Phishhook Add-In

Last Modified on 03/29/2024 3:31 pm CDT

PhishHook Outlook Add-in

To ensure users report suspicious emails to the proper team Phishproof offers the Outlook Add-In, PhishHook, where end users can report potential phishing threats in real-time.

As part of our holistic training solution, we promotes security awareness by enabling users to actively participate in identifying possible phishing emails.

Users who correctly identify phishing simulation emails from PhishProof receive positive reinforcement as soon as they click the PhishHook Add-in.

Logs of identified potential threats with email header information are also available for IT personnel to monitor in order to protect the organization and prevent widespread vulnerability.

Before Deploying your First Campaign, we recommend installing Phishhook if applicable, and educating users on how to report Phishing emails using this Outlook Add-In.

Before Organization-Wide Deployment the tool can be installed and activated for a small group of users.

PhishHook Add-in Best Practices and Instructions

1. Download PhishHook Add-in files or Copy the PhishHook Manifest URL by logging into your PhishProof Admin portal.
2. Follow the instructions for Office 365/Outlook 2016+ deployments options (Recommended).
3. Send preliminary emails to users informing them of how to use the PhishHook Add-In to report suspicious emails.
4. Send a test campaign to a select group.
5. If the test is successful, send a phishing campaign to users.
6. Monitor flagged phishing emails.

For Windows, Mac, and webmail, including the Outlook app for mobile devices, Please use the PhishHook Manifest URL for O365/Outlook 2016+

PhishHook is not supported for the following use-cases:

- On-Premise Exchange environments
- Shared mailboxes (The add-in works for individual user mailboxes)

We offer a few options for installing Phishhook for your Organization on Outlook.

The recommended option is Centralized Group Deployment through MS Office 365's Admin Console. Instructions for this installation method can be found here:

For testing purposes this add-in can also be installed by an individual by following the instructions found here:

Centralized Group Deployment through MS Office 365 Admin Console

We recommend using the Microsoft 365 Admin Console to install PhishHook on your Office 365 Outlook Web Application (OWA). This will push the add-in to all users so that they can report phishing emails from their desktop, mobile, or online Office 365 Outlook webmail. This will work on Outlook for Windows and Mac versions as well.

Reminder: As with any deployment, be sure to first deploy the PhishHook add-in to a small group of test users before rolling it out company-wide.

Through centralized deployment with the MS 365 Admin console, the PhishHook add-in is quite easy to install.

Once you have logged into the **MS 365 Admin console**, follow these steps:

1. Create a test group using the navigation bar to the left, click on**Groups ->+ Add a group**. Follow the instructions on screen to add users to your new group.

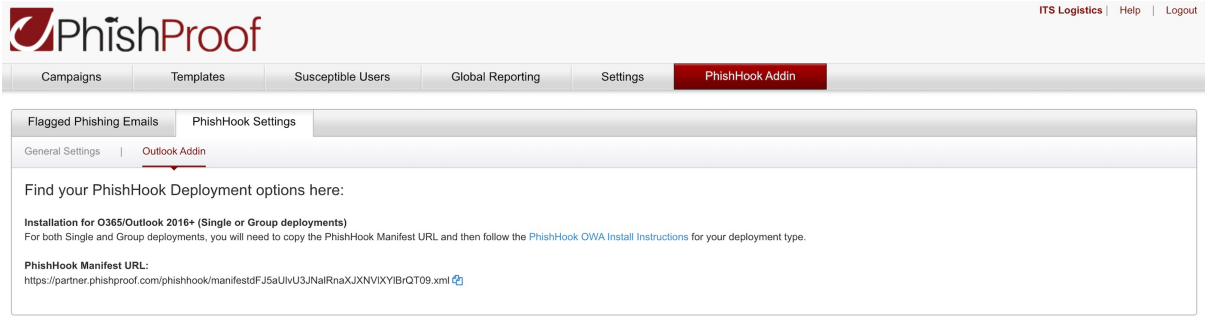
2. Using the navigation bar again, click on **Services & add-ins -> + Deploy Add-In**

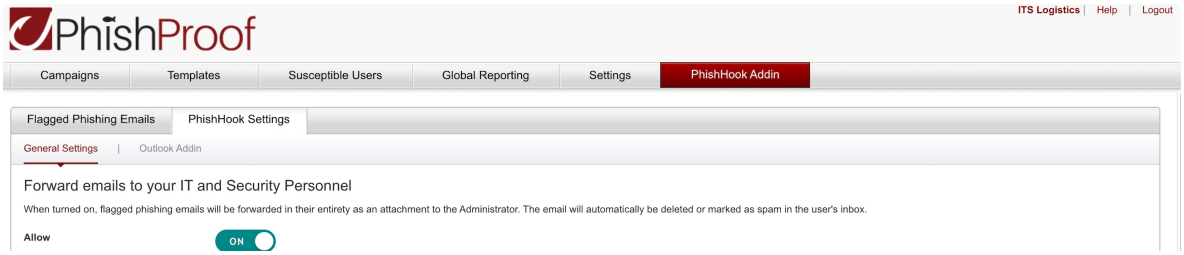
3. Follow the instructions on screen for Centralized Deployment.

Be sure to choose the option: “I have a URL for the manifest file.

4. In a separate browser tab, Open PhishProof through the iLMS Admin Console under the Applications tab. Click on **PhishHook Add-In -> PhishHook Settings**.

Then Copy the Manifest URL under the Office 365 Outlook Web for Mac and Windows download option.





Note: Each Phishhook Manifest URL is encrypted with your organization's unique ID

6. Return to the MS 365 Admin Console and paste the manifest URL in its corresponding field and click *Next*.

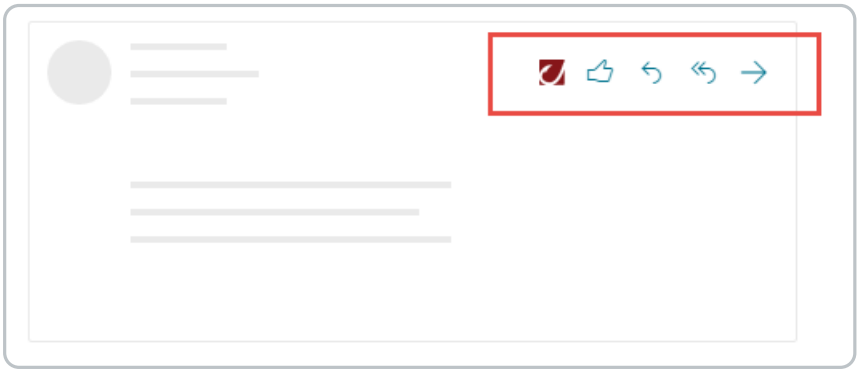
7. During your test deployment, select "Specific users/groups" to roll out the add-in to your test users. Otherwise, select "Everyone" when you are ready to roll out PhishHook company-wide.

8. Click the *Deploy now* button

9. We recommend sending out a message requesting everyone to relaunch Office, look for the new phishing reporting tool, and a short message on how to report a phish and its importance.

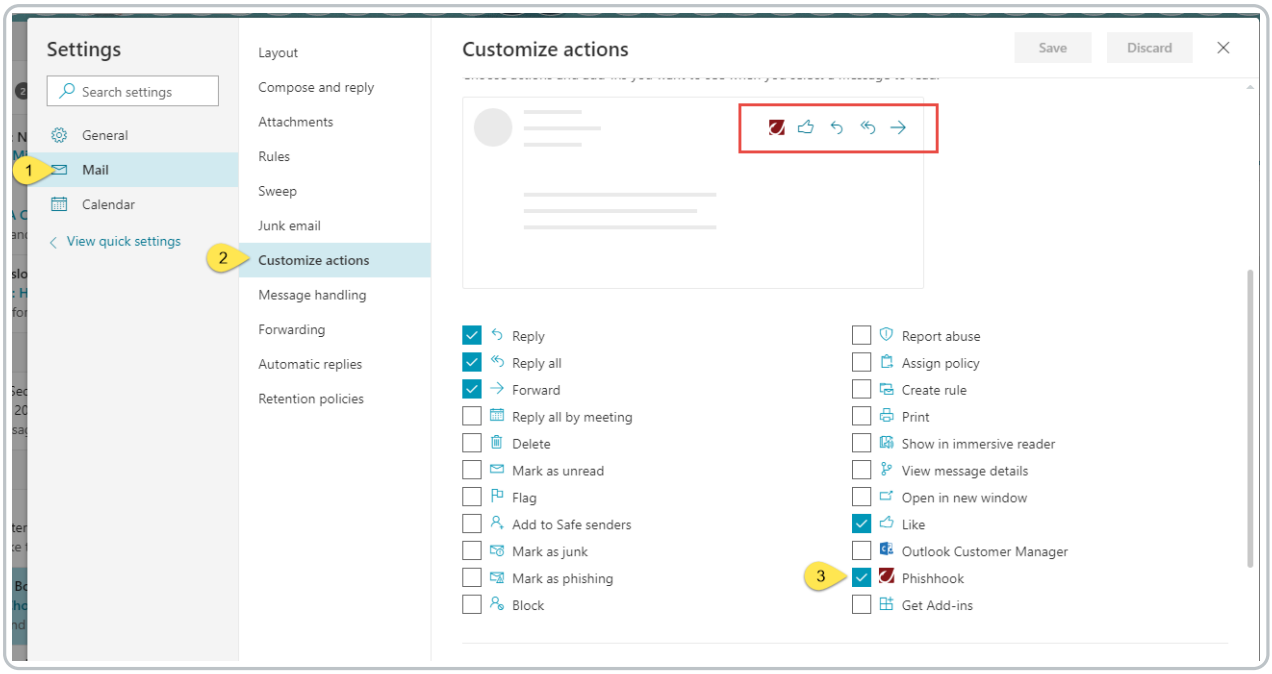
For detailed instructions, please read *Manage deployment of Office 365 add-ins in the Microsoft 365 admin center*.

Please have your users follow the PhishHook Reporting steps outlined in the PhishProof User's Guide to begin actively reporting phishing scams in real time.



If you're using OWA inside a browser and do not see the PhishHook button displayed at the top of each email as in the image above, follow these steps.

- Open the Outlook Settings (Gear Icon) in the upper right corner of OWA.
- Click "View all Outlook Settings,"
- Click "Mail" and "Customize actions."
- Scroll down to "Message Surface" section and check the box next to PhishHook.
- The PhishHook icon will now show in your Actions list for easy and convenient reporting.

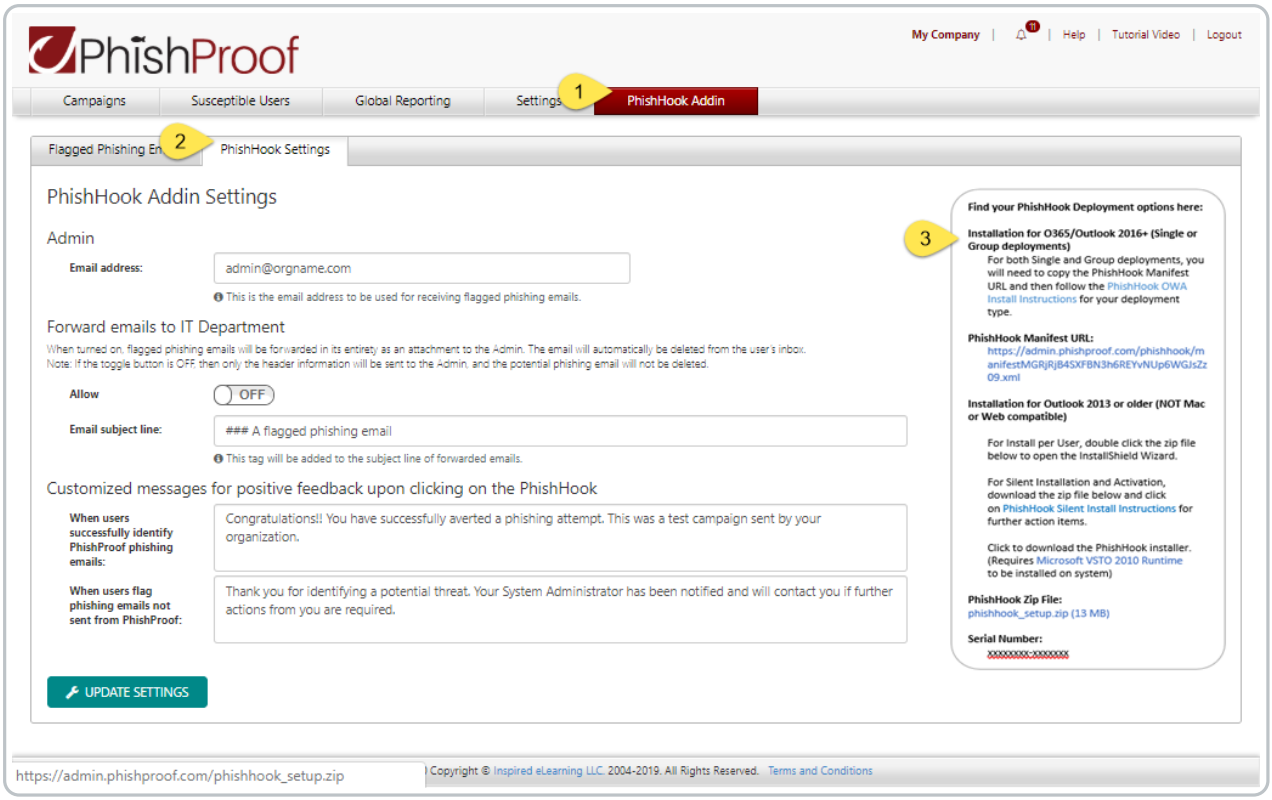


Note: The Outlook 365 version of this plug-in does not currently differentiate between phishing simulations from Phishproof and other potential real-world phishing emails. All emails reported by users will be forwarded to the internal email address specified for review.

Single Deployment through MS Office 365 Outlook Web Application (OWA)

For Single deployments, you can send the PhishHook Manifest URL to a user and have them install the PhishHook Add-in directly through their O365 Outlook Web Application.

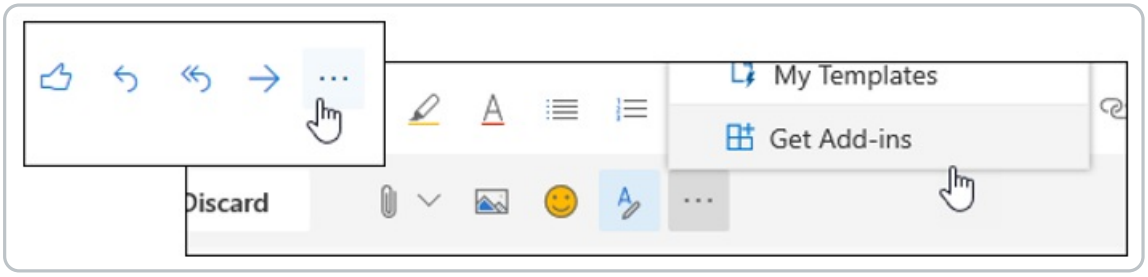
1. Navigate to the PhishProof Admin Console. Click on **PhishHook Add-In -> PhishHook Settings**. Steps to access shown here.



2. Copy the PhishHook Manifest URL and send it to the user.

3. Have your user open their O365 Outlook Web App and click on any email in their inbox.

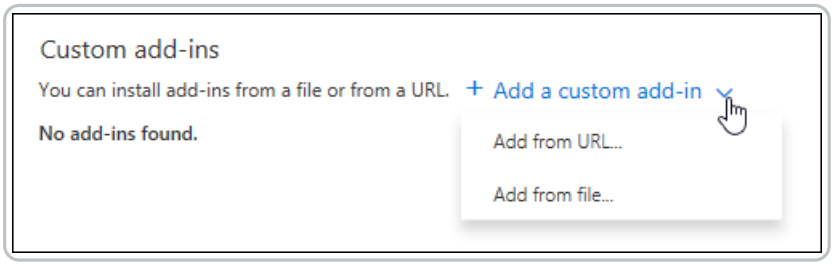
4. Click on the “More Actions” icon and scroll down to select “Get Add-ins.



5. Select My add-ins.

6. Scroll to the bottom of the page to Custom add-ins

7. Select “Add a custom add-in,” then “Add from URL…”

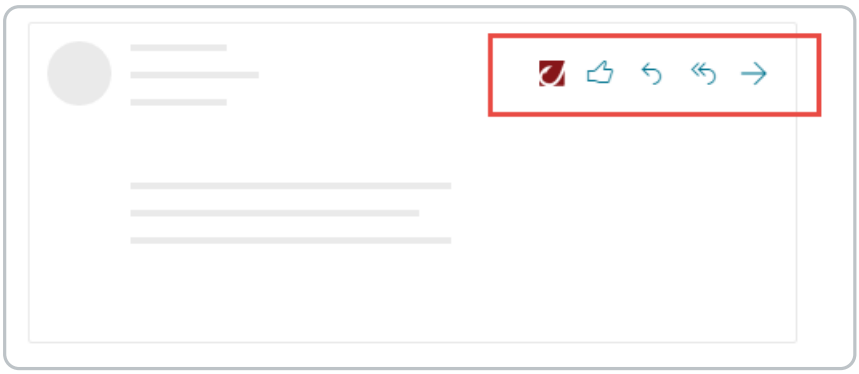


8. The user must enter the PhishHook Manifest URL that you provided.

Note: Each Phishhook Manifest URL is encrypted with your organization's unique ID

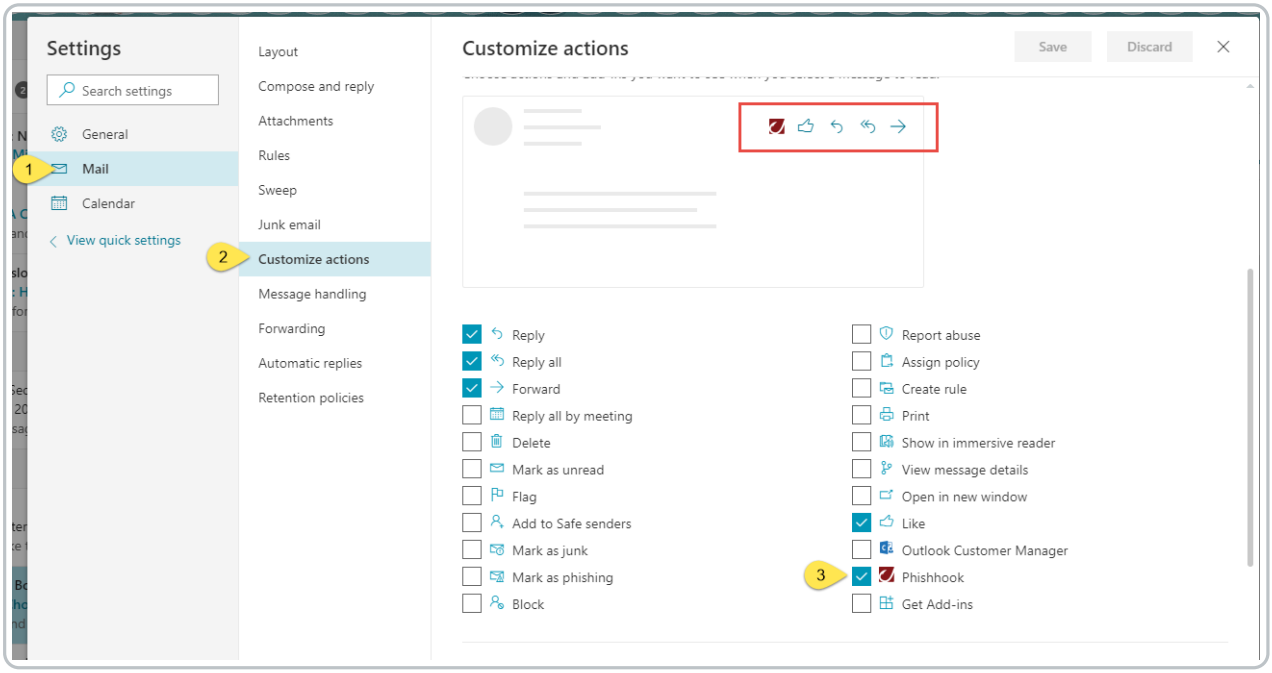
8. We recommend sending out a message on how to report a phish and its importance.

For detailed instructions, please read *Sideload Outlook add-ins for testing*. (Microsoft Article)



If you're using OWA inside a browser and do not see the PhishHook button displayed at the top of each email as in the image above, follow these steps.

- Open the Outlook Settings (Gear Icon) in the upper right corner of OWA.
- Click "View all Outlook Settings,"
- Click "Mail" and "Customize actions."
- Scroll down to "Message Surface" section and check the box next to PhishHook.
- The PhishHook icon will now show in your Actions list for easy and convenient reporting.



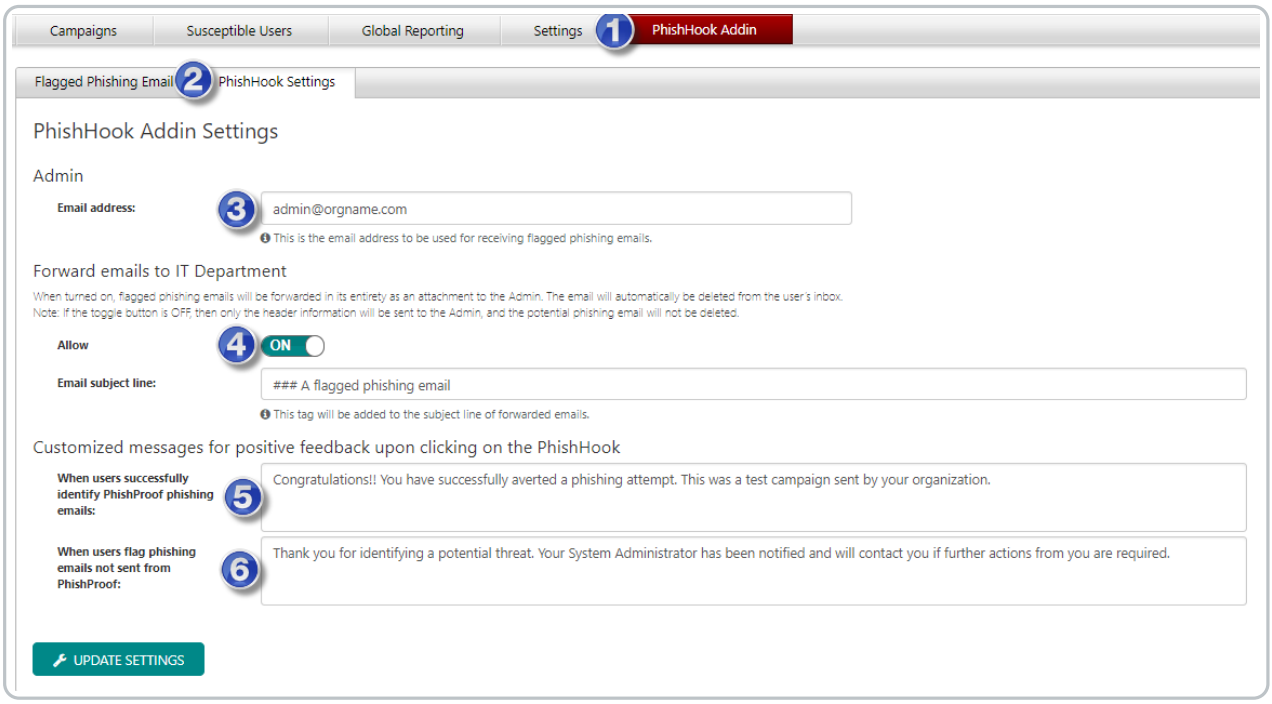
Note: The Outlook 365 version of this plug-in does not currently differentiate between phishing simulations from Phishproof and other potential real-world phishing emails. All emails reported by users will be forwarded to the internal email address specified for review.

Phishhook: Administrator Settings

Log in to your PhishProof Admin Console. Then, Navigate to the PhishHook Add-in tab.

Click on the Settings subtab to customize the sender email address and various messages. Click Update Settings when all changes have been completed.

Details are listed for each section of the Setting Tab below:

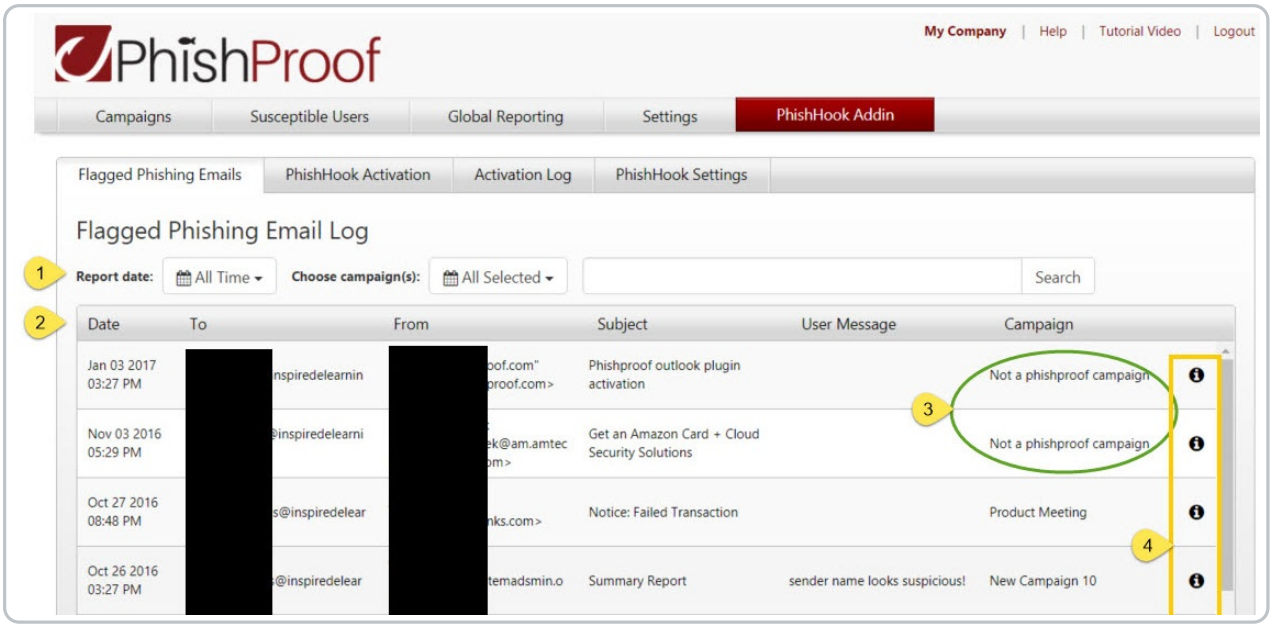


1. PhishHook Add-in Main tab
2. Settings subtab
3. This field allows you to input an email address to which reported emails will be sent.
4. This toggles the ability for emails to be forwarded to the Admin email address listed above.
   The data in the subject field will be added to the subject of the emails forwarded to the email address.
5. This message will be displayed when users successfully identify a PhishProof assessment email.
6. This message will be displayed when users identify a potential phishing email.

Monitoring the Flagged Phishing Email Log

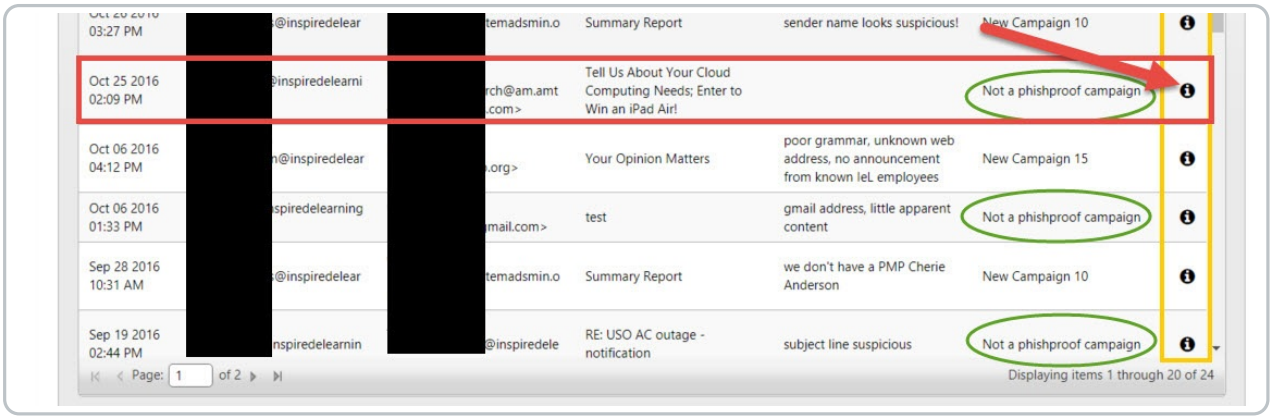
To view the log of user flagged phishing emails, navigate to the PhishHook Add-in tab, and click on the Flagged Phishing Emails sub-tab.

Notable items have been listed below:



1. Sorting is available by Report date, Campaign Name, or Not a Campaign. The default lists all flagged emails by date.
2. Not only is the recipient, sender, and subject line of the original email displayed, but also the user message upon reporting the email in its respective column.
3. In the Campaign column, flagged emails that are recognized as part of a phishing campaign will be labeled with its corresponding campaign name. Flagged emails originating from a source other than PhishProof will be labeled as Not a Phishproof campaign (green circle) and should be closely monitored by IT Staff.
4. Admins can then click on the Information icon to the right of each Campaign name in order to investigate the origin of the suspicious email. The email header information will be displayed in a pop-up.

For example, lets examine the email dated, Oct. 25, 2016, highlighted in red in the screenshot below:



When its Information icon is clicked, a pop-up window will appear with the following header information:

This information is provided in order to help the IT staff investigate real threats so that they can notify or warn their company employees of the threat.

Reporting Emails with Phishhook

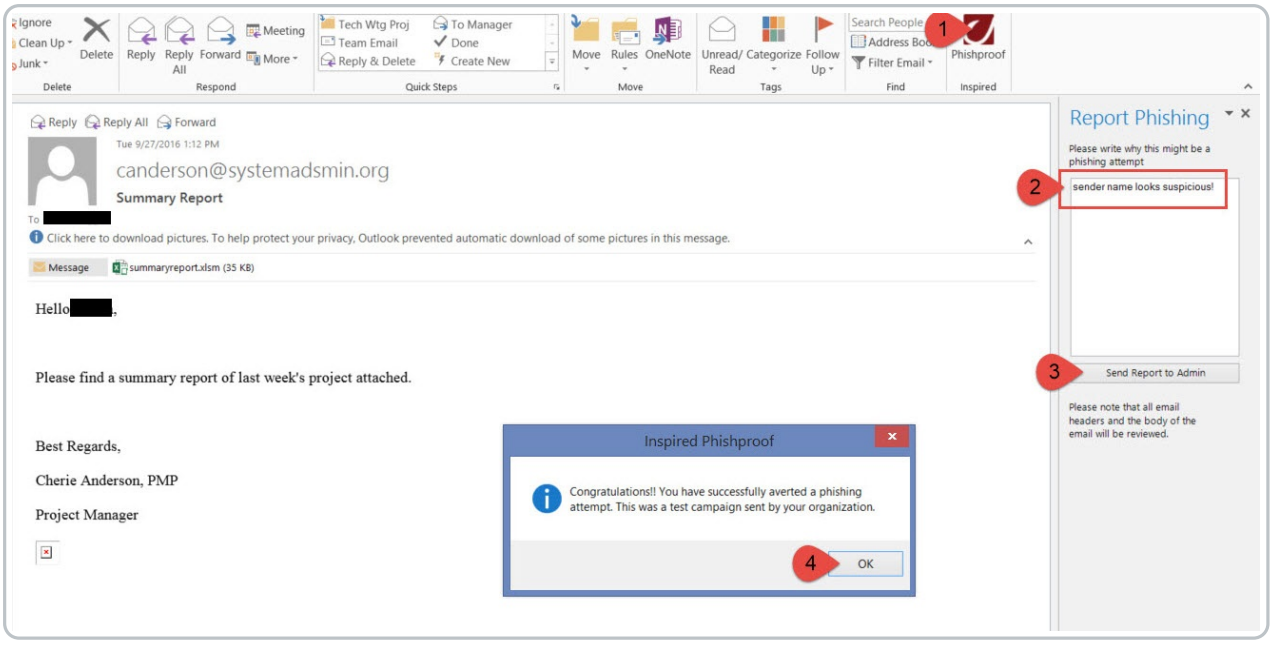
User Perspective

Reporting Potential Phishing Threats in real-time

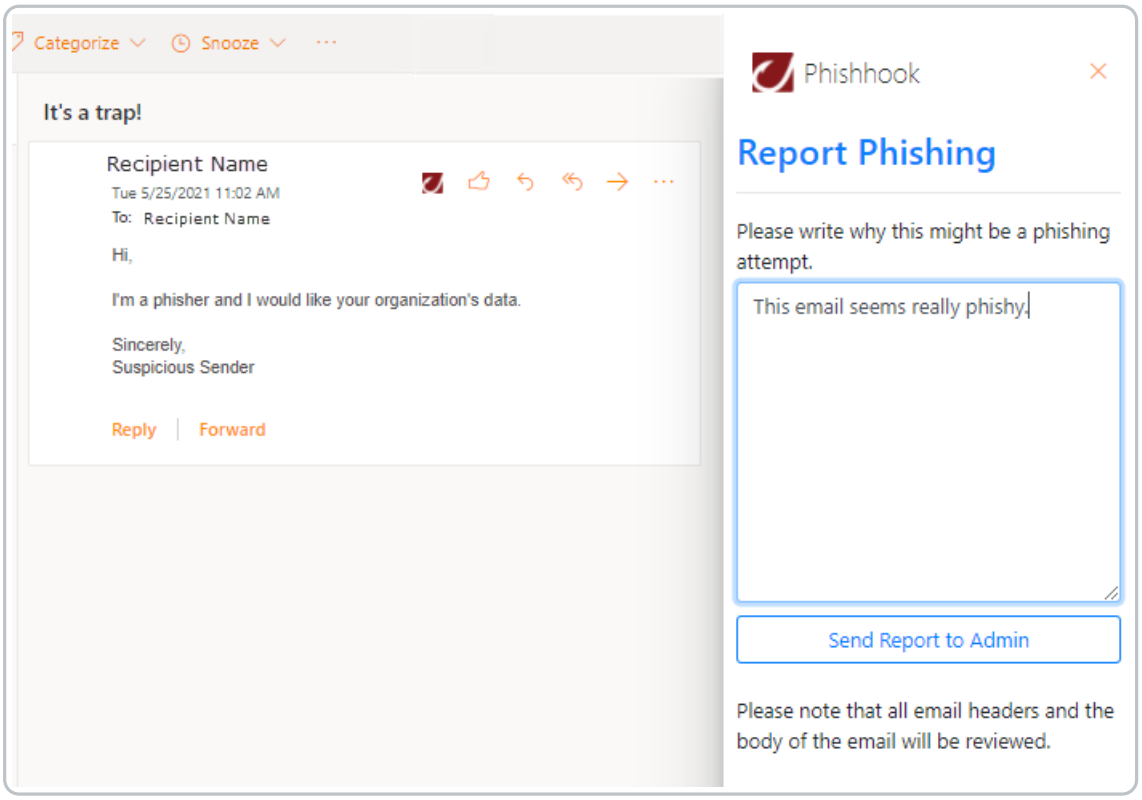
You may now begin clicking on the PhishHook button whenever you come across a suspicious email that resembles a phishing attack. The report and original email will be sent to your IT Department for review.

1. Click on the PhishHook button in the Outlook ribbon, or in the upper-right corner of your email on web.
2. The Report Phishing side pane will show on the right. Leaving a description is optional
3. Click the Send Report to Admin button to complete the reporting process.
4. A confirmation message will pop-up. Please click OK and continue with your daily routine.

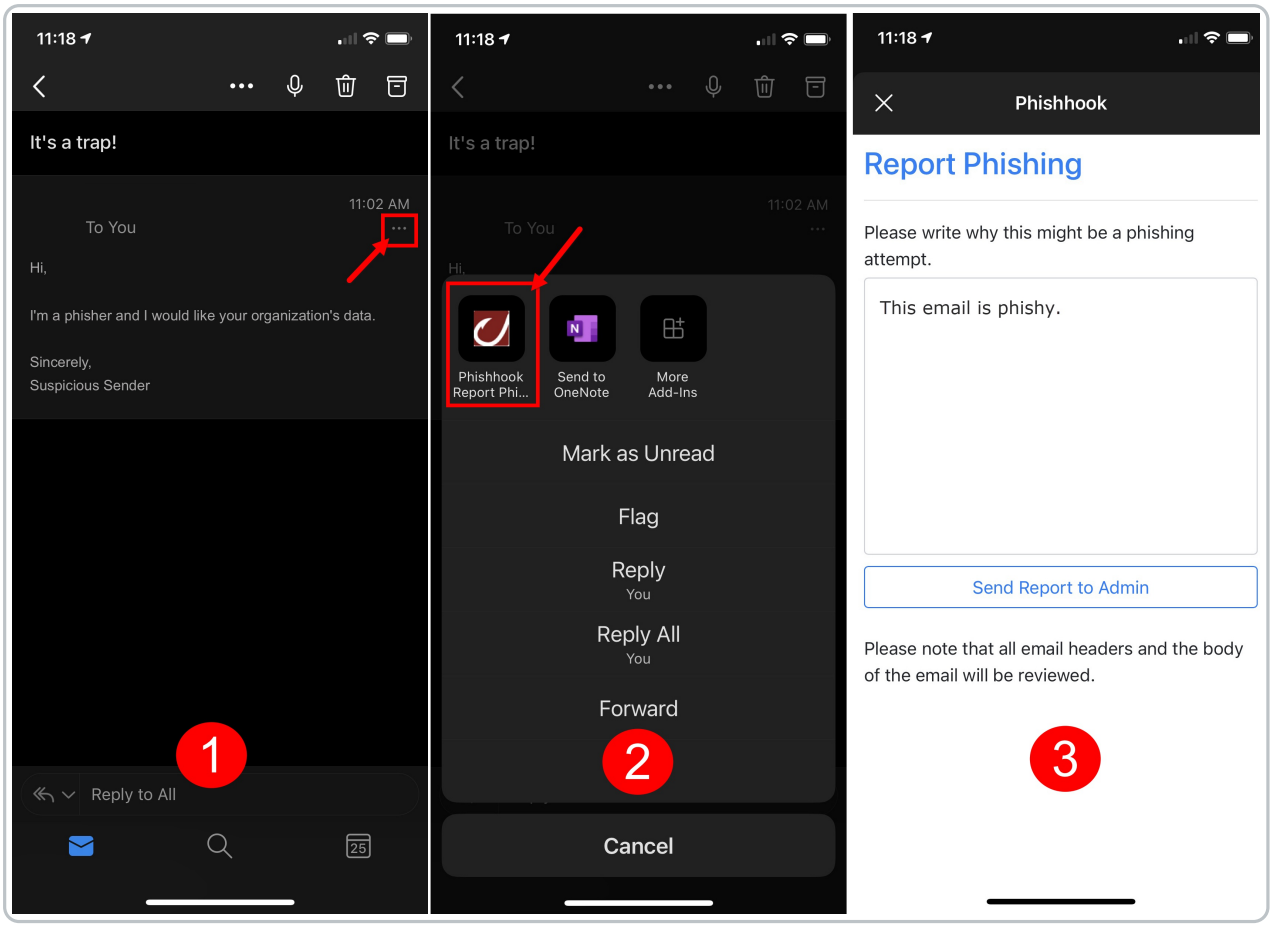
Outlook Desktop Client



Outlook Web Client



Outlook Mobile Client



Note: The Outlook 365 version of this plug-in does not currently differentiate between phishing simulations from Phishproof and other potential real-world phishing emails. All emails reported by users will be forwarded to the internal email address specified for review.

PhishHook Gmail Add-on Admin Guide

To ensure users report suspicious emails to the proper team, Phishproof offers the Gmail Add-On, PhishHook, where end users can report potential phishing threats in real-time.

As part of our holistic training solution, we promote security awareness by enabling users to actively participate in identifying possible phishing emails. Users who correctly identify phishing simulation emails from PhishProof receive positive reinforcement when they click the PhishHook Add-on. Logs of identified potential threats with email header information are also available for IT personnel to monitor to protect the organization and prevent widespread vulnerability.

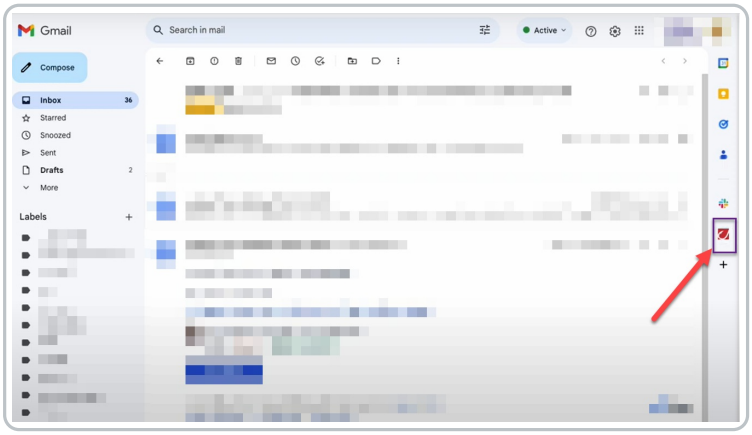
Before deploying your first campaign, we recommend installing Phishhook, if applicable, and educating users on reporting Phishing emails using this Gmail Add-on. Before organization-wide deployment, the tool can be installed and activated for a small group of users.

PhishHook Add-on Best Practices and Instructions

1. Navigate to iLMS and log in; click **Phishhook addin** in the top navigation bar
2. Select **PhishHook Settings**, click **General Settings** to review, then select Gmail Add-on, where you will be presented with 3 steps

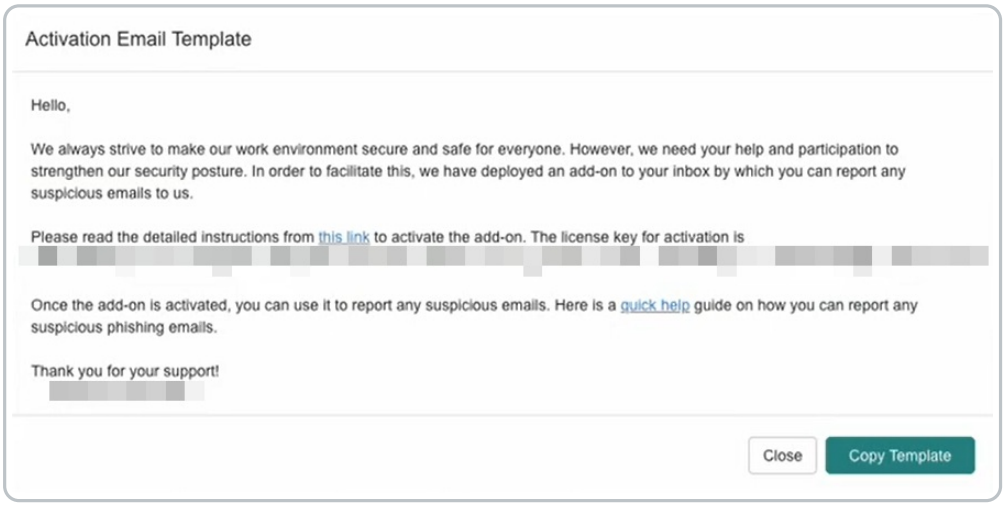
Step 1: Install Gmail Add-on

1. Navigate to PhishHook - Google Workspace Marketplace and click **Install**
2. You will be presented with a screen notifying you that you are granting access to your data; select the option to install the app automatically for either Everyone at your organization or Certain groups or organization units
3. Click **Finish**
4. To verify the installation, go to your Gmail inbox and click the arrow to show the side panel in the bottom right; you will see the PhishHook icon here



Steps 2 & 3: License Key & Send Email to End Users

1. Go back to the PhishProof console and ensure you are still on the **PhishHook Settings** screen
2. Under Step 3, click **View Activation Email Template**, then click **Copy Template**; the template will automatically include Step 2 (the license key)
3. Open a new email, add your subject, and paste the template into the body
    - Link to End-User Guide
4. After adding the appropriate email addresses or distribution lists, send the email as normal



Inspired eLearning Recommends

1. Send a preliminary email informing users how to use the PhishHook Add-In to report suspicious emails
2. Send a test campaign to a select group
3. If the test succeeds, send users a phishing campaign

After PhishHook is activated, you can review emails end users have flagged as phishing attempts within the PhishProof console.

1. From within the PhishProof console, go to **Phishhook addin**
2. Select **Flagged Phishing Email Log**; this will show you all emails that have been flagged as phishing

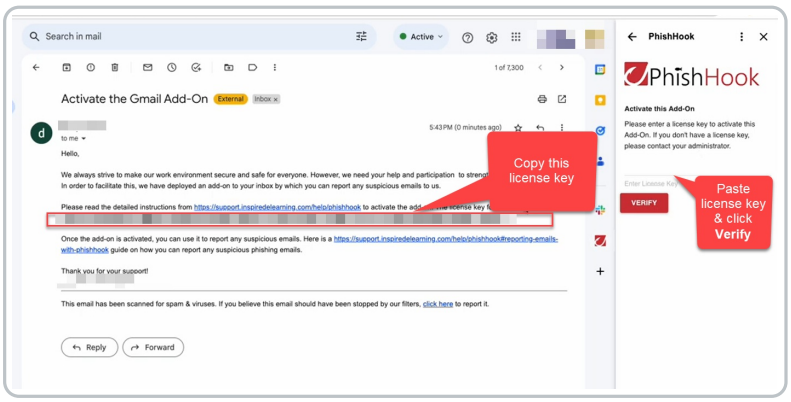
---

PhishHook End-User Guide

This guide will show you how to activate the PhishHook Gmail Add-on and report suspicious emails.

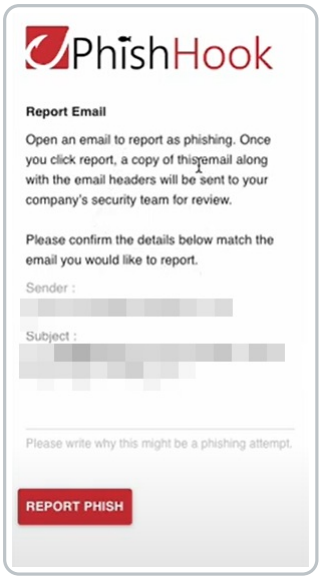
Activate Gmail Add-on

1. Select the add-on icon on the sidebar and Gmail will ask if you want to give the add-on access to your account; click Authorize Access and follow the steps to allow PhishHook access to your Gmail account
2. You should have received an email from your administrator about the PhishHook add-on that includes a license key; copy the license key from that email
3. In the PhishHook add-on, paste the license key and click **Verify**



Report Emails with Gmail Add-on

1. To report phishing attempts once PhishHook has been activated, open the suspicious email and click on the PhishHook icon in the sidebar
2. If desired, include a note on the text line about why you feel it might be a phishing attempt
3. Click **Report Phish**; the email you reported will be marked as Spam and moved to your Spam folder



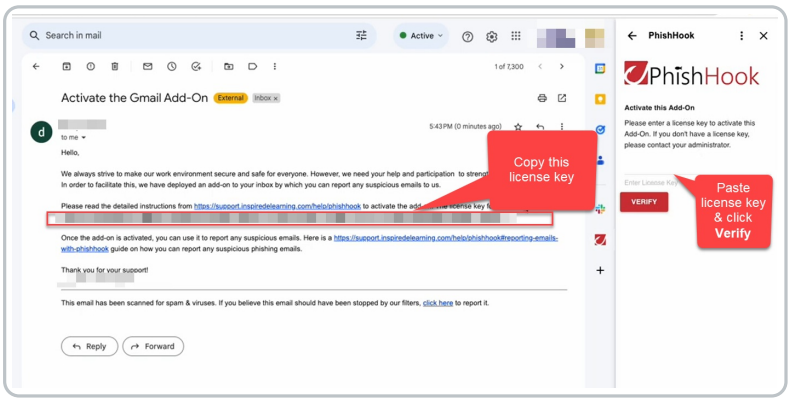
PhishHook Gmail Add-on End-User Guide: Activate Add-on

To ensure users report suspicious emails to the proper team, Phishproof offers the Gmail Add-On, PhishHook, where end users can report potential phishing threats in real-time. As part of our holistic training solution, we promote security awareness by enabling users to actively participate in identifying possible phishing emails.

This guide will show you how to activate the PhishHook Gmail Add-on and report suspicious emails.

Activate Gmail Add-on

1. Select the add-on icon on the sidebar and Gmail will ask if you want to give the add-on access to your account; click Authorize Access and follow the steps to allow PhishHook access to your Gmail account
2. You should have received an email from your administrator about the PhishHook add-on that includes a license key; copy the license key from that email
3. In the PhishHook add-on, paste the license key and click **Verify**



PhishHook Gmail Add-on End-User Guide: Report

Emails via Add-on

To ensure users report suspicious emails to the proper team, Phishproof offers the Gmail Add-On, PhishHook, where end users can report potential phishing threats in real-time. As part of our holistic training solution, we promote security awareness by enabling users to actively participate in identifying possible phishing emails.

This guide will show you how to report suspicious emails using the PhishHook Gmail Add-on.

Report Emails with Gmail Add-on

1. To report phishing attempts once PhishHook has been activated, open the suspicious email and click on the PhishHook icon in the sidebar
2. If desired, include a note on the text line about why you feel it might be a phishing attempt
3. Click **Report Phish**; the email you reported will be marked as Spam and moved to your Spam folder