suspicious email. It has been forwarded to your security team for further review. Your actions are helping to keep your company safe.

Email Handling After Report

○ No action

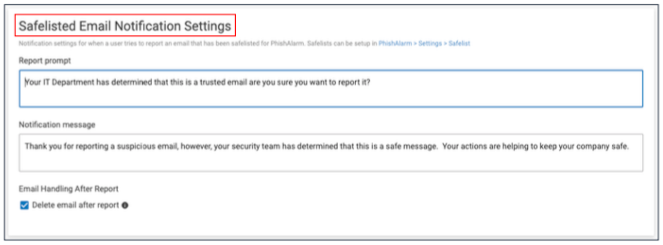
● Delete email

○ Move to junk

Notification Message	Enter the text that will appear in the notification pop up message to the end user who rep malicious phishing email or keep the default text displayed in the field.
Email Handling After Report	Select one of the following: • No action: The email will remain in the end user's Inbox. • Delete email: The email will automatically move to the end user's Delete folder after deleting in accordance with the company policies. • Move email to junk: The email will automatically move to the end user's junk folder.

8. In the **Safelisted Email Notification Settings** section, define the confirmation message text that displays when an

end user reports an email that has been safelisted in PhishAlarm and how to handle the email after it is reported. Refer to Configuring Safelist Emails for more information about configuring safelisting via the **PhishAlarm > Settings > Safelist** tab.



Safelisted Email Notification Settings

Notification settings for when a user tries to report an email that has been safelisted for PhishAlarm. Safelists can be setup in PhishAlarm > Settings > Safelist

Report prompt

Your IT Department has determined that this is a trusted email are you sure you want to report it?

Notification message

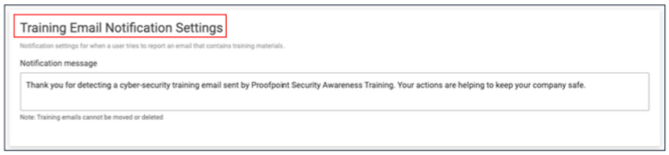
Thank you for reporting a suspicious email, however, your security team has determined that this is a safe message. Your actions are helping to keep your company safe.

Email Handling After Report

☑ Delete email after report

Report Prompt	Enter the text that will appear in the pop-up message or keep the default text displayed i message will appear when the end user attempts to report an email that is a safe messa address/domain that was safelisted by your organization.
Notification Message	Enter the text that will appear in the notification to the end user who proceeds with repor email or keep the default text.
Email Handling After Report	Select the **Delete email after report** checkbox if you want the reported email automatica end user’s Delete folder after it is reported for deleting in accordance with the company p

9. In the Training Email Notification Settings section, define the confirmation message text that displays when a user reports an email that was sent from the Security Education Platform, such as Training Assignment and Reminder notifications.



Training Email Notification Settings

Notification settings for when a user tries to report an email that contains training materials.

Notification message

Thank you for detecting a cyber-security training email sent by Proofpoint Security Awareness Training. Your actions are helping to keep your company safe.

Note: Training emails cannot be moved or deleted

Notification Message	Enter the text that will appear in the notification to the end user who reports a safe emai sent from the Security Education Platform or keep the default text displayed in the field.

10. Click **SAVE CHANGES** to keep the settings entered on the page.

Configuring Reported Email Forwarding Options

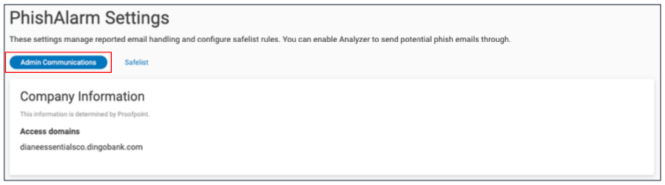
When end users report emails using the PhishAlarm button, you can configure forwarding options for each type of email, such as simulated phish, potential phish, safelisted, or training.

Use the steps below to configure the email forwarding options for PhishAlarm.

1. Sign into the Security Education Platform.

2. Click **PhishAlarm > Settings**.

3. Click the **Admin Communications** tab.



PhishAlarm Settings

These settings manage reported email handling and configure safelist rules. You can enable Analyzer to send potential phish emails through.

Company Information

This information is determined by Proofpoint.

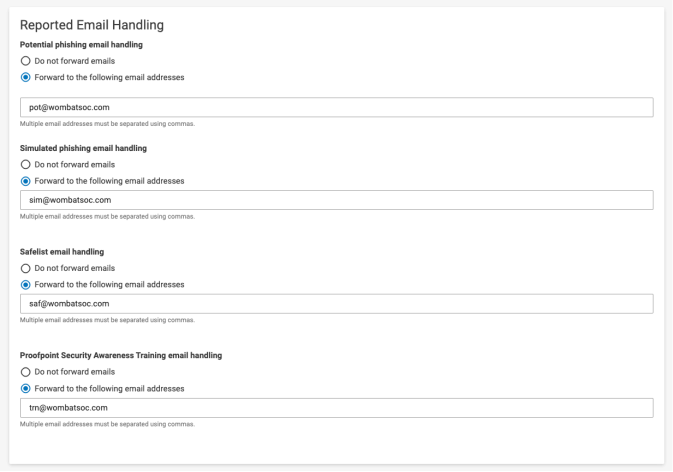
Access domains

dianeessentialsco.dingobank.com

Note: The “Company Information” section at the top of the page is read-only and contains the Access Domains for your company.

4. In the **Reported Email handling** section, use the table below to select how you want PhishAlarm to handle the emails reported by end users for these email types:

- Potential phishing email handling
- Simulated phishing emails (from Phishing Simulation)
- Safelist email handling
- Proofpoint Security Awareness training emails



Reported Email Handling

Potential phishing email handling

○ Do not forward emails
● Forward to the following email addresses

pot@wombatsoc.com

Multiple email addresses must be separated using commas.

Simulated phishing email handling

○ Do not forward emails
● Forward to the following email addresses

sim@wombatsoc.com

Multiple email addresses must be separated using commas.

Safelist email handling

○ Do not forward emails
● Forward to the following email addresses

saf@wombatsoc.com

Multiple email addresses must be separated using commas.

Proofpoint Security Awareness Training email handling

○ Do not forward emails
● Forward to the following email addresses

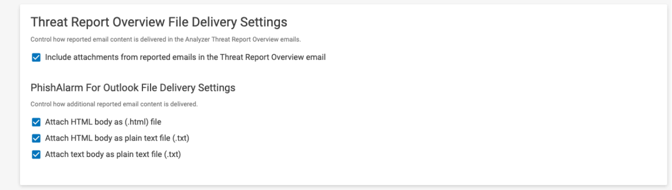
trn@wombatsoc.com

Multiple email addresses must be separated using commas.

Do Not Forward Emails	Select this option if you do not want to forward the emails to anyone.

Forward to the Following Email Address	Select this option to forward the emails to the email address(es) that you specify in Use a comma to separate multiple emails addresses. There is no limit to the numb that can be added.

7. In the **File Delivery Settings** section, configure how to forward reported emails with attachments from PhishAlarm For Exchange in the Analyzer Threat Report Overview emails. You can select more than one option or none.



Threat Report Overview File Delivery Settings

Control how reported email content is delivered in the Analyzer Threat Report Overview emails.

☑ Include attachments from reported emails in the Threat Report Overview email

PhishAlarm For Outlook File Delivery Settings

Control how additional reported email content is delivered.

☑ Attach HTML body as (.html) file

☑ Attach HTML body as plain text file (.txt)

☑ Attach text body as plain text file (.txt)

Note: PhishAlarm For Exchange environments include a headers.txt attachment that contains only the headers of the reported email. In addition to the headers being in an attachment text file (.txt), PhishAlarm For Exchange also includes the headers in the body of the email.

Forward the included attachments in the reported Phish	Select this option to include the email attachments when forwarding to the designate
Attach HTML body as (.html) file	Select this option to forward any HTML content in an email as an HTML attachment
Attach HTML body as plain text (.txt) file	Select this option to forward any HTML content in an email as a plain text attachmer original email.
Attach text body as plain text (.txt) file	Select this option to forward plain text email as a plain text attachment.

8. Click **SAVE CHANGES** to keep the settings entered on the page.

Configuring Safelist Emails

You can create rules to safelist designated email addresses. Safelisting involves specifying IP addresses, email addresses, or domain names that are considered trustworthy. When a user reports an email from a safelisted address, a prompt can display with a custom message to confirm the submission.

Note: The message text for the prompt is configured on the End-user Communications tab under the Safelisted Email Notification Settings section.

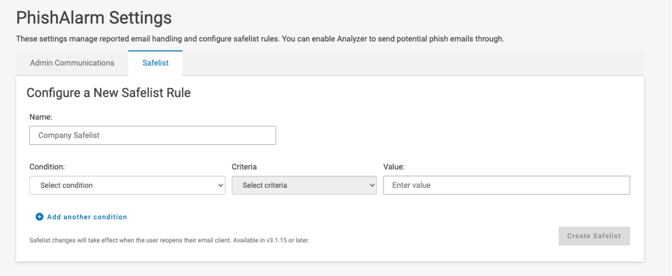
Use the steps below to configure the safelist emails.

1. Sign into the Security Education Platform.

2. Click **PhishAlarm** > **Settings**.

3. Click the **Safelist** tab.

4. Enter a title for the safelist in the **Name** field. Once created, the list can be accessed, edited and deleted in the **Safelist** section.



PhishAlarm Settings

These settings manage reported email handling and configure safelist rules. You can enable Analyzer to send potential phish emails through.

Configure a New Safelist Rule

Name: Company Safelist

Condition: Select condition

Criteria Select criteria

Value: Enter value

Safelist changes will take effect when the user reopens their email client. Available in v3.1.15 or later.

5. Select the Condition for the safelist and its corresponding **Criteria** and **Value** as follows.

Subject Line	This condition allows safelisting based on the email's Subject line text. If this condition is selected, enter the following fields: • **Criteria***: Select an option from the drop-down list. (See * below table for Criteria definitions.) • **Value**: Enter the text in the Subject line to be used for matching. The query is case sensitive. For exar Value is "[INTERNAL]," the system would match the Subject line of an email, "[INTERNAL] Please sul against one with "Submit your timesheet to your manager" in the Subject line.
Header	This condition allows safelisting based on a general query against all the information in the emai the queries. This option is for querying against any of the header information sent along with the body of the in **Name: Key** pairs. The PhishAlarm configuration has separate fields for each. If this condition is selected, enter the following fields: • **Criteria*** and **Value for name** (See * below table for Criteria definitions.) • **Criteria*** and **Value for key** (See * below table for Criteria definitions.) For example: If **Value for name** is DKIM and **Criteria** is Contains, and **Value for key** is d=xyzco

then the header below would not match because the **key** is d=email.microsoftonline.com and n

DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; s=200608;

d=email.microsoftonline.com; h=From:To:Subject:Date:MIME-Version:Reply-

To:List-ID:Cc:Message-ID:Content-Type:Content-Transfer-Encoding;

The three **Criteria** options for the safelist:

- **Starts with**: The query is matched if the **Value** is at the start of the Condition being queried against. For example, if the Value is "abc," then it will match against "abc123" but not "123abc".
- **Contains** The query is matched if the **Value** is contained somewhere in the string being queried against. For example, if the Value is "abc," then it will match against "abc123," "1abc23", and "123abc", but it will not match against "a123bc.
- **Advanced (Regex)** The query is matched using standard regex rules (not recommended)

6. To provide multiple query options, you can add more conditions for this safelist entry by clicking the **Add another condition** link. All conditions and criteria must match for the email to pass. **Note:** In all cases of matching for Criteria, the query is case sensitive. Safelist changes will take effect when the user reopens their email client.

7. Enable/Disable **Allow end-users to report emails matching this rule.** In the Admin Communications tab and under the Safelist email forwarding options, **Do not forward emails** is selected.

8. Click **CREATE SAFELIST**

9. Once created, the new entry displays in the **Safelists** table at the bottom of the page.

10. If needed, entries can be edited or deleted by clicking the corresponding **EDIT** or **DELETE** link.

PhishAlarm Safelisting Requirements

PhishAlarm connects to the Training Platform with a secured web connection on port 443 (TLS 1.2 or higher). Ensure that the appropriate URL for your hosted location is safelisted in your organization's firewall and proxy server to allow PhishAlarm to communicate securely with the Training Platform.

Note: For the most current safelisting information, access Community and search for "Safelisting Guide."

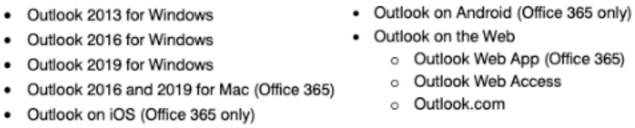
PhishAlarm for Exchange URLs	
For North America	https://addin-us.securityeducation.com

For European Union	https://addin-eu.securityeducation.com
For Asia Pacific	https://addin-oz.securityeducation.com
PhishAlarm For Exchange will also make calls to the following URLs:	https://appsforoffice.microsoft.com/ https://outlook.office365.com/EWS/Exchange.asm https://outlook.office.com/api/ https://addin-us.securityeducation.com

Note: Exchange Web Services (EWS) must be externally available for on-premise Exchange. In addition, OAUTH is required in order to use the PhishAlarm Add -in. The IP address, 52.1.14.157 (for North America), is for the resources that will be accessing your EWS for your on-premise Exchange Server. You must safelist 52.1.14.157 to allow the email from the EWS to reach our PhishAlarm server.

PhishAlarm For Exchange Installation

When deployed, PhishAlarm For Exchange (Office 365) will be automatically available through the web application as well as the following clients:



- Outlook 2013 for Windows
- Outlook 2016 for Windows
- Outlook 2019 for Windows
- Outlook 2016 and 2019 for Mac (Office 365)
- Outlook on iOS (Office 365 only)
- Outlook on Android (Office 365 only)
- Outlook on the Web
  - Outlook Web App (Office 365)
  - Outlook Web Access
  - Outlook.com

Exchange Server Requirements

Microsoft 365 - mail server requirements are in place. However, for users connected to on-premises installations of Exchange Server, the following requirements apply:

- Exchange Web Services (EWS) must be enabled and must be exposed to the Internet. PhishAlarm requires EWS to function properly.

- Oauth (Modern Auth) must be enabled for the Exchange Organization and the server must have a valid authentication certificate for the server to issue valid identity tokens.

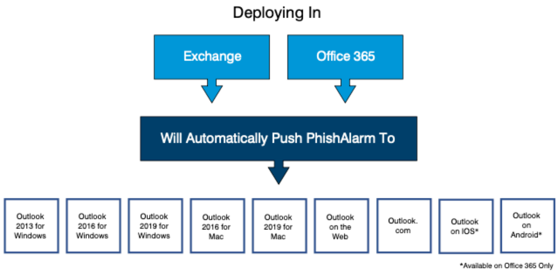
Note:

- Mobile add-ins are not supported on the U.S. Government Community Cloud (GCC) or on-premise Microsoft Exchange

Servers.

- Subscription versions of Outlook for Office 365 requires Edge Webview 2 Runtime.*
- Perpetual versions of Outlook 2013, 2016, and 2019 require Internet Explorer.*
- When deploying PhishAlarm For Exchange in an Exchange on-premises environment, Exchange Web Services (EWS) must be enabled.
- When using PhishAlarm For Exchange in virtual application environments, follow the guidance and best practices from your IT department on successfully supporting add-ins in such environments.

* Please see - https://docs.microsoft.com/en-us/off...ce-web-add-ins



Obtaining the Exchange Manifest URL Link

Use the steps below to obtain your Exchange Manifest URL link to use in the sections that follow.

1. Sign in the Security Education Platform

2. Click **PhishAlarm > Add-in Setup**

3. Click the **Install** tab

4. Scroll down to the **PhishAlarm For Exchange** section and click the **Copy** link next to the **Manifest** Link

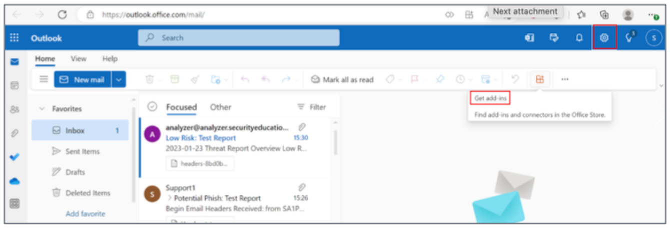
5. Depending on how you are installing the PhishAlarm add-in, proceed to either Installing the PhishAlarm Add-In for a Single User or Installing the PhishAlarm Add-In for Your Entire Organization where the manifest URL will be needed.

Installing the PhishAlarm Add-In for a Single User

Use the steps below to install PhishAlarm For a single user.

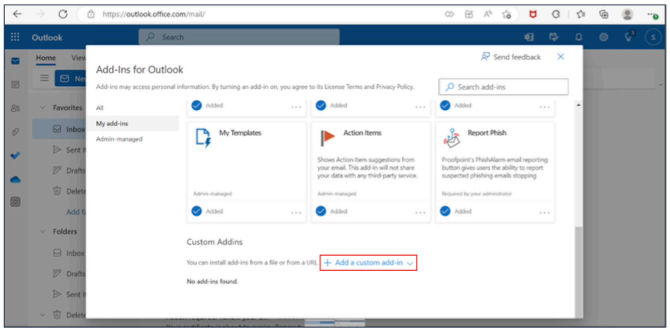
1. Log into your **account at https://outlook.office.com/owa/**

2. Select the **Settings** gear, and then select **Get add-ins**

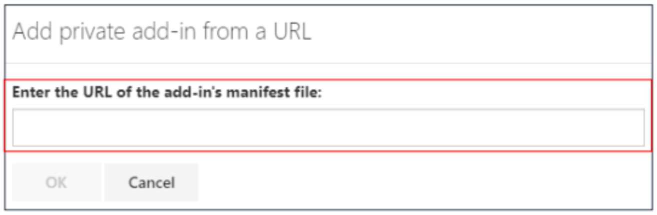


3. Select **My add-ins** from the left menu, and then select **+ Add a custom add-in** at the bottom.

4. Select **Add from URL** from the drop-down menu.

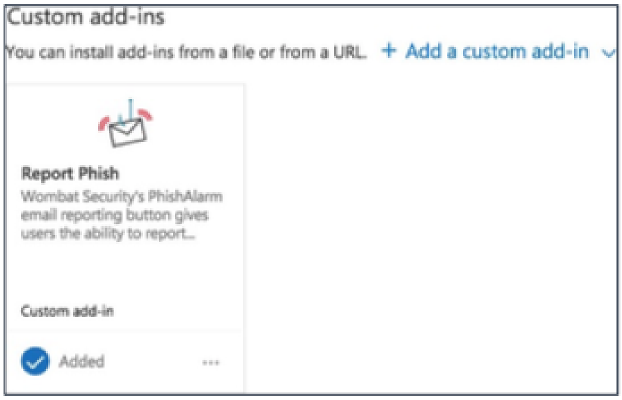


5. Paste the **URL** for the manifest file and click **OK**. Refer to Obtaining the Exchange Manifest URL Link to get a copy of the URL to paste here.


Add private add-in from a URL
Enter the URL of the add-in's manifest file:
OK
Cancel

6. Choose **Install**

7. Once the add-in is installed, you will see it added to your list of **Custom add-ins**.


Custom add-ins
You can install add-ins from a file or from a URL.
+ Add a custom add-in
Report Phish
Wombat Security's PhishAlarm email reporting button gives users the ability to report...
Custom add-in
Added

Installing the PhishAlarm Add-In for Your Entire Organization for On-Premises Exchange Server

Use the steps below to install PhishAlarm For your entire organization.

1. Log into the office portal at https://admin.microsoft.com or into your local Exchange 2013, 2016 or 2019 server.

2. Expand **Settings** and choose **Integrated Apps**

3. Select **Upload custom apps**

4. Under **Choose how to upload app**, select **Provide link to manifest file** and paste the PhishAlarm Manifest Link

5. Click **Validate**, then click **Next**

6. Specify which user(s) will have access to the PhishAlarm Add-In (everyone, specific users/groups, or just me) and click **Deploy** now

7. Click **Deploy** to finalize deployment

PhishAlarm Add-in Permissions

Microsoft is updating its add-in permissions process in January 2025, requiring **PhishAlarm Add-in** users to take specific actions to maintain uninterrupted functionality. This update transitions from legacy Exchange tokens to **Nested App Authentication (NAA)**, enhancing authentication and identity protection for Office 365 users.

How do I update my permissions?

Administrators of new and existing customers will need to accept a new series of permissions within to allow PhishAlarm for Exchange to access microsofts new authentication method.

To accept new permissions, use the following steps:

1. Open your Security Awareness platform and in the left column open **PhishAlarm > Add-in Setup > Install**

2. Scroll to Nested App Authentication for Office Add-ins and select **Connect**.

3. Authenticate to the resulting Microsoft 365 page using your Global Administrator account, select **Accept**.

What permissions are needed?

The following delegated permissions are needed for PhishAlarm for Exchange to continue to work properly.

- **Mail.Read** – Read user mail – This allows us to retrieve the email for analysis.
- **Mail.Read.Shared** - Read user and shared mail - This allows us to retrieve the email for analysis when reported from a shared mailbox.
- **Mail.ReadBasic** - Read user basic mail - This allows us to retrieve the email for analysis but omits the body, previewBody, attachments, and any extended properties. This is superseded by Mail.Read.
- **Mail.ReadBasic.Shared** - Read user and shared basic mail - This allows us to retrieve the email for analysis when reported from a shared mailbox but omits info in the body, bodyPreview, uniqueBody, attachments, extensions, and any extended properties. This is superseded by Mal.Read.Shared.
- **Mail.Readwrite** – Read and write access to user mail – This allows PhishAlarm to Move/Delete the items after the report is complete.
- **Mail.ReadWrite.Shared** - Read and write user and shared mail - This allows PhishAlarm to Move/Delete the items after the report from a shared mailbox is complete.
- **Mail.send** – Send mail as a user – This allows PhishAlarm to forward the mail as the user to an IT mailbox before analysis completes (Potential Phish Forwarding).
- **Mail.Send.Shared** – Send mail on behalf of others - This allows PhishAlarm to forward the reported mail from a shared mailbox as the user to an IT mailbox before analysis completes (Potential Phish Forwarding).
- **User.Read** – Sign in and read user profile – This allows us to review and log the user information reporting the mail.

For more details and a step-by-step guide, refer to the Nested App Authentication Update - Proofpoint Essentials Add-ins documentation here