Security Awareness Training Partner Guide

Catch Phish Outlook Plug-In

Instant in-email phishing analysis & training access

Internal Use Only

Telesystem
IT's About Trust

#HackersSuck

www.TrustTelesystem.com

Catch Phish Email Analysis Tool

Table of Contents

Catch Phish Email Analysis Tool

Resources

- Security Awareness Training Program Overview
- User Management Partner How-To Guide
- Catch Phish Partner FAQ
- Catch Phish Management FAQ
- Catch Phish User FAQ
- Catch Phish Deployment Video
- Catch Phish Go-to-Market Kit

What is the Catch Phish Outlook Plug-In?

Advanced email analysis and access to security training with the click of a button

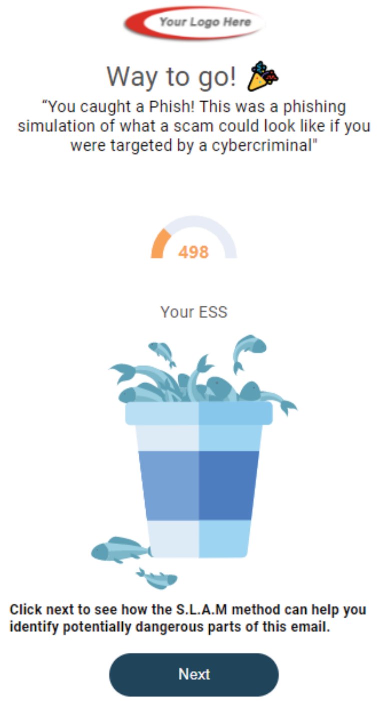
EMAIL ANALYSIS

- **Problem:** Old-school phishing education simply tests a user's ability to identify a phishing email. There are two outcomes: either they identify it, or fall for it, but the simulation doesn't *actually* teach users about **what** makes these emails phishy.
- **Our solution:** With the click of a button, employees can leverage machine learning and artificial intelligence to highlight sender, link, attachment, and message red flags in phishing simulations AND real, live emails that hit their inbox.

SECURITY TRAINING

- **Problem:** Employees struggle to keep up with their ongoing security program. Whether they're too busy to log into the portal to take the training or forget their password and don't want to bother changing it – employees aren't doing their part.
- **Our solution:** With in-email access to the weekly training videos and quizzes, they never have to leave their inbox to stay up-to-date on the latest security trends ever again.

THE BASICS OF THE CATCH PHISH OUTLOOK PLUG-IN



Way to go!

"You caught a Phish! This was a phishing simulation of what a scam could look like if you were targeted by a cybercriminal"

Click next to see how the S.L.A.M method can help you identify potentially dangerous parts of this email.

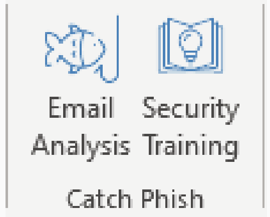
Our Catch Phish Outlook Plug-In has two main functionalities: Email Analysis and Security Training.

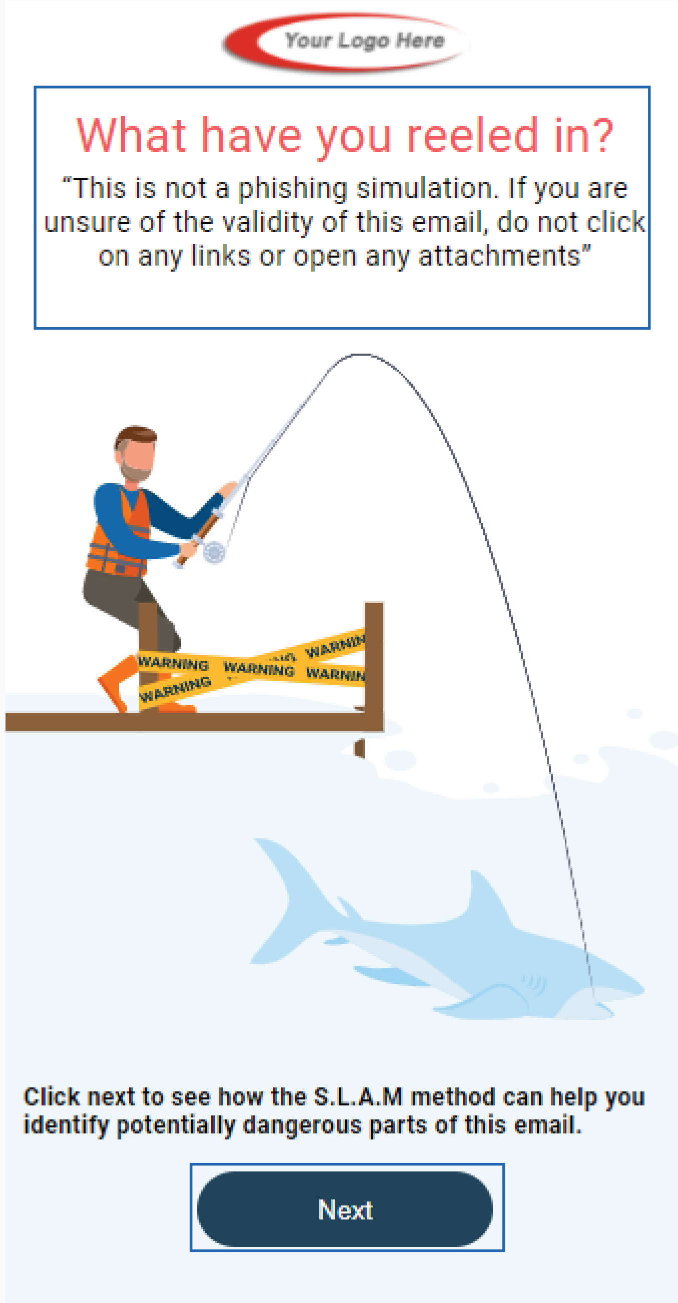
- **Email Analysis:** Users can click this button in their toolbar to leverage machine learning and artificial intelligence to confidently verify the legitimacy of any email that hits their inbox.
- **Security Training:** Users can access the weekly Micro Training videos and quizzes, re-watch any previous videos, or complete their Annual Trainings and quiz with the click of this button in their toolbar!

1. Education Corner. *The Learning Pyramid.* https://www.educationcorner.com/the-learning-pyramid.html

Feature Breakdown of the Catch Phish Outlook Plug-In

Instant access to tools that provide in-email education and support





What have you reeled in?

"This is not a phishing simulation. If you are unsure of the validity of this email, do not click on any links or open any attachments"

Click next to see how the S.L.A.M method can help you identify potentially dangerous parts of this email.

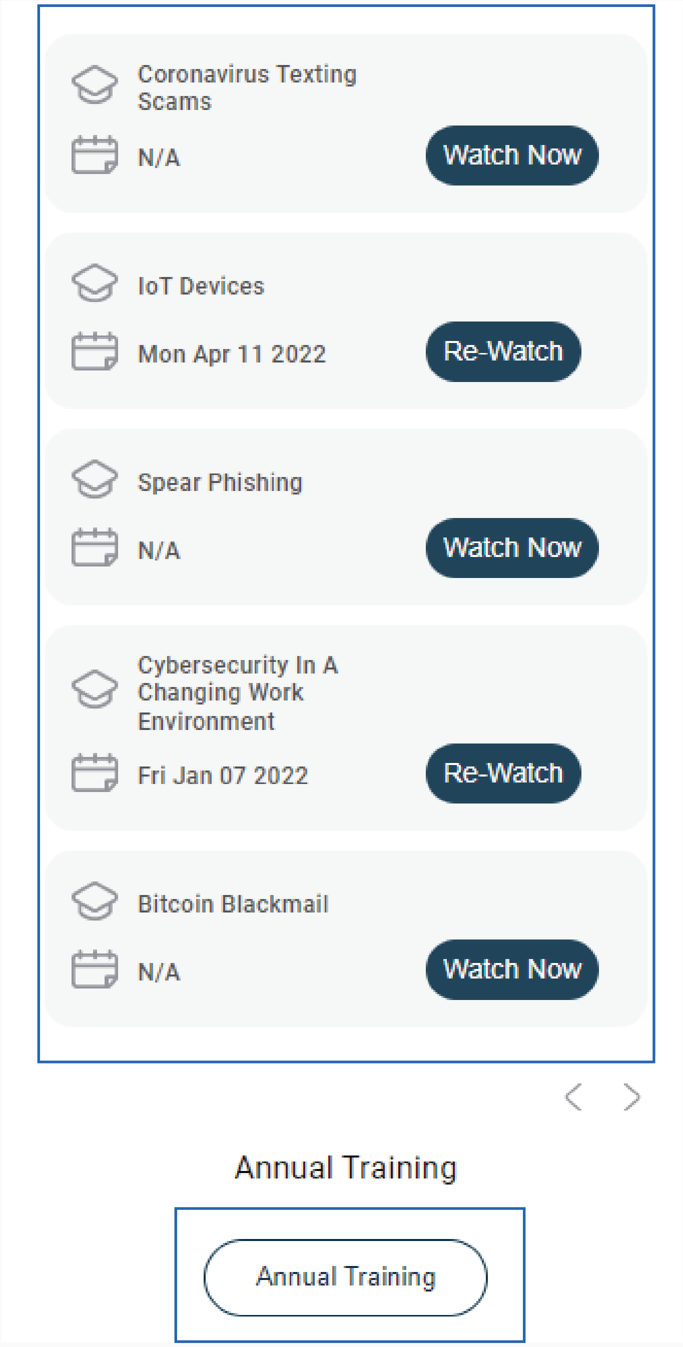
Next

Catch Phish Email Analysis

- If a user clicks the "Email Analysis" button on a phishing simulation email, they will be positively rewarded with confetti and can receive credit back on their ESS if they've previously failed a phishing simulation.
- If a user clicks the "Email Analysis" button on an email that is NOT a simulation, the screen will warn them that this is not a simulation (*see left screen*).
- Users can click the "**Next**" button to use machine learning and artificial intelligence to identify flagged elements such as sender details, links, language, and attachments, and get insight into the validity of the email.

Catch Phish Security Training

- If a user clicks the "Security Training" button, the screen on the right will appear, giving them access to all the Micro Training videos available for them to watch! That's right, users can access their ongoing training videos without logging into the portal and, without even leaving Outlook!
- Users can watch the Micro Training videos, take the quizzes, or re-watch any previously taken Micro-Training videos!
- NEW – The Annual Training classes are now available via the Catch Phish interface. Users can watch the full class and take the corresponding quiz.



Coronavirus Texting Scams
N/A
Watch Now

IoT Devices
Mon Apr 11 2022
Re-Watch

Spear Phishing
N/A
Watch Now

Cybersecurity In A Changing Work Environment
Fri Jan 07 2022
Re-Watch

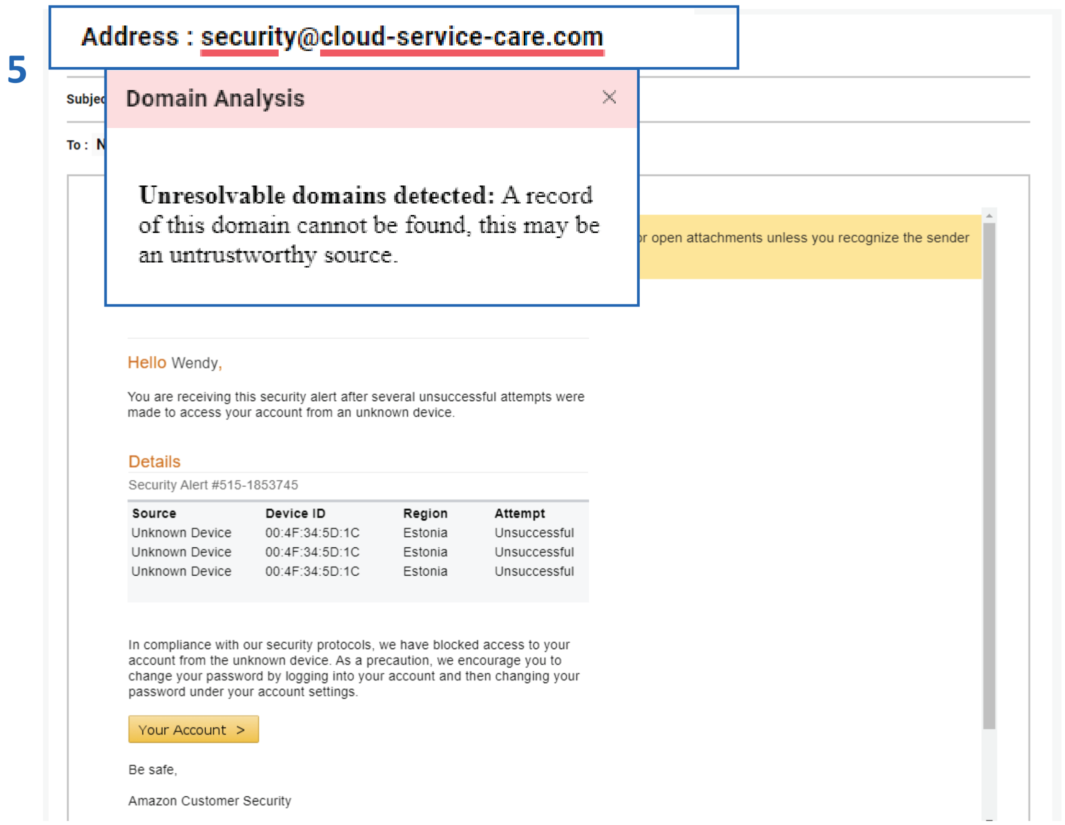
Bitcoin Blackmail
N/A
Watch Now

Annual Training

Annual Training

Feature Breakdown of the Catch Phish Outlook Plug-In

Understanding the “Email Analysis” feature inside Catch Phish



Address : security@cloud-service-care.com

Domain Analysis ×

Unresolvable domains detected: A record of this domain cannot be found, this may be an untrustworthy source.

r open attachments unless you recognize the sender

Hello Wendy,

You are receiving this security alert after several unsuccessful attempts were made to access your account from an unknown device.

Details

Security Alert #515-1853745

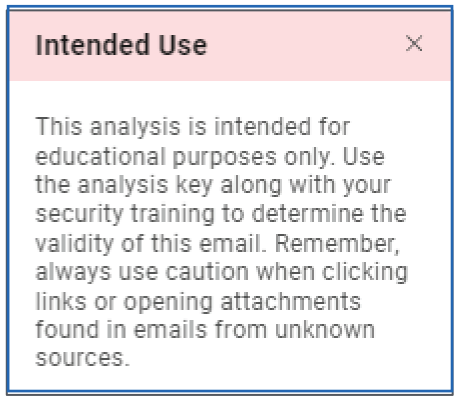
Source	Device ID	Region	Attempt
Unknown Device	00:4F:34:5D:1C	Estonia	Unsuccessful
Unknown Device	00:4F:34:5D:1C	Estonia	Unsuccessful
Unknown Device	00:4F:34:5D:1C	Estonia	Unsuccessful

In compliance with our security protocols, we have blocked access to your account from the unknown device. As a precaution, we encourage you to change your password by logging into your account and then changing your password under your account settings.

Your Account >

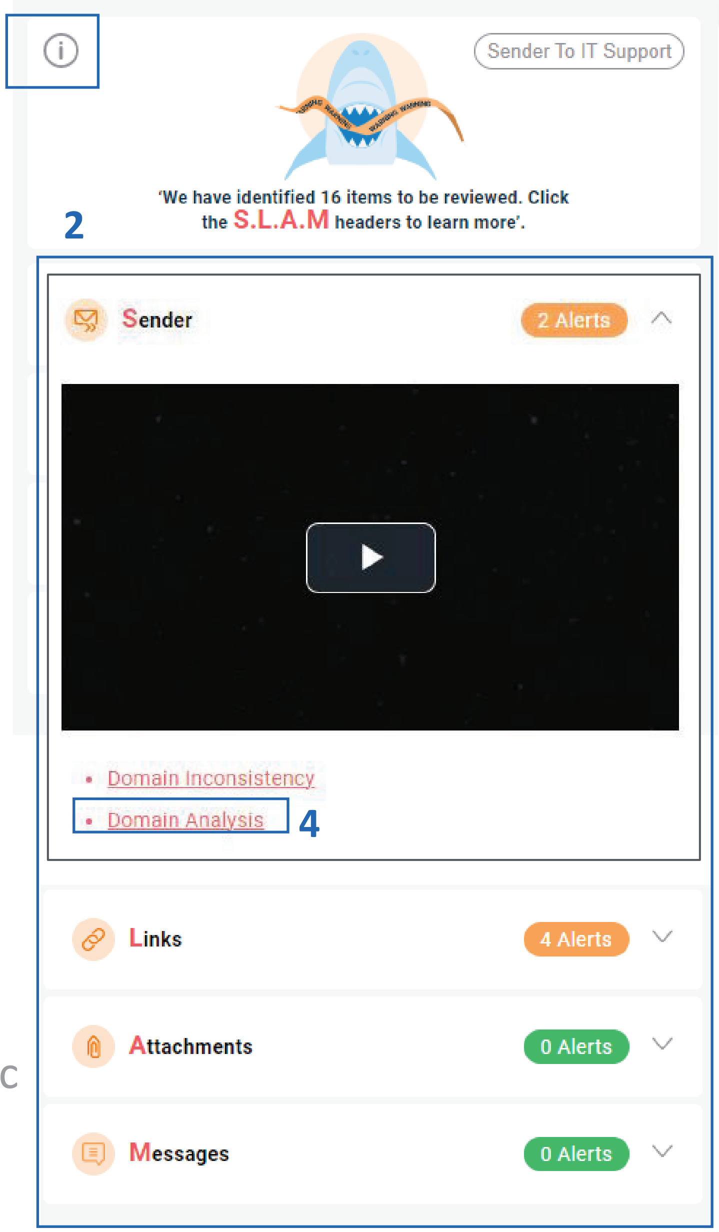
Be safe,

Amazon Customer Security



Intended Use ×

This analysis is intended for educational purposes only. Use the analysis key along with your security training to determine the validity of this email. Remember, always use caution when clicking links or opening attachments found in emails from unknown sources.



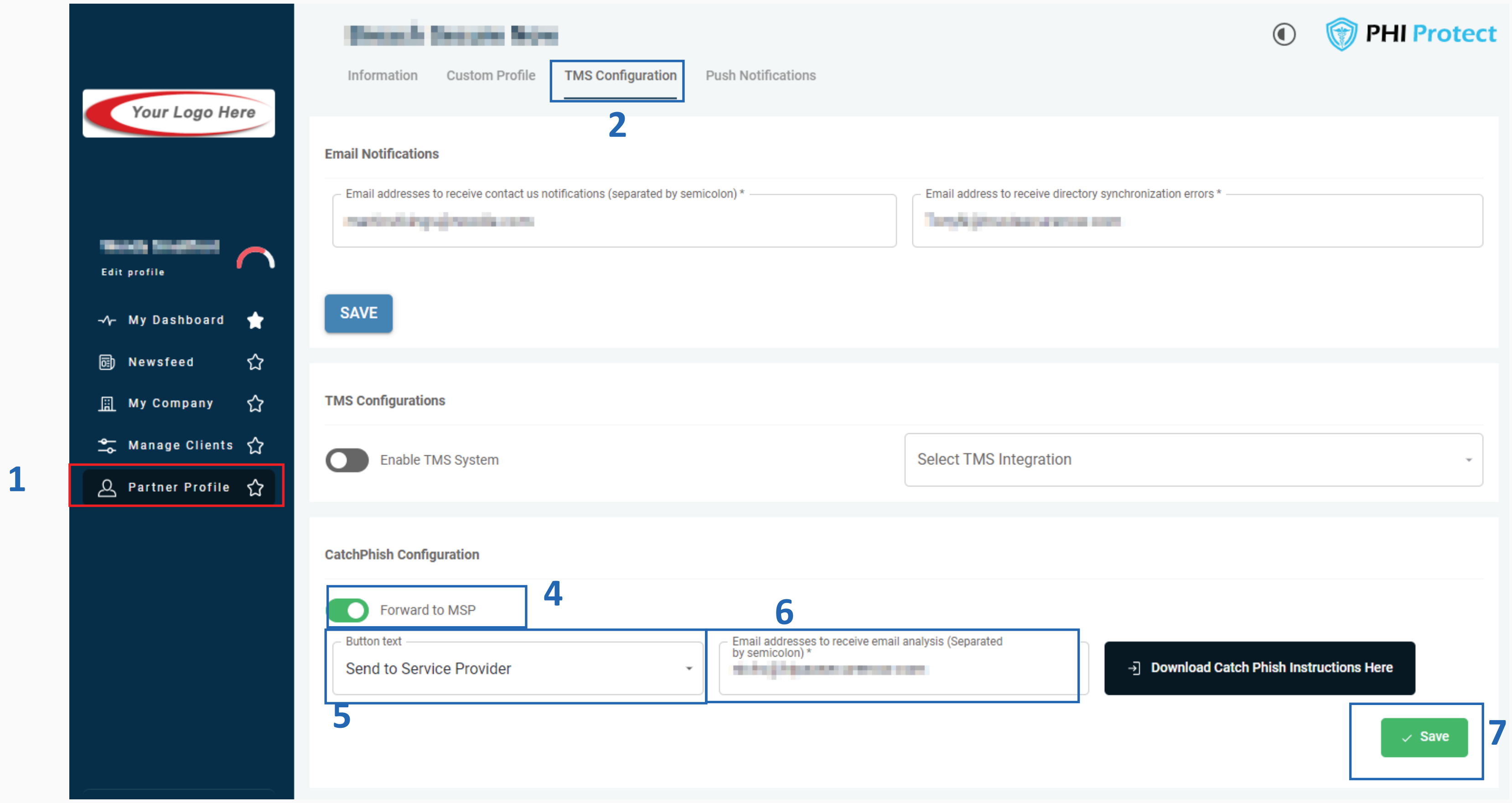
‘We have identified 16 items to be reviewed. Click the S.L.A.M headers to learn more’.

- Domain Inconsistency
- Domain Analysis

1. The “information” icon provides a disclaimer and helpful hints on how to use the Email Analysis feature
2. Initial analysis based on the SLAM method: Sender, Links, Attachments, Message
3. Expand each section to view flagged elements along with a training video on the topic
4. Further clicking on the flagged element will identify where the element was discovered in the email
5. Hover over the flagged element within the email for a detailed description of the potential issue

Catch Phish Analytics & Management – Global Level

Tools for Partner Administrators to analyze and customize their Catch Phish Outlook Plug-In



Email Notifications

Email addresses to receive contact us notifications (separated by semicolon) *: [redacted]

Email address to receive directory synchronization errors *: [redacted]

SAVE

TMS Configurations

Enable TMS System

Select TMS Integration

CatchPhish Configuration

Forward to MSP

Button text: Send to Service Provider

Email addresses to receive email analysis (Separated by semicolon) *: [redacted]

Download Catch Phish Instructions Here

✓ Save

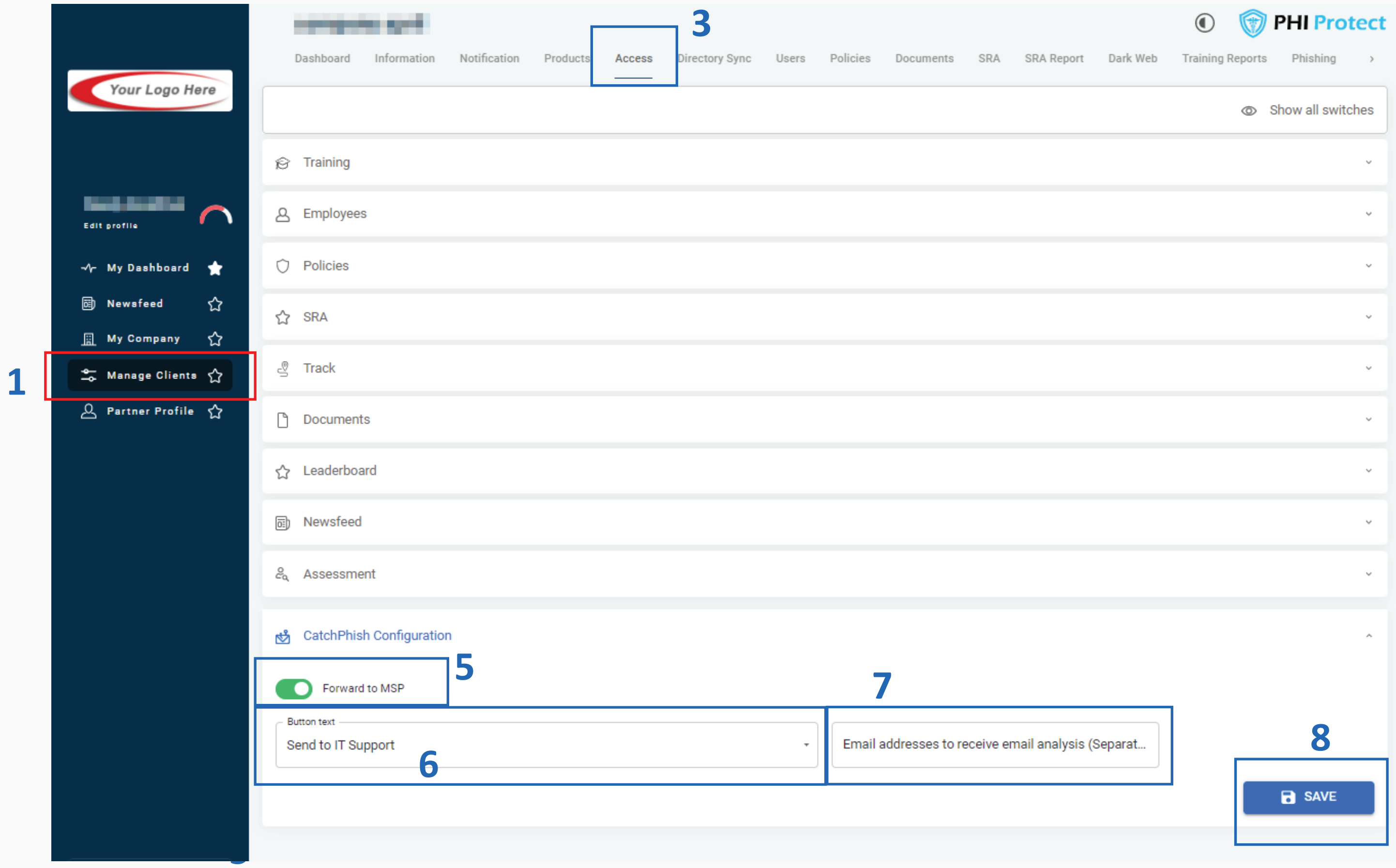
Global Catch Phish Configurations

Customize the Catch Phish Email Analysis tool settings for ALL your clients at the Global level. To customize specific settings for individual clients, see page 8 for steps.

1. Log into the portal with your Partner Administrator credentials, click “Partner Profile” on the left menu
2. Click on the “TMS Configuration” tab
3. Navigate to the Catch Phish Configuration section at the bottom of the page
4. **Forward To MSP** – provides users with the ability to forward their scanned message to the email account of your choosing
5. **Button Text** – Choose the desired button language to appear for your users
6. **Email notification** – provide the email address(es) that you would like this forwarded message to be sent to
7. Save changes when you are finished!

Catch Phish Analytics & Management – Client Level

Tools for Partner Administrators to analyze and customize their Catch Phish Outlook Plug-In



Forward to MSP

Button text: Send to IT Support

Email addresses to receive email analysis (Separat...

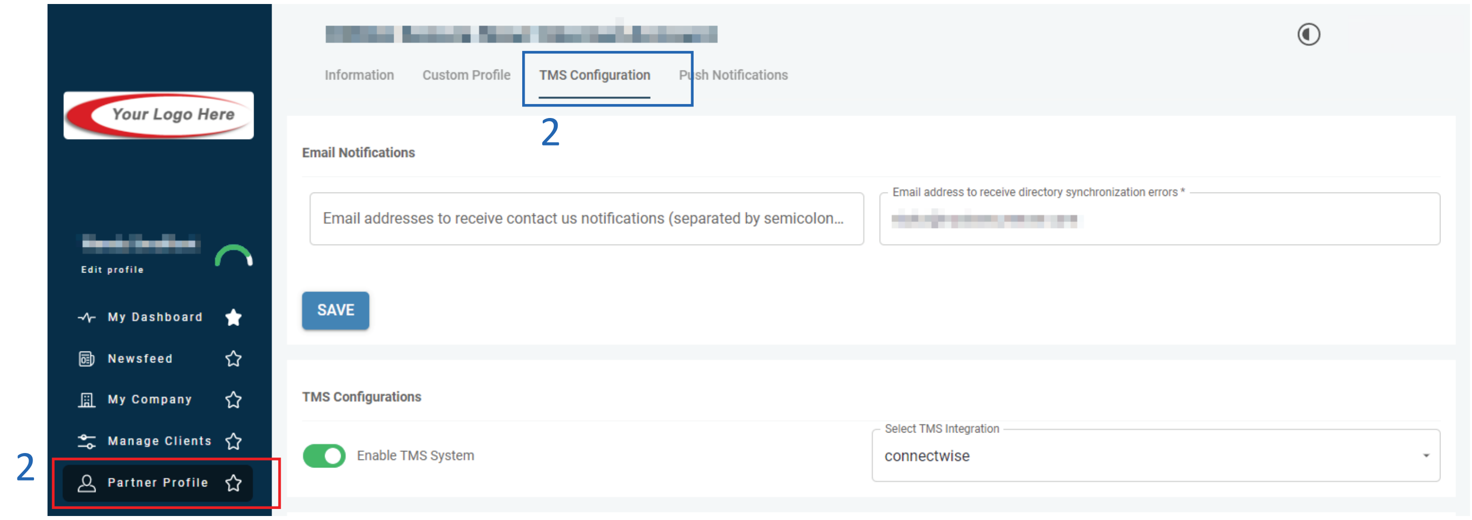
Client Level Catch Phish Configurations

Customize the Catch Phish tool for your individual clients. <u>These settings will override settings at the global level for the client</u>.

1. Log into the portal with your Partner Administrator credentials, click “Manage Clients” on the left menu
2. Click on the client you are looking to configure Catch Phish notifications for – Ensure they have the tool implemented first
3. Click on the “Access” tab
4. At the bottom of this section, you will see options for “CatchPhish Configuration”
5. **Forward To MSP** – provides users with the ability to forward their scanned message to the email account of your choosing
6. **Button Text** – Choose the desired button language to appear for your users
7. **Email notification** – provide the email address(es) that you would like this forwarded message to be sent to
8. Save changes when you are finished!

Catch Phish Email Forwarding Setup

Forward possible phishing emails to your PSA or desired email address



[redacted]

Information | Custom Profile | TMS Configuration | Push Notifications

2

Email Notifications

Email addresses to receive contact us notifications (separated by semicolon...

Email address to receive directory synchronization errors *: [redacted]

SAVE

TMS Configurations

Enable TMS System

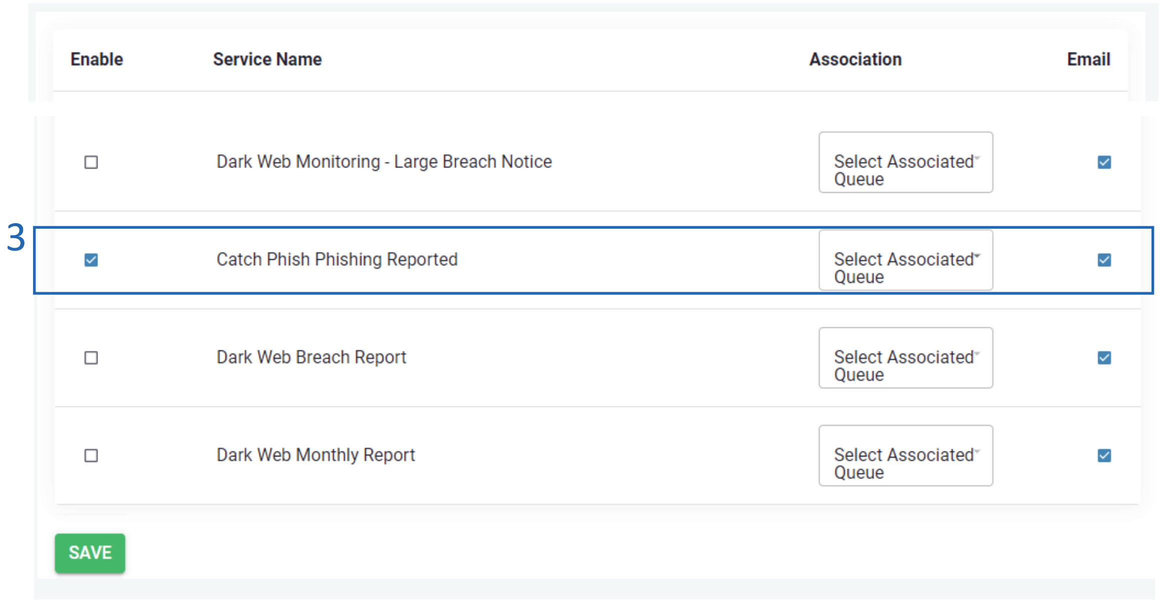
Select TMS Integration: connectwise

Need help setting up your PSA integration?

- Download the Autotask PSA setup guide here
- Download the ConnectWise PSA setup guide here

Configure the email forwarding settings inside the "PSA Configuration" screen inside the PII Protect Portal

1. Login as a Partner Administrator to the PII-Protect portal
2. Select the "**Partner Profile**" application on the left, then the "**TMS Configuration**" tab to be taken to your PSA and notification settings page.
3. Setup your email forwarding settings for Catch Phish:
   - If a PSA integration is setup, emails will be sent to the associated queue for "Catch Phish Phishing Reported"
   - If no PSA integration is setup, emails will be sent to the email entered under "Email address" section in the Catch Phish Configuration section (see page 7).



Enable	Service Name	Association	Email
☐	Dark Web Monitoring - Large Breach Notice	Select Associated Queue	☑
☑	Catch Phish Phishing Reported	Select Associated Queue	☑
☐	Dark Web Breach Report	Select Associated Queue	☑
☐	Dark Web Monthly Report	Select Associated Queue	☑

SAVE

Catch Phish Minimum Requirements

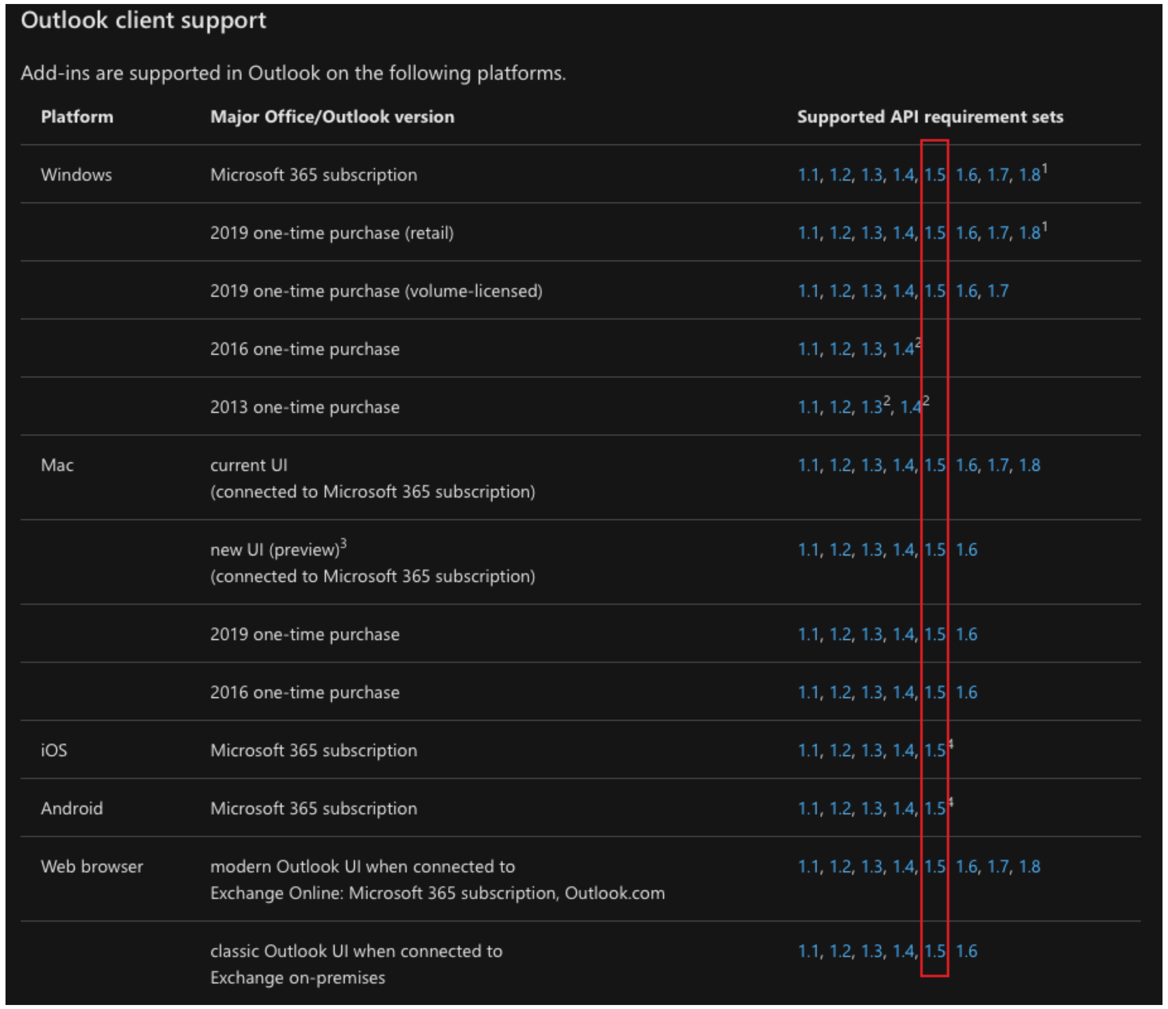
You and your clients must be on Office 365 with Centralized Deployment enabled

CHECK REQUIREMENTS

Catch Phish is available for Outlook web, mobile, and API version 1.5 and newer.

Deploying once will enable Catch Phish for all included users on all eligible applications.

Customer must have a paying subscription with our Employee Vulnerability Assessment (EVA).



Outlook client support

Add-ins are supported in Outlook on the following platforms.

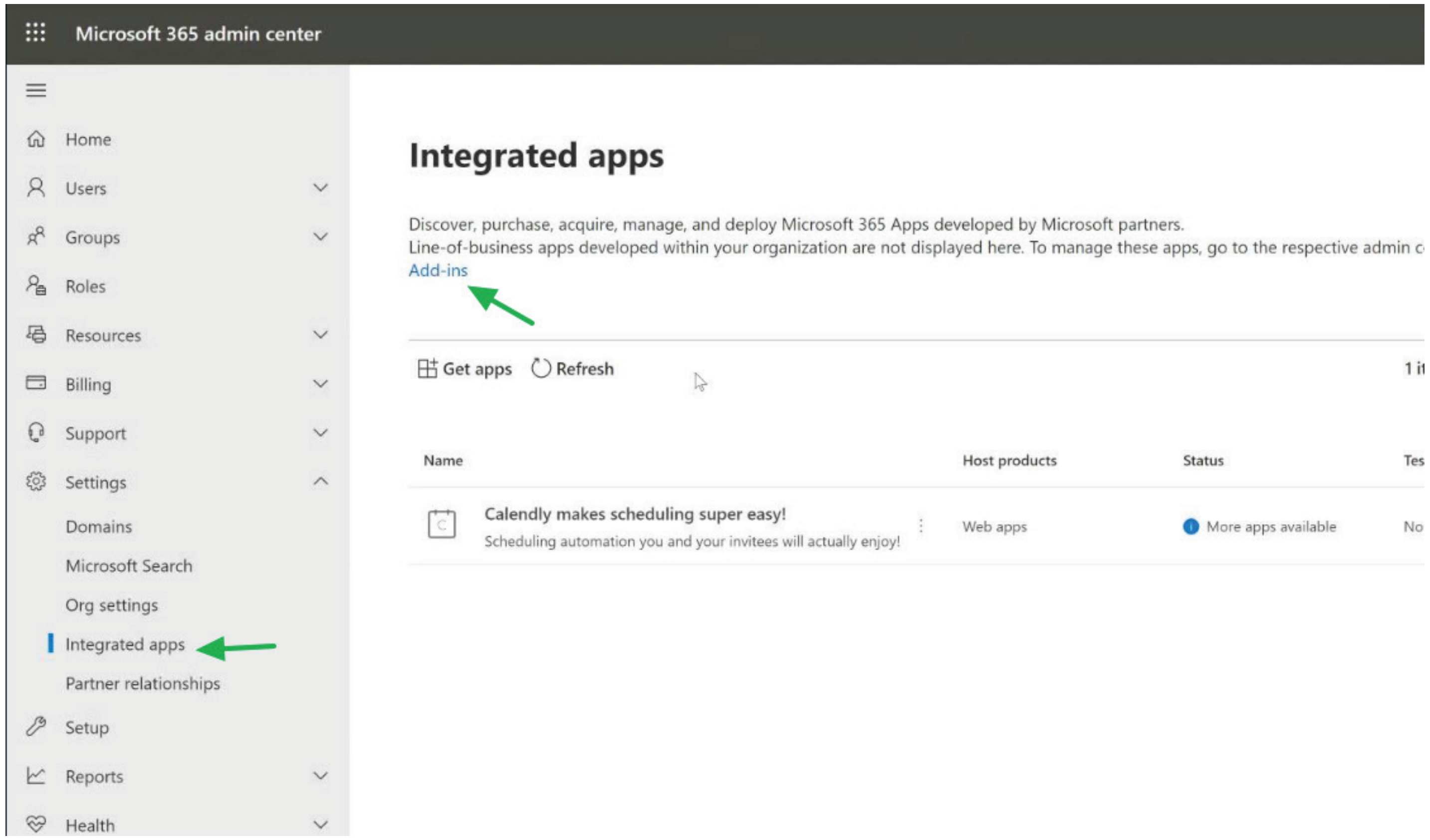
Platform	Major Office/Outlook version	Supported API requirement sets
Windows	Microsoft 365 subscription	1.1, 1.2, 1.3, 1.4, 1.5 1.6, 1.7, 1.8[1]
	2019 one-time purchase (retail)	1.1, 1.2, 1.3, 1.4, 1.5 1.6, 1.7, 1.8[1]
	2019 one-time purchase (volume-licensed)	1.1, 1.2, 1.3, 1.4, 1.5 1.6, 1.7
	2016 one-time purchase	1.1, 1.2, 1.3, 1.4[2]
	2013 one-time purchase	1.1, 1.2, 1.3[2], 1.4[2]
Mac	current UI (connected to Microsoft 365 subscription)	1.1, 1.2, 1.3, 1.4, 1.5 1.6, 1.7, 1.8
	new UI (preview)[3] (connected to Microsoft 365 subscription)	1.1, 1.2, 1.3, 1.4, 1.5 1.6
	2019 one-time purchase	1.1, 1.2, 1.3, 1.4, 1.5 1.6
	2016 one-time purchase	1.1, 1.2, 1.3, 1.4, 1.5 1.6
iOS	Microsoft 365 subscription	1.1, 1.2, 1.3, 1.4, 1.5[4]
Android	Microsoft 365 subscription	1.1, 1.2, 1.3, 1.4, 1.5[4]
Web browser	modern Outlook UI when connected to Exchange Online: Microsoft 365 subscription, Outlook.com	1.1, 1.2, 1.3, 1.4, 1.5 1.6, 1.7, 1.8
	classic Outlook UI when connected to Exchange on-premises	1.1, 1.2, 1.3, 1.4, 1.5 1.6

Deploying the Catch Phish Outlook Plug-In

LOGIN TO THE MICROSOFT O365 ADMIN CENTER

Navigate to Settings → Integrated apps and click the **"Add-In"** link at the top of the screen

You can also use the following URL to navigate directly there https://admin.microsoft.com/AdminPortal/Home#/Settings/AddIns



Integrated apps

Discover, purchase, acquire, manage, and deploy Microsoft 365 Apps developed by Microsoft partners.
Line-of-business apps developed within your organization are not displayed here. To manage these apps, go to the respective admin c
Add-ins

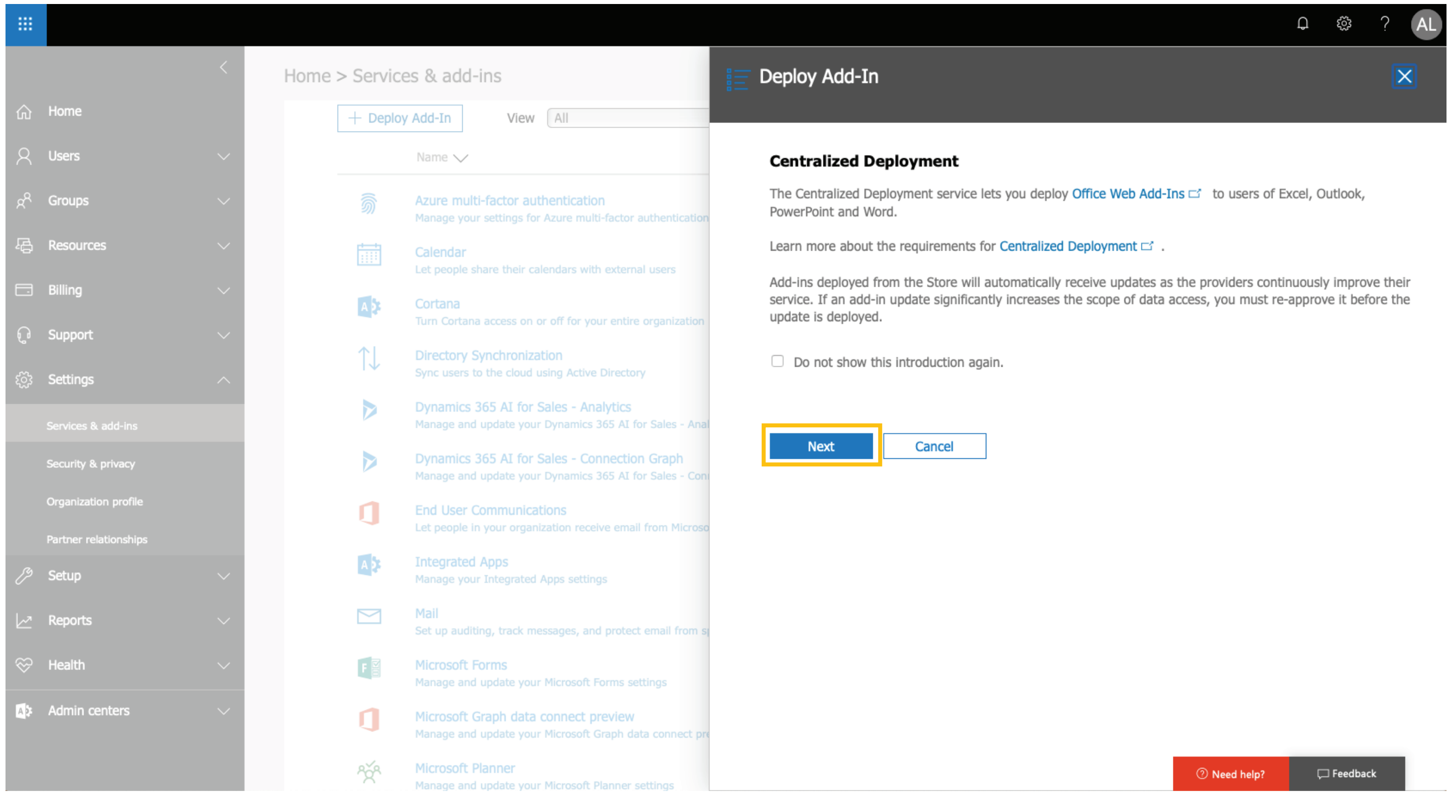
Name	Host products	Status	Tes
Calendly makes scheduling super easy! Scheduling automation you and your invitees will actually enjoy!	Web apps	● More apps available	No

Deploying the Catch Phish Outlook Plug-In

CONFIGURE THE DEPLOYMENT SETTINGS

Click **“Deploy Add-in”**

Review the overview for Centralized Deployment and hit: **“Next”**



Deploy Add-In

Centralized Deployment

The Centralized Deployment service lets you deploy Office Web Add-Ins to users of Excel, Outlook, PowerPoint and Word.

Learn more about the requirements for Centralized Deployment .

Add-ins deployed from the Store will automatically receive updates as the providers continuously improve their service. If an add-in update significantly increases the scope of data access, you must re-approve it before the update is deployed.

☐ Do not show this introduction again.

AL
Home
Users
Groups
Resources
Billing
Support
Settings
Services & add-ins
Security & privacy
Organization profile
Partner relationships
Setup
Reports
Health
Admin centers
Home > Services & add-ins
Deploy Add-In
View
All
Name
Azure multi-factor authentication
Manage your settings for Azure multi-factor authentication
Calendar
Let people share their calendars with external users
Cortana
Turn Cortana access on or off for your entire organization
Directory Synchronization
Sync users to the cloud using Active Directory
Dynamics 365 AI for Sales - Analytics
Manage and update your Dynamics 365 AI for Sales - Anal
Dynamics 365 AI for Sales - Connection Graph
Manage and update your Dynamics 365 AI for Sales - Con
End User Communications
Let people in your organization receive email from Microso
Integrated Apps
Manage your Integrated Apps settings
Mail
Set up auditing, track messages, and protect email from s
Microsoft Forms
Manage and update your Microsoft Forms settings
Microsoft Graph data connect preview
Manage and update your Microsoft Graph data connect pr
Microsoft Planner
Manage and update your Microsoft Planner settings
Next
Cancel
Need help?
Feedback

Deploying the Catch Phish Outlook Plug-In

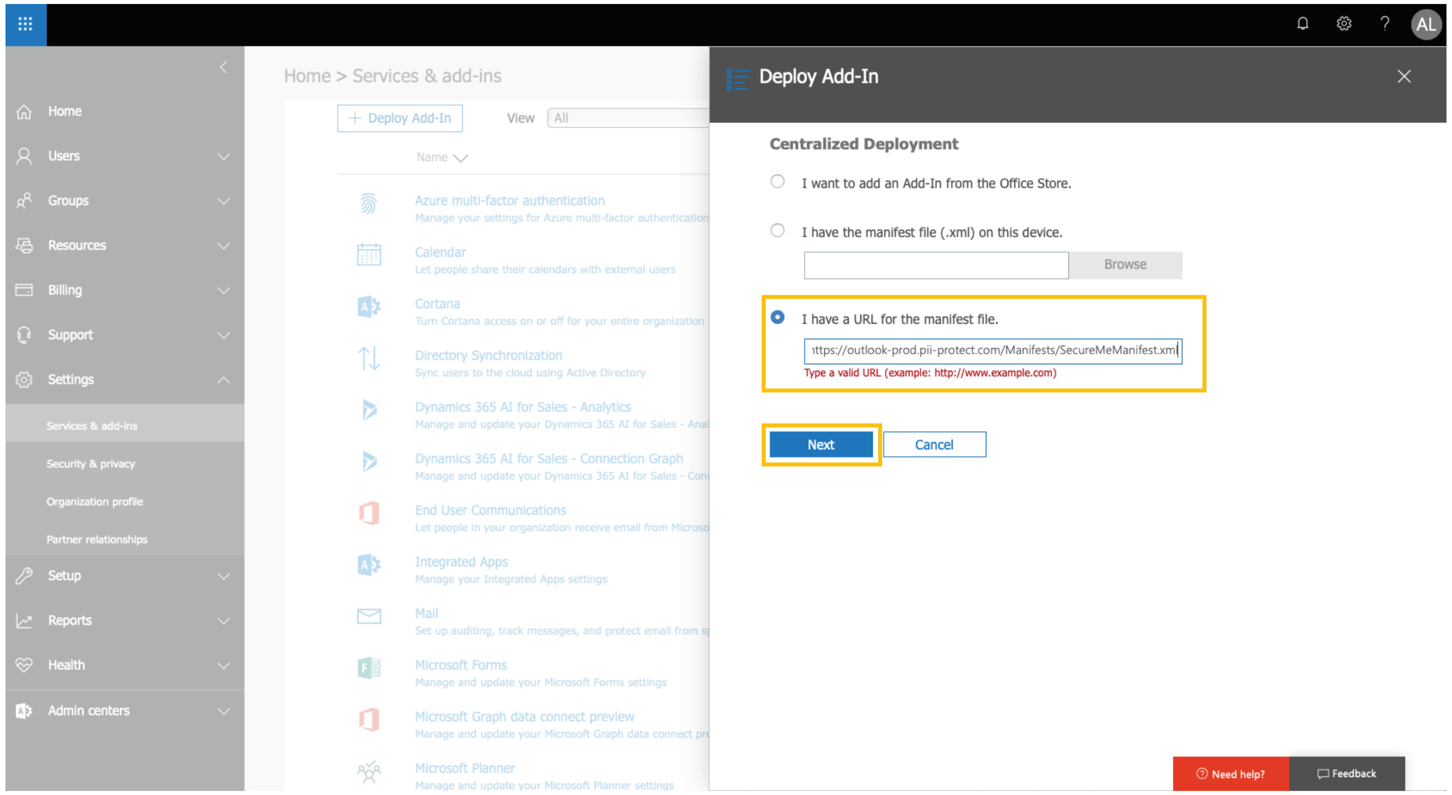
SELECT THE URL OPTION FOR THE MANIFEST FILE

Paste the URL for the manifest file inside the textbox:

https://catchphish.email/SecureMeManifest.xml

Note: https:// must be in the URL even if https:// is already displayed in grey on the left-hand side

Then hit **"Next"** to continue



Deploy Add-In

Centralized Deployment

○ I want to add an Add-In from the Office Store.

○ I have the manifest file (.xml) on this device.

Browse

● I have a URL for the manifest file.

ıttps://outlook-prod.pii-protect.com/Manifests/SecureMeManifest.xml

Type a valid URL (example: http://www.example.com)

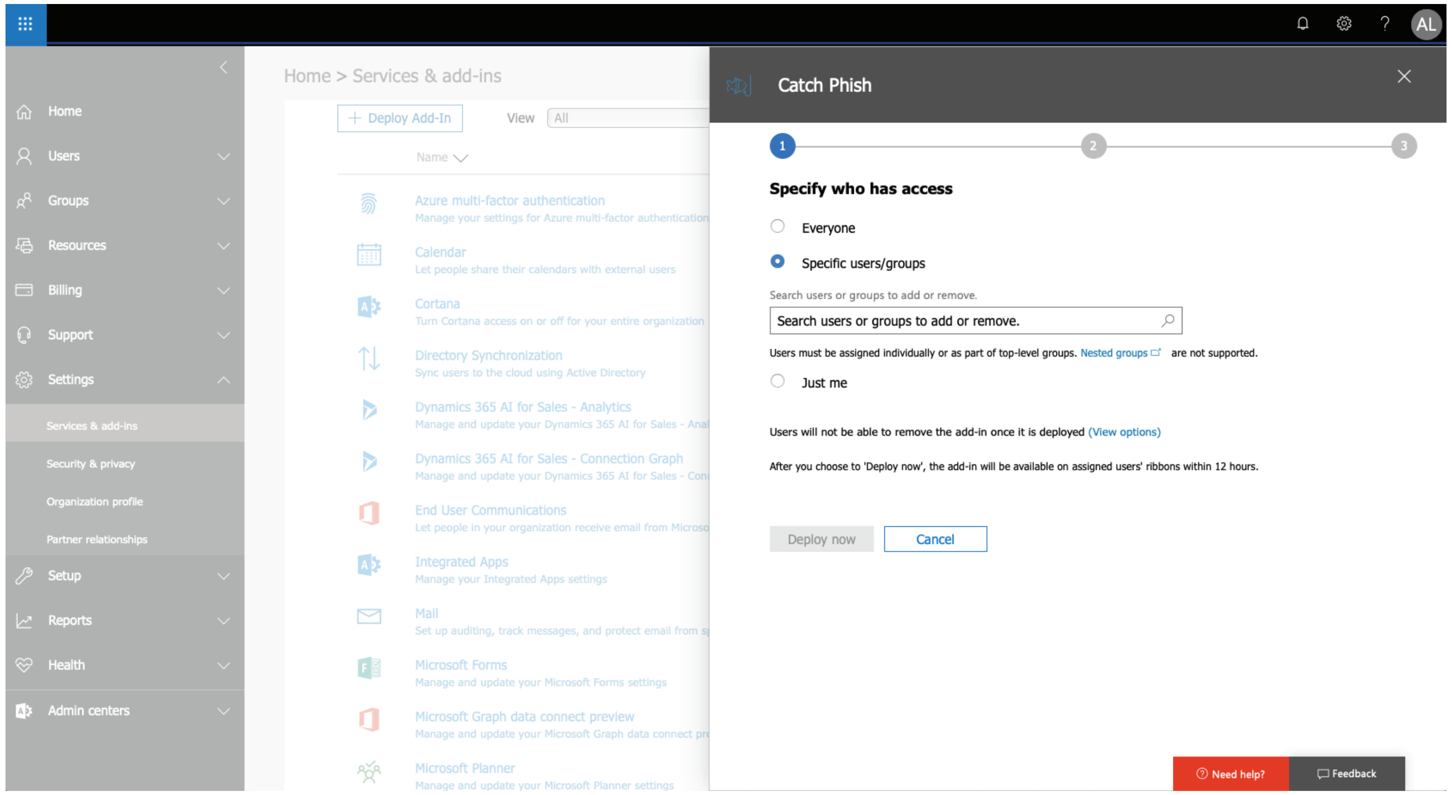
Next

Cancel

Deploying the Catch Phish Outlook Plug-In

SPECIFY ACCESS TO THE EMAIL ANALYSIS TOOL

Configure access to the Catch Phish Outlook Plug-In. You can choose to deploy to all users, or to specific users/groups



Azure multi-factor authentication
Manage your settings for Azure multi-factor authentication

Calendar
Let people share their calendars with external users

Cortana
Turn Cortana access on or off for your entire organization

Directory Synchronization
Sync users to the cloud using Active Directory

Dynamics 365 AI for Sales - Analytics
Manage and update your Dynamics 365 AI for Sales - Anal

Dynamics 365 AI for Sales - Connection Graph
Manage and update your Dynamics 365 AI for Sales - Con

End User Communications
Let people in your organization receive email from Microso

Integrated Apps
Manage your Integrated Apps settings

Mail
Set up auditing, track messages, and protect email from s

Microsoft Forms
Manage and update your Microsoft Forms settings

Microsoft Graph data connect preview
Manage and update your Microsoft Graph data connect pr

Microsoft Planner
Manage and update your Microsoft Planner settings

Catch Phish

1 — 2 — 3

Specify who has access

○ Everyone

● Specific users/groups

Search users or groups to add or remove.

Search users or groups to add or remove.

Users must be assigned individually or as part of top-level groups. Nested groups are not supported.

○ Just me

Users will not be able to remove the add-in once it is deployed (View options)

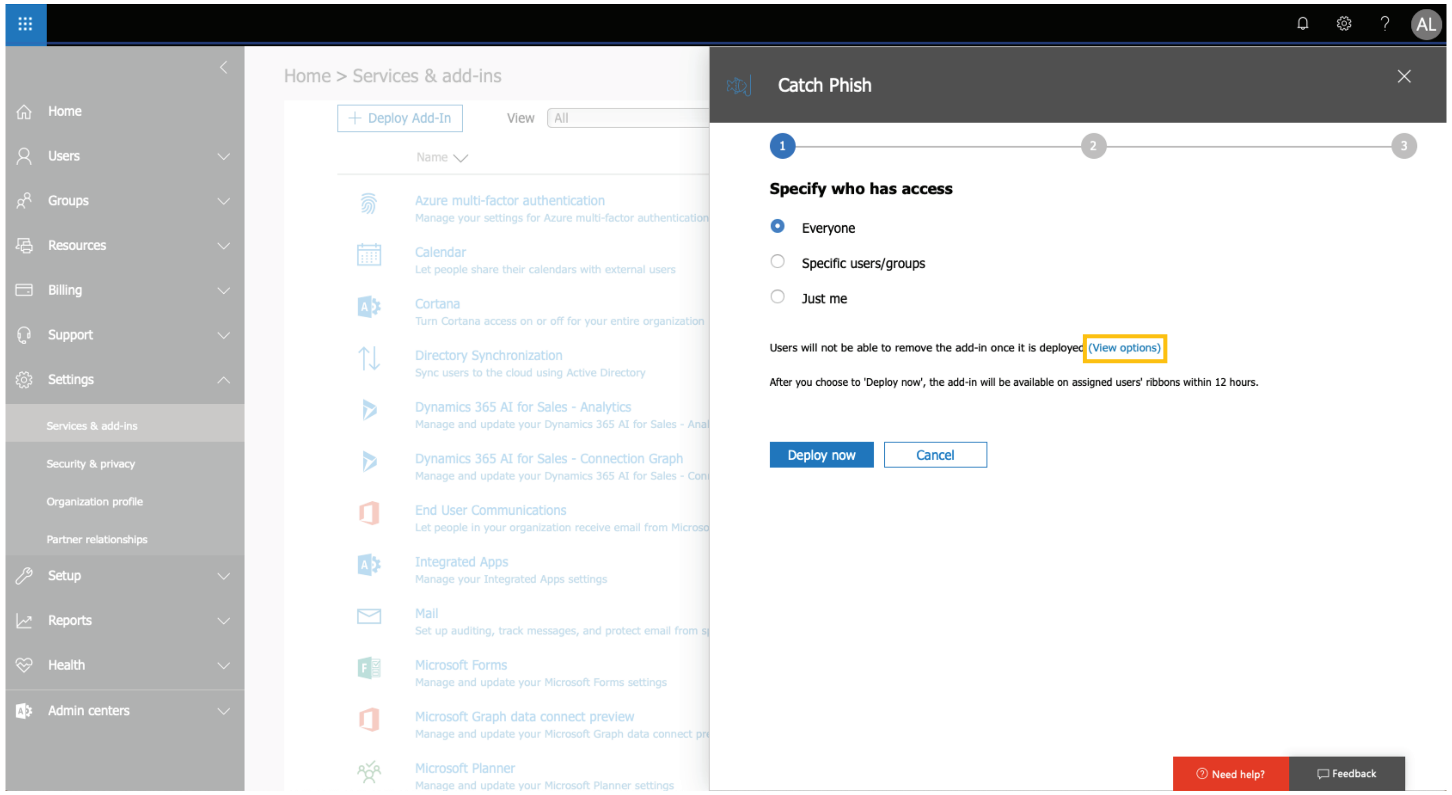
After you choose to 'Deploy now', the add-in will be available on assigned users' ribbons within 12 hours.

Deploy now | Cancel

Deploying the Catch Phish Outlook Plug-In

EDIT THE DEPLOYMENT METHOD

Edit the deployment settings by clicking **"View Options"**


AL
Home
Users
Groups
Resources
Billing
Support
Settings
Services & add-ins
Security & privacy
Organization profile
Partner relationships
Setup
Reports
Health
Admin centers
Home > Services & add-ins
+ Deploy Add-In
View
All
Name
Azure multi-factor authentication
Manage your settings for Azure multi-factor authentication
Calendar
Let people share their calendars with external users
Cortana
Turn Cortana access on or off for your entire organization
Directory Synchronization
Sync users to the cloud using Active Directory
Dynamics 365 AI for Sales - Analytics
Manage and update your Dynamics 365 AI for Sales - Anal
Dynamics 365 AI for Sales - Connection Graph
Manage and update your Dynamics 365 AI for Sales - Con
End User Communications
Let people in your organization receive email from Microso
Integrated Apps
Manage your Integrated Apps settings
Mail
Set up auditing, track messages, and protect email from s
Microsoft Forms
Manage and update your Microsoft Forms settings
Microsoft Graph data connect preview
Manage and update your Microsoft Graph data connect pr
Microsoft Planner
Manage and update your Microsoft Planner settings
Need help?
Feedback

Catch Phish

1 2 3

Specify who has access

● Everyone

○ Specific users/groups

○ Just me

Users will not be able to remove the add-in once it is deployed (View options)

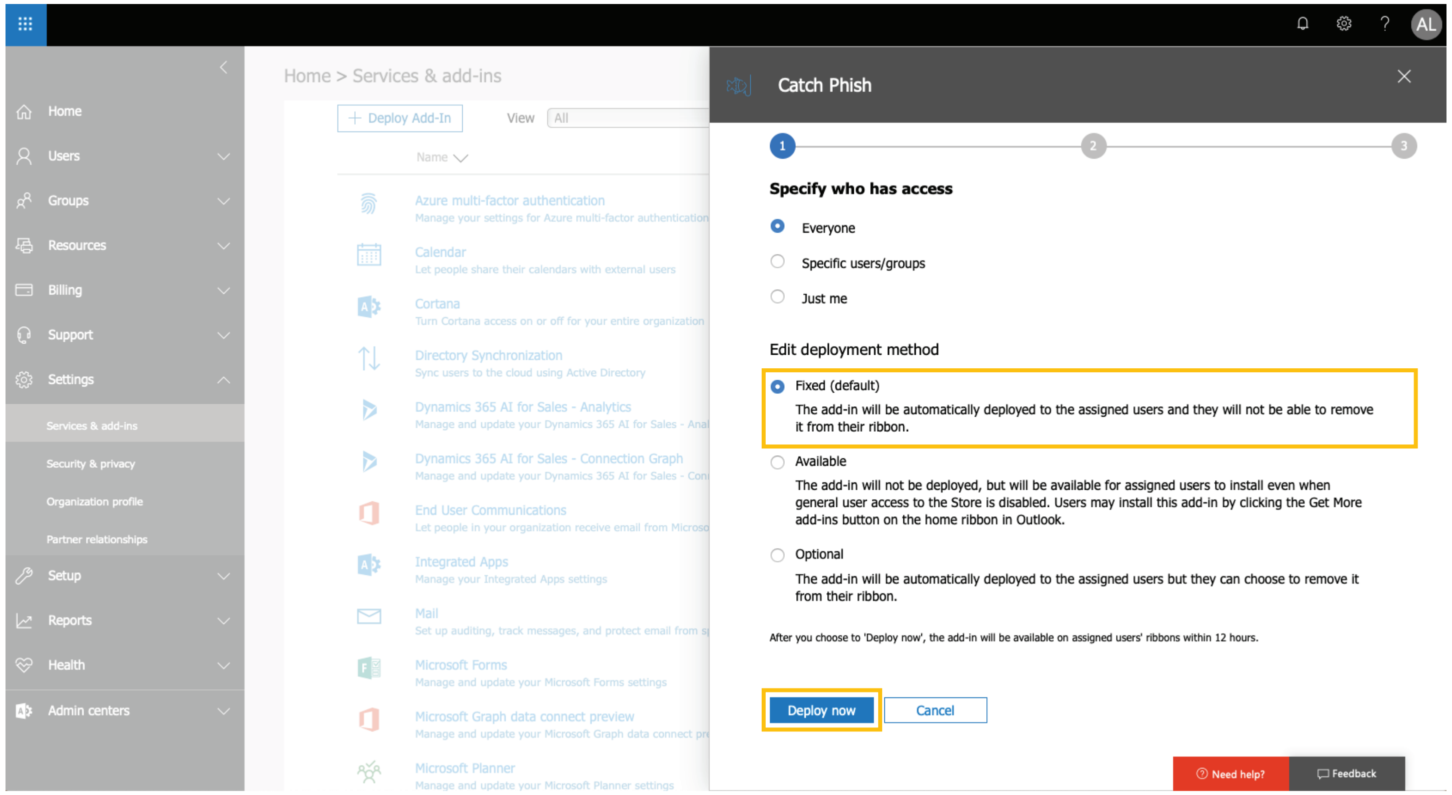
After you choose to 'Deploy now', the add-in will be available on assigned users' ribbons within 12 hours.

Deploy now | Cancel

Deploying the Catch Phish Outlook Plug-In

EDIT THE DEPLOYMENT METHOD

Ensure the **"Fixed (default)"** option is selected. Click the **"Deploy now"** button to deploy the Catch Phish Email Analysis Tool to all desired users



Azure multi-factor authentication
Manage your settings for Azure multi-factor authentication

Calendar
Let people share their calendars with external users

Cortana
Turn Cortana access on or off for your entire organization

Directory Synchronization
Sync users to the cloud using Active Directory

Dynamics 365 AI for Sales - Analytics
Manage and update your Dynamics 365 AI for Sales - Anal

Dynamics 365 AI for Sales - Connection Graph
Manage and update your Dynamics 365 AI for Sales - Con

End User Communications
Let people in your organization receive email from Microso

Integrated Apps
Manage your Integrated Apps settings

Mail
Set up auditing, track messages, and protect email from s

Microsoft Forms
Manage and update your Microsoft Forms settings

Microsoft Graph data connect preview
Manage and update your Microsoft Graph data connect pr

Microsoft Planner
Manage and update your Microsoft Planner settings

Specify who has access

● Everyone

○ Specific users/groups

○ Just me

Edit deployment method

● Fixed (default)
The add-in will be automatically deployed to the assigned users and they will not be able to remove it from their ribbon.

○ Available
The add-in will not be deployed, but will be available for assigned users to install even when general user access to the Store is disabled. Users may install this add-in by clicking the Get More add-ins button on the home ribbon in Outlook.

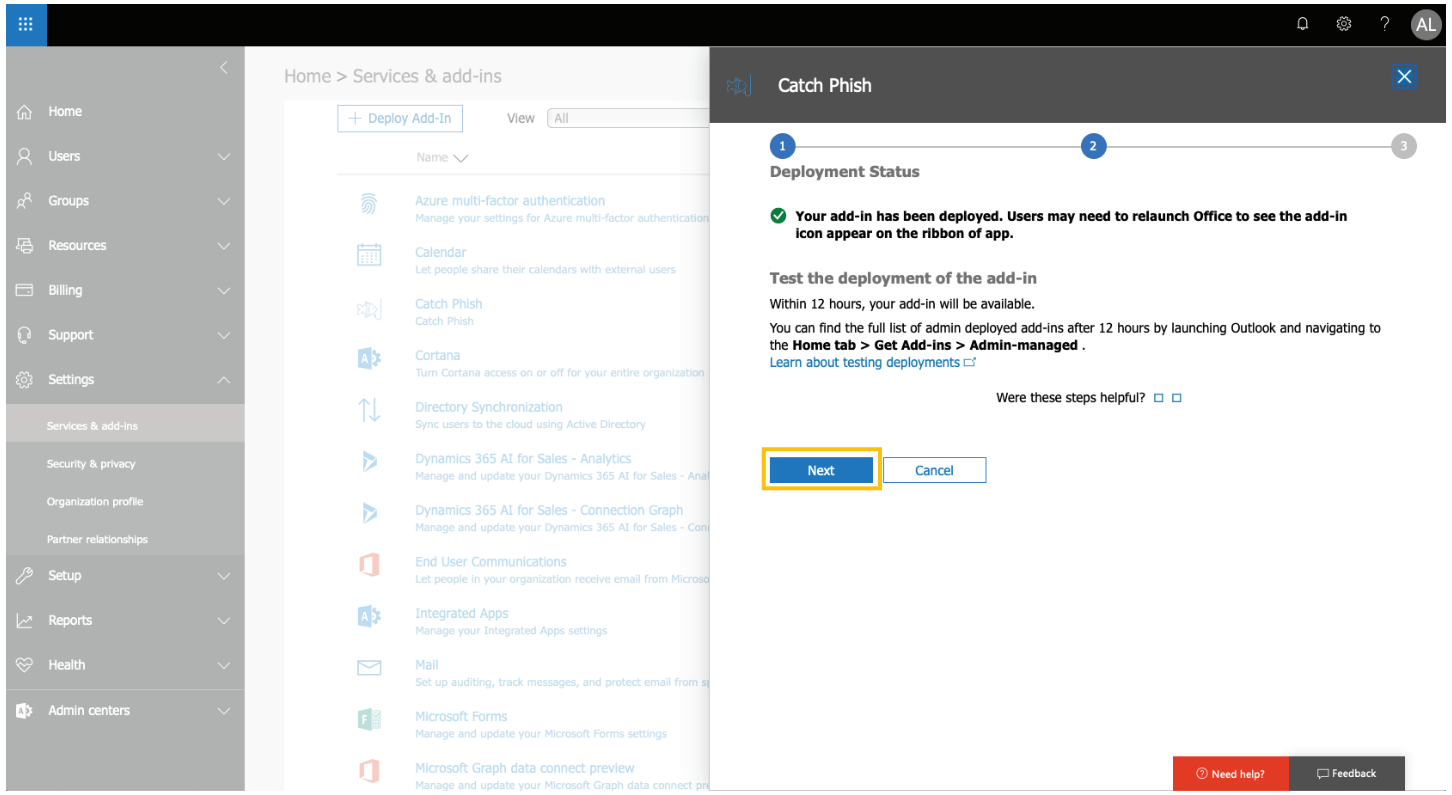
○ Optional
The add-in will be automatically deployed to the assigned users but they can choose to remove it from their ribbon.

After you choose to 'Deploy now', the add-in will be available on assigned users' ribbons within 12 hours.

Deploying the Catch Phish Outlook Plug-In

REVIEW YOUR DEPLOYMENT STATUS

Click the **“Next”** button after reviewing the delay notice



Azure multi-factor authentication
Manage your settings for Azure multi-factor authentication

Calendar
Let people share their calendars with external users

Catch Phish
Catch Phish

Cortana
Turn Cortana access on or off for your entire organization

Directory Synchronization
Sync users to the cloud using Active Directory

Dynamics 365 AI for Sales - Analytics
Manage and update your Dynamics 365 AI for Sales - Anal

Dynamics 365 AI for Sales - Connection Graph
Manage and update your Dynamics 365 AI for Sales - Con

End User Communications
Let people in your organization receive email from Microso

Integrated Apps
Manage your Integrated Apps settings

Mail
Set up auditing, track messages, and protect email from s

Microsoft Forms
Manage and update your Microsoft Forms settings

Microsoft Graph data connect preview
Manage and update your Microsoft Graph data connect pr

Catch Phish

1 — 2 — 3

Deployment Status

✓ **Your add-in has been deployed. Users may need to relaunch Office to see the add-in icon appear on the ribbon of app.**

Test the deployment of the add-in

Within 12 hours, your add-in will be available.

You can find the full list of admin deployed add-ins after 12 hours by launching Outlook and navigating to the **Home tab > Get Add-ins > Admin-managed** .

Learn about testing deployments

Were these steps helpful? □ □

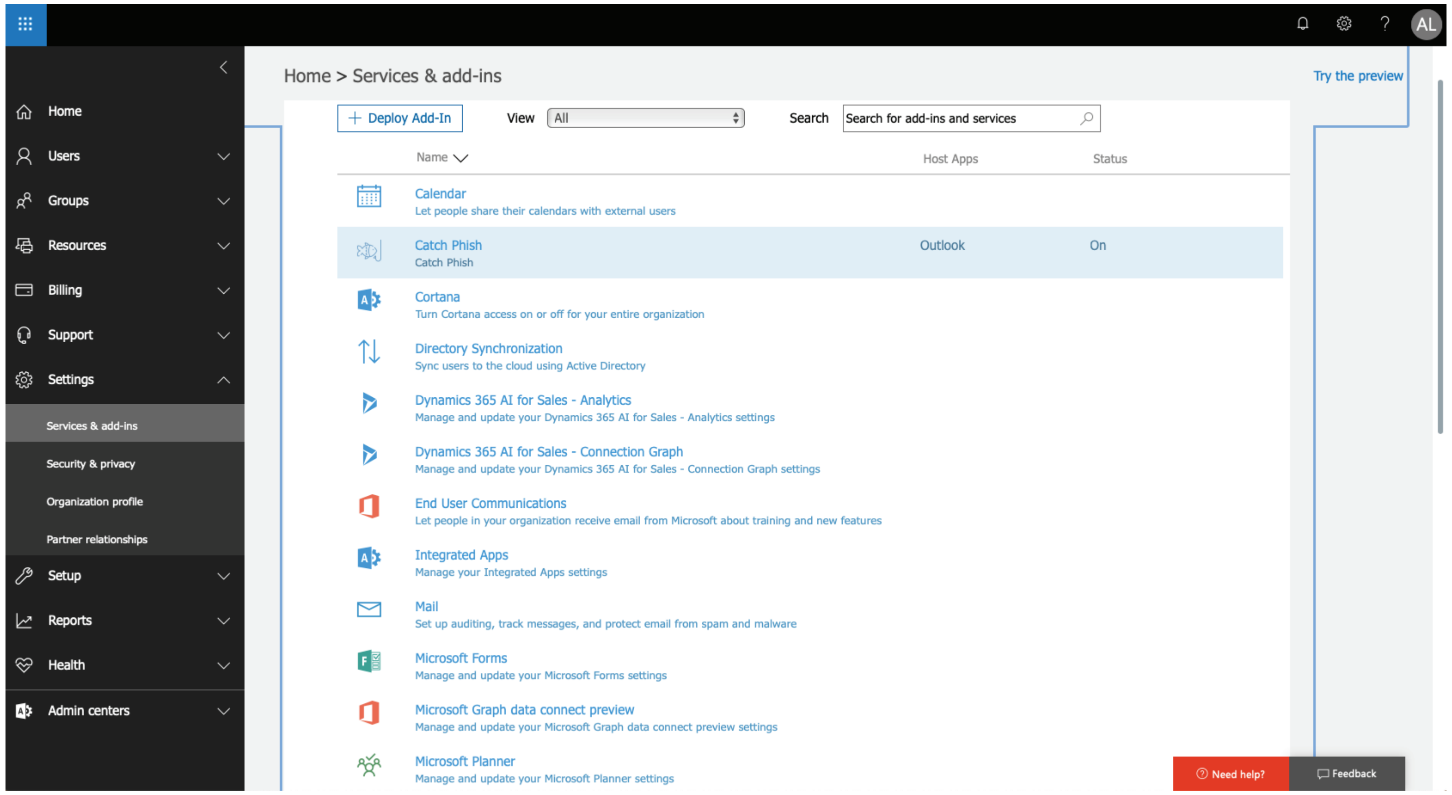
Next | Cancel

Deploying the Catch Phish Outlook Plug-In

NAVIGATE TO THE SERVICES & ADD-INS DASHBOARD

Confirm the Catch Phish Email Analysis Tool is accurate:

- ✓ Host Apps: **Outlook**
- ✓ Status: **On**



Name	Host Apps	Status
Calendar Let people share their calendars with external users		
Catch Phish Catch Phish	Outlook	On
Cortana Turn Cortana access on or off for your entire organization		
Directory Synchronization Sync users to the cloud using Active Directory		
Dynamics 365 AI for Sales - Analytics Manage and update your Dynamics 365 AI for Sales - Analytics settings		
Dynamics 365 AI for Sales - Connection Graph Manage and update your Dynamics 365 AI for Sales - Connection Graph settings		
End User Communications Let people in your organization receive email from Microsoft about training and new features		
Integrated Apps Manage your Integrated Apps settings		
Mail Set up auditing, track messages, and protect email from spam and malware		
Microsoft Forms Manage and update your Microsoft Forms settings		
Microsoft Graph data connect preview Manage and update your Microsoft Graph data connect preview settings		
Microsoft Planner Manage and update your Microsoft Planner settings		

You’re All Set!

You’ve successfully deployed the Catch Phish Outlook Plug-In! Repeat deployment steps for each customer you’d like to roll-out this advanced training tool to!

Telesystem®
IT’s About Trust®

#HackersSuck

www.TrustTelesystem.com