

# Phishproof Initial Setup

Last Modified on 03/29/2024 2:56 pm CDT

## Timezone

### Setting the Timezone

Before starting a campaign, it is recommended to adjust the System Time Zone under the Settings Tab to match that of your Organization Headquarters, or that of the majority of the users.

PhishProof will send phishing simulation emails based on this TimeZone setting.

Be sure to click the Update Settings button to apply changes.

The screenshot displays the PhishProof Settings interface. At the top, there are navigation tabs: Campaigns, Susceptible Users, Global Reporting, and Settings (highlighted with a blue box and a circled '1'). Below the tabs, there are sub-tabs: Settings (highlighted with a blue box and a circled '2') and Filter Robots. The main content area is titled 'User Timezone' and features a dropdown menu for 'Timezone:' set to '(GMT-06.00) Central Time (US & Canada)' (highlighted with a blue box and a circled '3'). Below this, there is a toggle switch for 'Allow data to be included in global statistics for PhishProof' which is currently turned 'ON'. Underneath, the 'Customer information settings' section includes input fields for 'Phone' and 'E-mail', and a '+ Select logo...' button. A note below the logo button states: 'Note: Maximum Image size is 210x210 pixel.' At the bottom left, there is a green 'UPDATE SETTINGS' button with a wrench icon (highlighted with a blue box and a circled '4').

## Logo and Contact Info

### Logo and Contact Information

Under the Settings Tab you can also populate contact info for your internal IT support team and add your organization logo. This info will be added to the Education Landing Page, which is the learning aid that allows your

users to gain timely insight when they are susceptible to a phishing simulation.

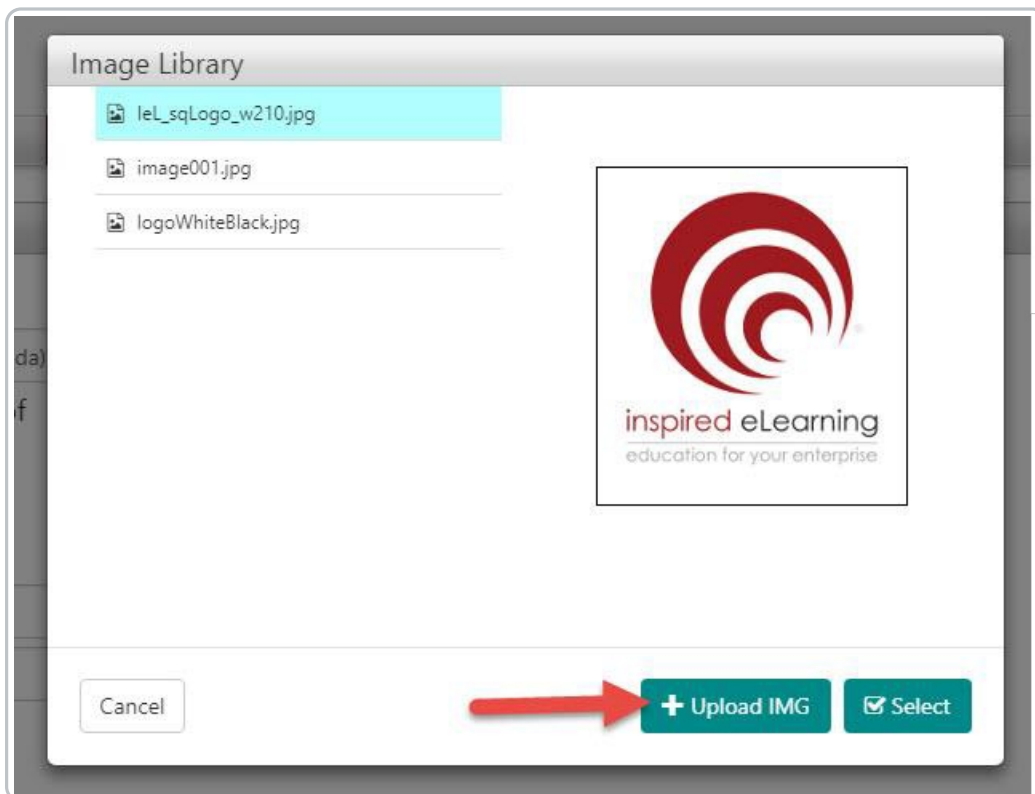
Simply, add your IT support information details, i.e. the phone number and/or email address of the point of contact for reporting or asking questions on potential phishing attacks.



You can further customize the Education Landing Page by inserting your company logo. Just click on the +Select Logo button and upload your logo.

Note: The maximum image size is 210 x 210 pixels. Accepted file types are jpg, jpeg, png, and gif.

Your logo and IT support information will be displayed in the upper right-hand corner of the Education Landing Page.



---

## Course Assignment and Rules

Each Phishproof simulation provides an opportunity to learn about real threats in a safe environment. If a learner does perform a risky action during one of the simulated phishing emails they are provided with immediate education in the form of a landing page. For many individuals, the education landing page may be enough

encouragement to build better habits. Other learners may require more in-depth training to reinforce best practices.

Phishproof's course assignment feature allows you to tailor the learning experience and assign additional education only where it is needed.

**Location:**

Phishproof > Susceptible Users Tab > Course Assignment sub-tab

## Course Assignments

Set the phishing count and choose one or multiple courses to be assigned when learners reach that threshold. You can specify up to 10 course assignment thresholds.



(click to view enlarged image)

### Add Assignments

Click the green + button to add an assignment. To delete an assignments click x button to the right of each item. You can add up to 10 different phishing count thresholds at which to assign training.

### Set Phishing Count

Type a number in the count field for each assignment. If a user's current phishing count reaches this threshold the specified training will be automatically assigned.

### Select Course(s) to assign

All available courses from the LMS are eligible for assignment. Click the dropdown to view all available content and check the boxes to select one or multiple courses to be assigned when a user reaches the specified phishing count.

**Course Assignments** You have unsaved content.  Apply To All Languages

Set the phishing count and choose one or multiple courses to be assigned when users reach that threshold. You can specify up to 10 course assignment thresholds. Once a user is assigned the last course their current phishing count will reset to 0 and the training assignments will repeat.

Count	Course to assign from iLMS
<input type="text" value="2"/>	1 Selected
<input type="text" value="3"/>	<input type="checkbox"/> S-131-SL-03: Security Awareness: Be a Strong Link
<input type="text" value="4"/>	<input type="checkbox"/> S-141: Security Awareness Essentials
	<input type="checkbox"/> S-161-AP: Defending Against Phishers
	<input type="checkbox"/> S-161-AP-05: Phishing Defense Essentials
	<input checked="" type="checkbox"/> S-162-PH-01: Phishing Defense Best Practices
	<input type="checkbox"/> S-173-02: Security Awareness – A Day In The Life

**Note:** We recommend selecting phishing-focused courses that are not in use with your regularly assigned LMS content for ease of tracking and reporting. This allows you to more easily create reports that focus solely on remedial training assigned via Phishproof.

### Apply to All Languages

To apply the same course assignment settings to all languages check the "Apply To All Languages" checkbox in the upper-right corner.

If preferred, different course assignment options can be specified for each language by selecting languages from the dropdown at the top of the page.



## Notification Email

### From Email

The email notification will come from this address. The dropdown allows you to choose whether the email sends from the phishproof.com domain or [inspiredlms.com](https://inspiredlms.com) which will match emails from the LMS.

Check

### From Name

This is the friendly name learners will see as the sender of the email.

### Email Subject

Customize the subject of your email. Please note the default text is already translated for you.

If the subject of the email is customized it can either be applied to all other languages in English, or you can implement your own custom-translated content.

*Please note: Any custom-translated text must be provided by your organization as this is not a service offered.*

### Apply to All Languages

To apply the same settings for From Email, From Name, or Email Subject to all other available languages check the box next to each section before saving. If preferred, different options can be specified for each language by selecting languages from the dropdown at the top of the page.

#### Notification Email

<b>From Email</b>	<input type="text" value="noreply"/> @ <input type="text" value="phishproof.com"/>	<input type="checkbox"/> Apply To All Languages
<b>From Name</b>	<input type="text" value="My Company"/>	<input type="checkbox"/> Apply To All Languages
<b>Email Subject</b>	<input type="text" value="You have been assigned training"/>	<input type="checkbox"/> Apply To All Languages

### Email

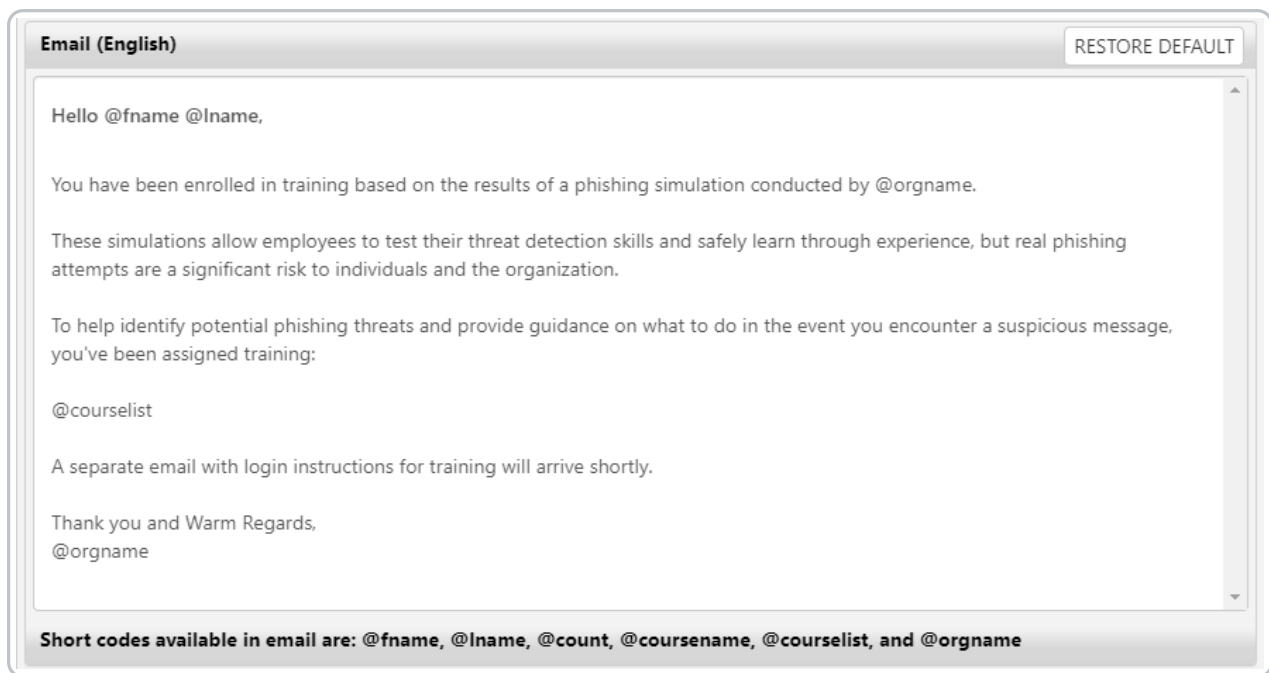
This is the email notification that is sent to the learner each time they are assigned a course as a result of a Phishing Campaign. This notification informs them of the reason the course has been assigned and instructs them on what to expect.

The text of this email can be customized for each language by selecting the language from the dropdown at the top of the page.

*Please note: Any custom-translated text must be provided by your organization as this is not a service offered.*

### Short Codes

A few system variables have been provided to dynamically populate information such as the learner's first and last name, the course list, the learner's phishing count, and your organization's name. All available system variables are listed at the bottom of the email editing pane.



### Update Settings

Once you're ready to save your settings click "Update Settings" at the bottom of the page. Remember to check the "Apply to All Languages" box for any applicable settings you'd like to apply to every available language.

## Reset and Repeating Assignments

To ensure users continue to receive education even if they exceed all set thresholds for training assignments their "current phishing count" resets to 0 once they've been assigned all available training. They will then repeat the assignments at each threshold in the event their phishing count continues to increase.

Both the total all-time phishing count and the current phishing count for a learner can be viewed in the [Phishproof Susceptible Users Report](#), as well as details about which campaigns resulted in course assignments.

---

## 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 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 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:

### Centralized Group Deployment through MS Office 365's Admin Console

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

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

---

## 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

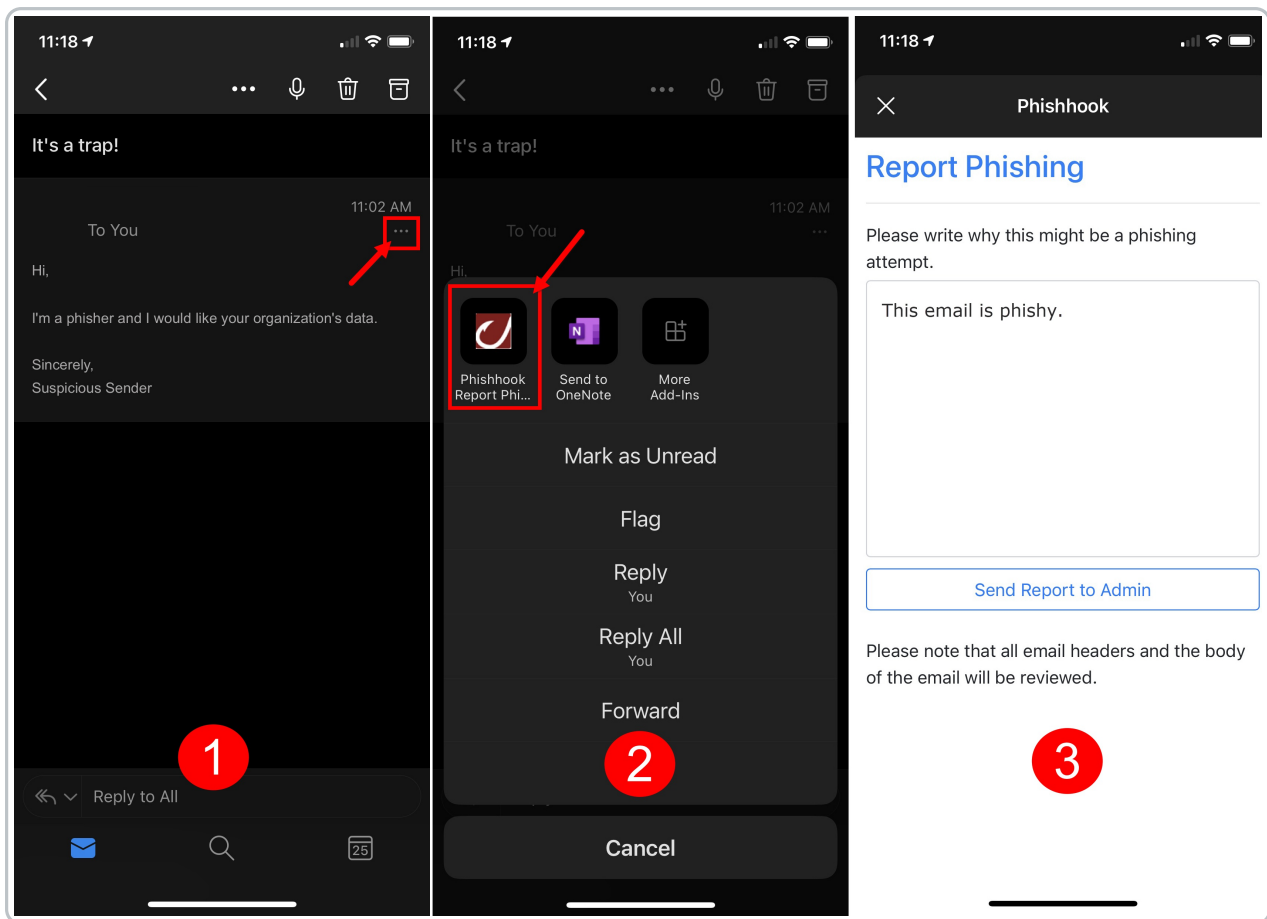


## Outlook Web Client

The screenshot shows the Outlook Web Client interface. On the left, an email is displayed with the subject "It's a trap!". The email content includes a recipient name, a date (Tue 5/25/2021 11:02 AM), and a message that reads: "Hi, I'm a phisher and I would like your organization's data. Sincerely, Suspicious Sender". Below the email content are "Reply" and "Forward" buttons.

On the right, a "Phishhook" dialog box is open, titled "Report Phishing". It contains the text: "Please write why this might be a phishing attempt." Below this is a text input field with the text "This email seems really phishy". At the bottom of the dialog is a button labeled "Send Report to Admin". Below the dialog, a note states: "Please note that all email headers and the body of the email will be reviewed."

## 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.

## Pilot Testing

### Pilot Testing before Deployment

For best results and extra assurance we highly recommend running a few rounds of Pilot Testing prior to rolling out campaigns to larger groups of users.

This ensures that simulation emails make it from Phishproof to the users inbox, that results record accurately without false positives, and that data is allowed be captured and sent back to the Phishproof console.

If possible, have members from different teams participate in the Pilot test, preferably with varying locations, GPO settings, etc.

The more diverse the group, the better.



**Note:** We recommend testing different template types as internal systems may handle emails with attachments and login forms differently than emails with links alone.

---

## Click Filter

### False Positives in Phishing Simulations

When sending out phishing simulations you may encounter false positives caused by security systems testing links in an email before it reaches the user's inbox. These are referred to as bot clicks. This function is a security measure to protect email recipients from malicious links, but it can cause false assessment failures and inaccurate results for phishing simulations.

Phishproof's click filter helps prevent bot clicks from counting against users by excluding specific IP addresses or ranges from phishing simulations.

#### Location:

Phishproof > Settings > Click Filter

### Identify Bot Clicks

We recommend running a pilot test with a small pool of individuals before sending phishing simulations to the entire company. Not only does ensure the email is delivered to the recipient's inbox, but this process also allows admins to ensure results are accurate and address any sources of false positives before full deployment.

For good measure, we also recommend testing with different template types as emails with attachments or faux login pages may be handled differently than emails with links alone.

Many false positives can be addressed with the proper allow listing of Phishproof's domains to exempt them from link analysis by spam filters and other security filters and systems, but any sources of false positives not addressed during the allow listing process can be filtered out in Phishproof so long as you know the IP address(es).

There are multiple ways to identify bot clicks. Here are a few potential indicators:

- Feedback from the intended recipient(s) stating they did not click despite the console reporting a click.
- Clicks that occur for multiple users at the exact same or almost the exact same time.  
(usually immediately after the email sends)
- The IP Address associated with the click belongs to one of your company's security products

### Locate IP Address Information for a Campaign

To view the IP address associated with a link click, form submission, or attachment opening in Phishproof follow the steps below.

- From the Campaigns page, click the name of the campaign to view campaign details
- Navigate to the "User Details" tab
- Enable the "Show User IP Information" in the upper right.
- All recorded IP addresses will display for the campaign.

- To Export the IP information click the "Export Results to Excel" button above the IP Information toggle.



## Add/Edit IP Addresses in Click Filter

If clicks from a specific IP address or IP range have been identified as bot clicks these IPs can be added to Phishproof's Click Filter.

Adding IPs to the filter prevents any clicks generated by these IPs from being counted in phishing simulations.

### Location:

Phishproof > Settings > Click Filter

To add an IP address or range of IP addresses to the click filter click the "Add IP Filter" button.

Filtering helps prevent false positives caused by entities other than the intended recipient interacting with the email. Many email security systems test emails before they reach the recipient's inbox to ensure their safety. Ignore clicks from specific sources by adding an IP or IP range to filter out of campaigns.

Ignore click tracking from these Hosts:

IP	Description
1.2.3.0-1.2.3.255	This is a Bot
1.2.3.255	This is also a Bot

Add IP Filter    Remove Susceptible Users Retroactively

Input the IP address or range of IP addresses in one of the formats specified in the pop-up and add a description. Once this is complete, click "Done" to save your new filter.

### Edit IP Filter

Network ranges can be specified as:

1. Wildcard format: **1.2.3.\***
2. CIDR format: **1.2.3.4/24**
3. Start-End IP format: **1.2.3.0-1.2.3.255**

IP Filter:

Description: (Max 2000 characters)

Cancel Update

Any clicks from the specified IP(S) will no longer count in future phishing simulations.



If any clicks in previous campaigns belong to one of the filtered IPs they can be removed with just a couple more steps.

## Remove Clicks from Previous Campaigns

Location:

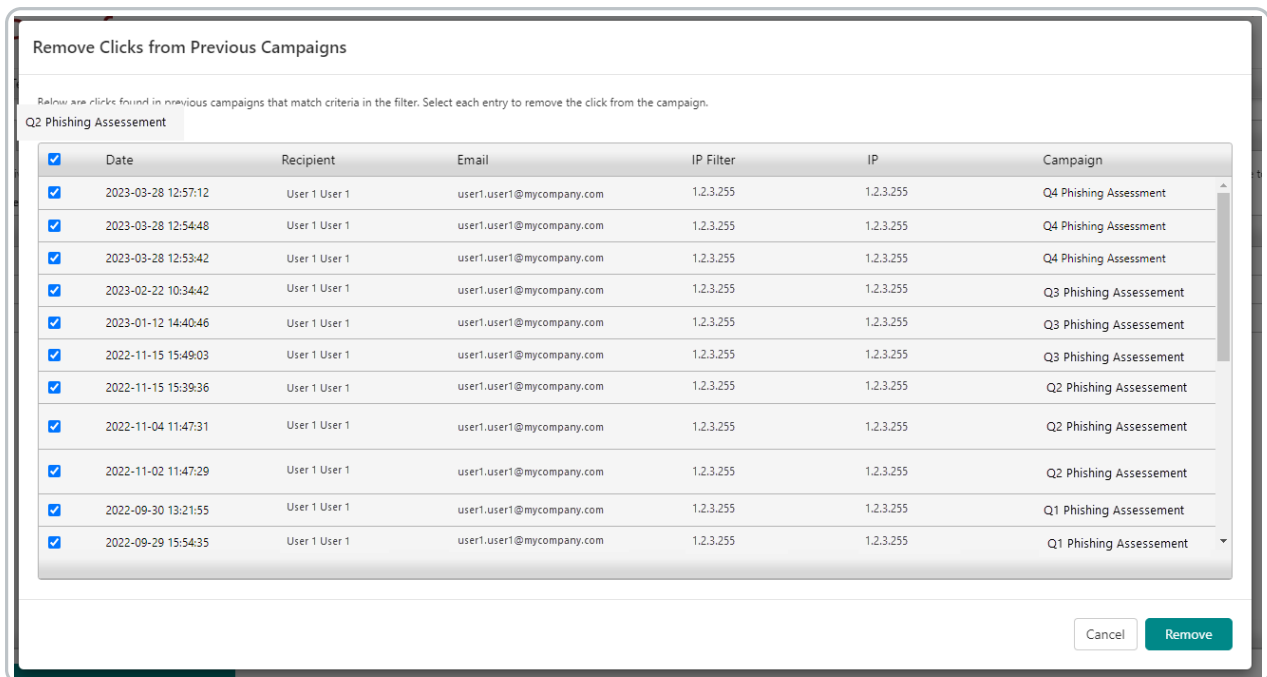
Phishproof > Settings > Click Filter

To remove clicks from previous campaigns based on your current IP filters click the "Remove Susceptible Users Retroactively" button at the bottom of the page.

1.2.3.255	This is also a Bot		
Add IP Filter		Remove Susceptible Users Retroactively	

Any clicks from previous phishing simulations that are associated with an IP address that is included in the Click filter will display. Select all the information you'd like to remove and when ready click the "Remove" button. Please note this action cannot be undone, so look over the selections carefully before confirming the removal.

All of the selected clicks will be removed from their respective campaigns and the user(s) will no longer display as having clicked a link during that campaign.



## 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.

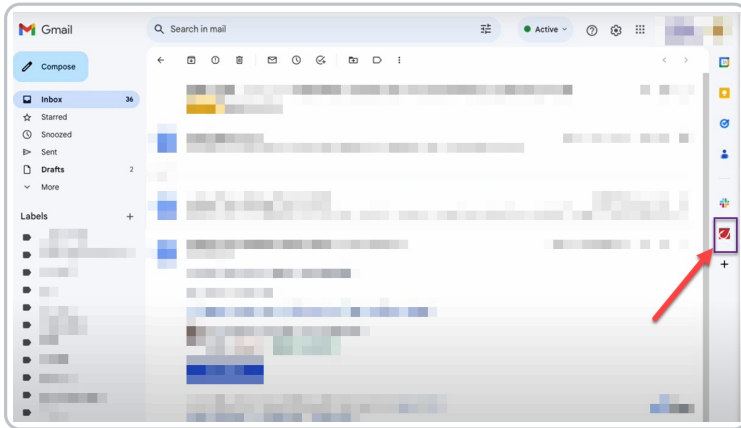
Before deploying your first campaign, we recommend installing Phishhook, if applicable, and educating users on reporting Phishing emails using this Gmail Add-on. Before organization-wide deployment, the tool can be installed and activated for a small group of users.

## 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

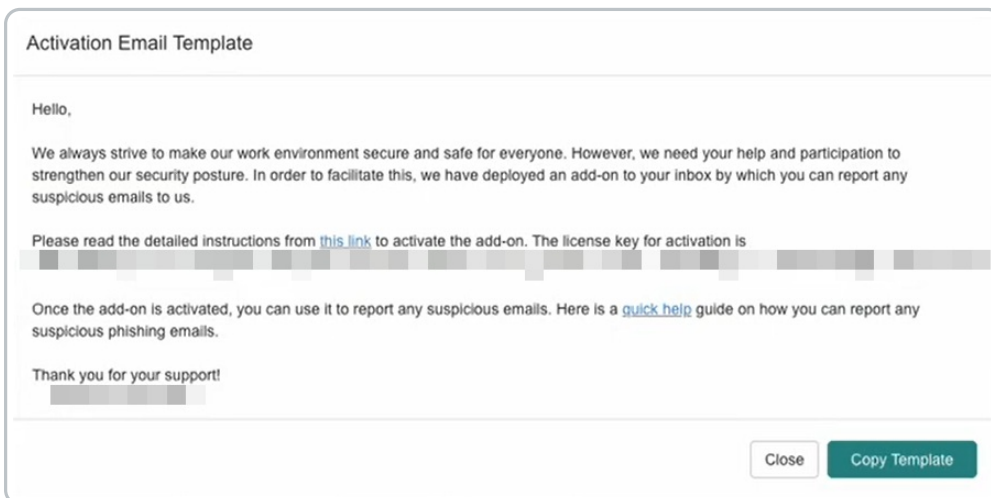
### Step 1: Install Gmail Add-on

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.

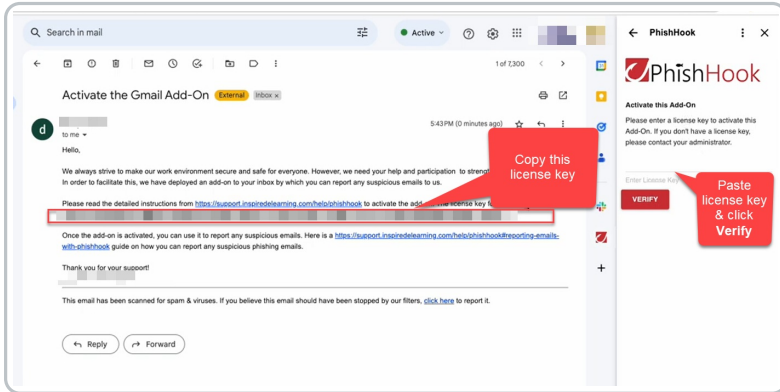
1. From within the PhishProof console, go to **Phishhook addin**
2. Select **Flagged Phishing Email Log**; this will show you all emails that have been flagged as phishing

# PhishHook End-User Guide

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

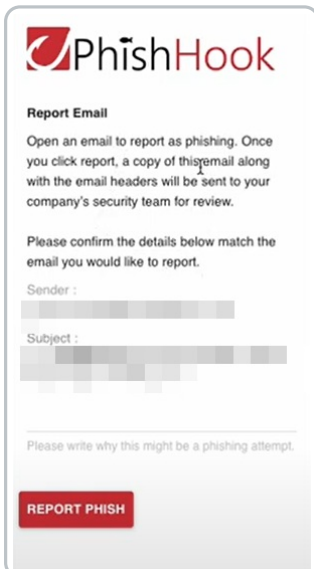
## Activate Gmail Add-on

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



---

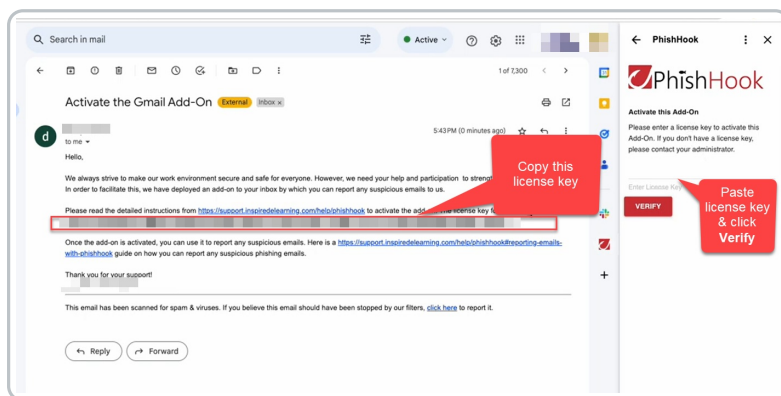
# PhishHook Gmail Add-on End-User Guide: Activate Add-on

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



**Report Email**

Open an email to report as phishing. Once you click report, a copy of this email along with the email headers will be sent to your company's security team for review.

Please confirm the details below match the email you would like to report.

Sender :

[Redacted]

Subject :

[Redacted]

Please write why this might be a phishing attempt.

**REPORT PHISH**

