Security Awareness Training
Catch Phish Plug-In

What is the Catch Phish Outlook Plug-In?

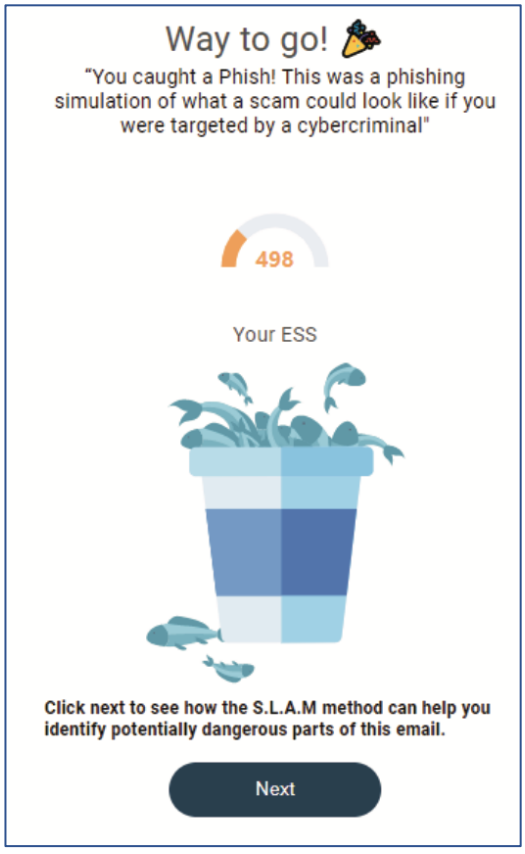
Advanced email analysis and access to security training with the click of a button.

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.



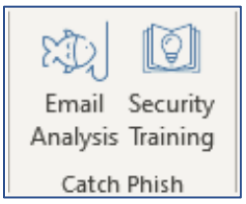
The Basics of the Catch Phish Outlook Plug-In

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!

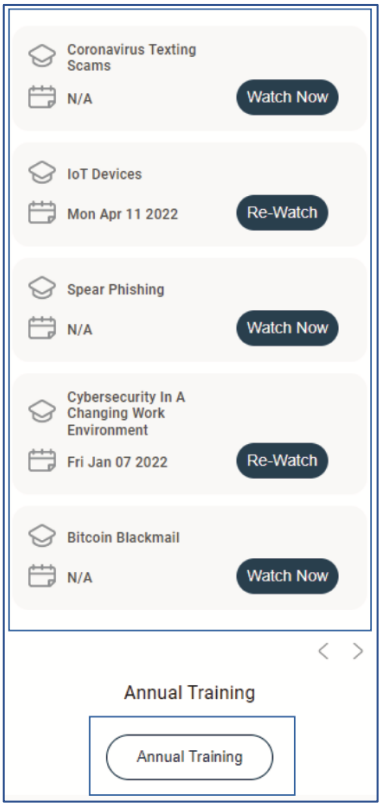
Feature Breakdown of the Catch Phish Outlook Plug-In

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



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.
    - Users can click the **"Next"** button to user 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.

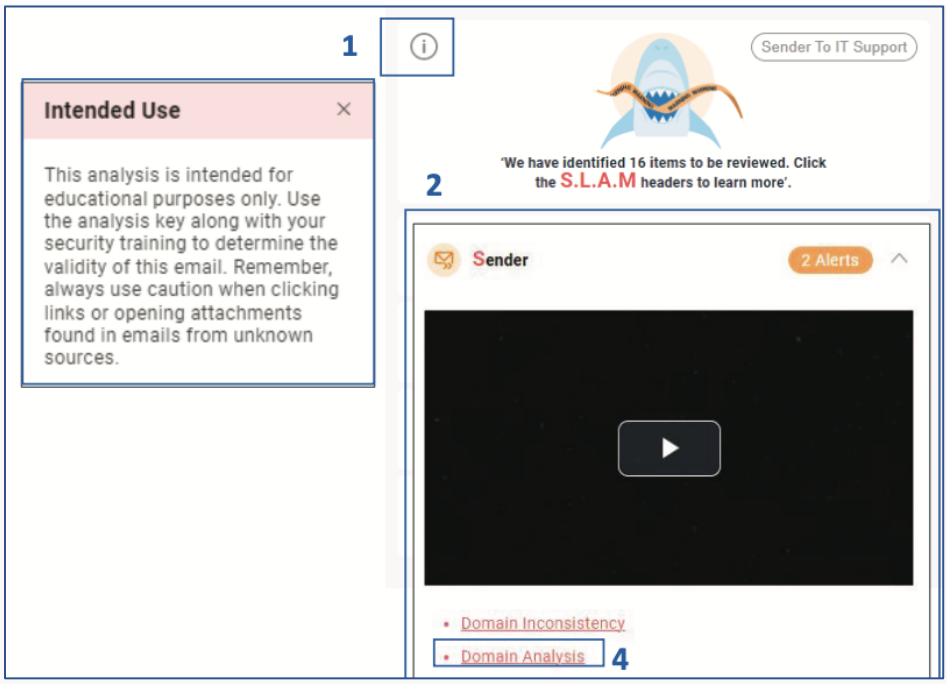


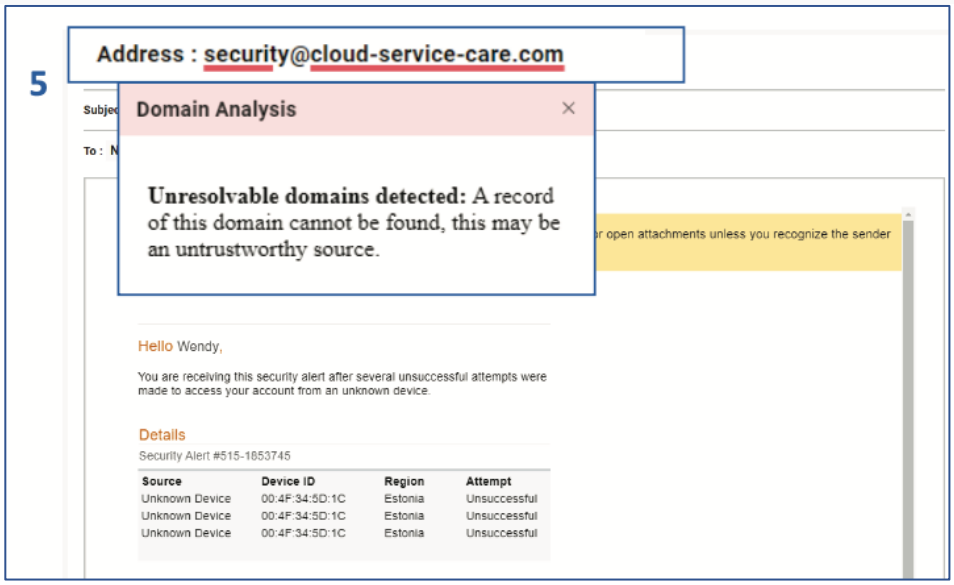
Catch Phish Security Training

- If a user clicks the "Security Training" button, the screen will pop-up 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!
- The Annual Training classes are now available via the Catch Phish interface. Users can watch the full class and take the corresponding quiz.

Understanding the “Email Analysis” feature inside Catch Phish

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 Minimum Requirements

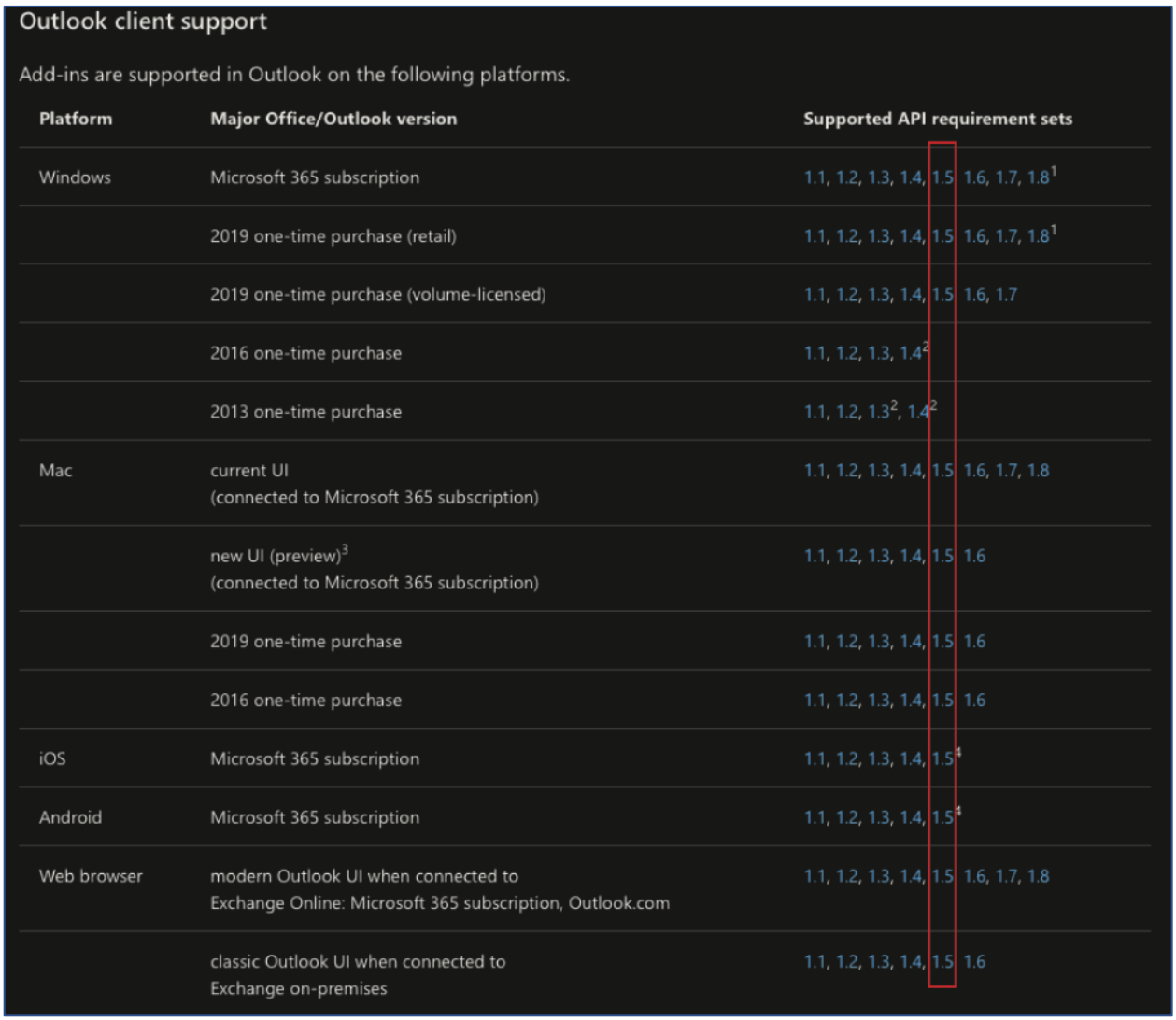
You must be on Office 365 with Centralized Deployment enabled.

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).



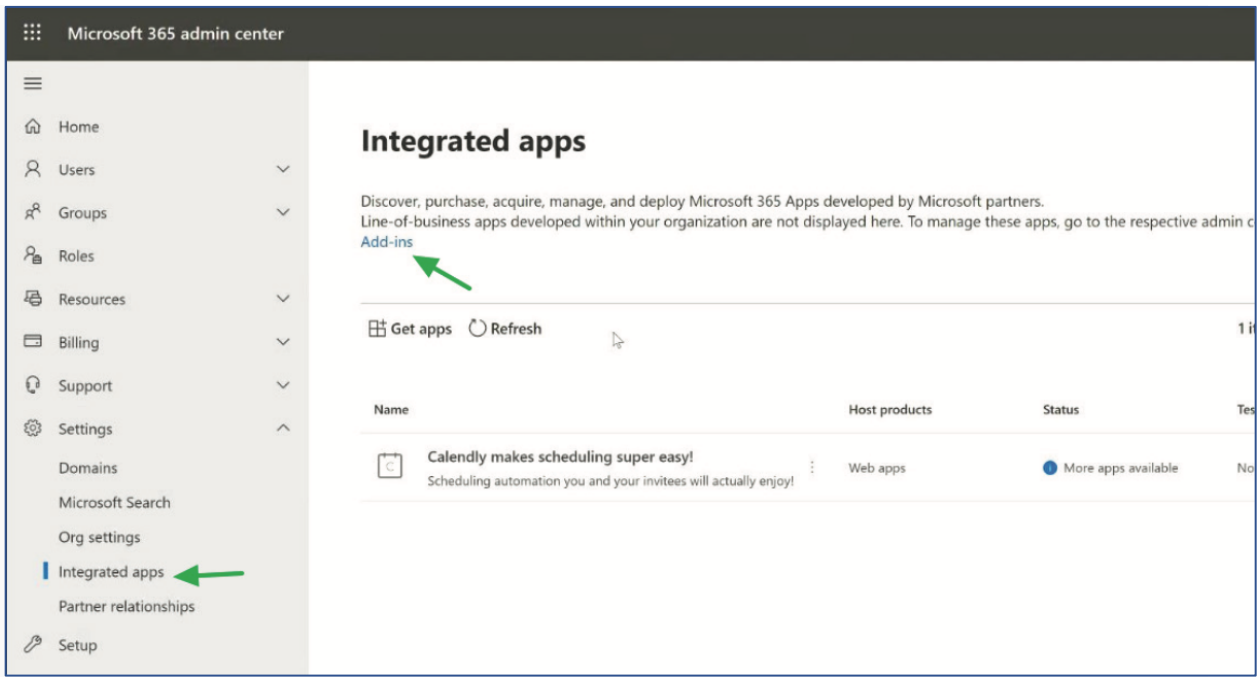
Outlook client support

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

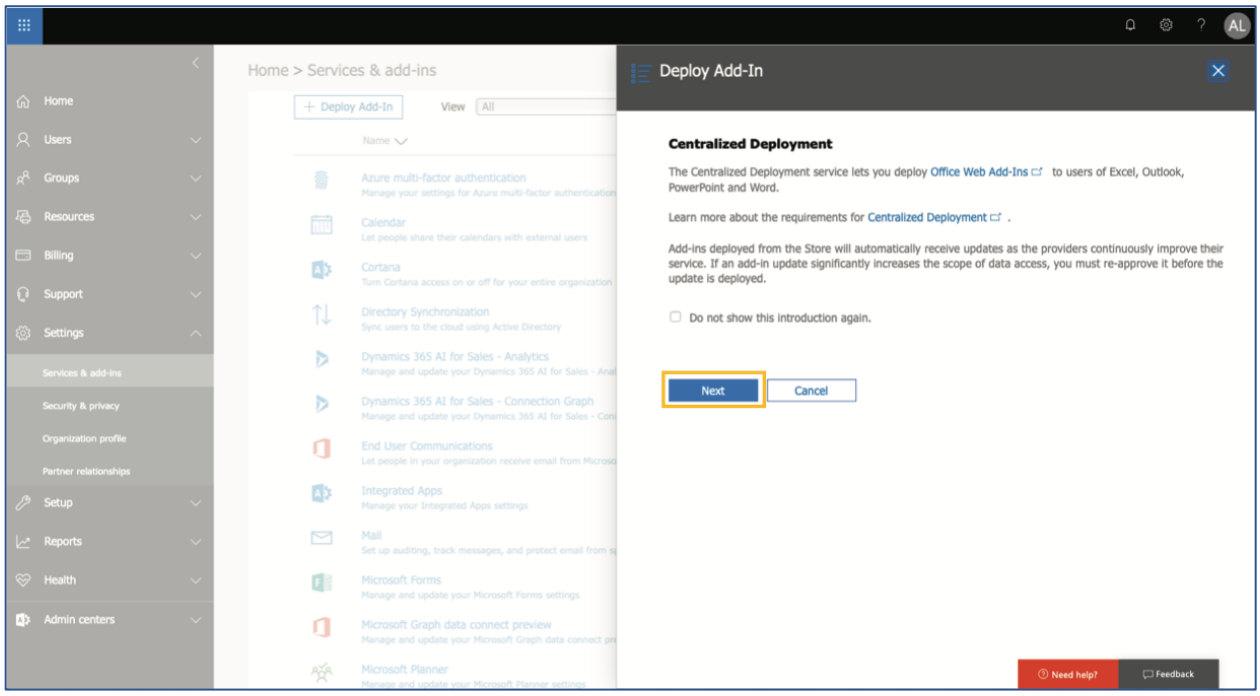
Deploying the Catch Phish Outlook Plug-In

1. Login to the Microsoft O365 Admin Center
2. Navigate to Settings > Integrated apps and click the **“Add-In”** link at the top of the screen

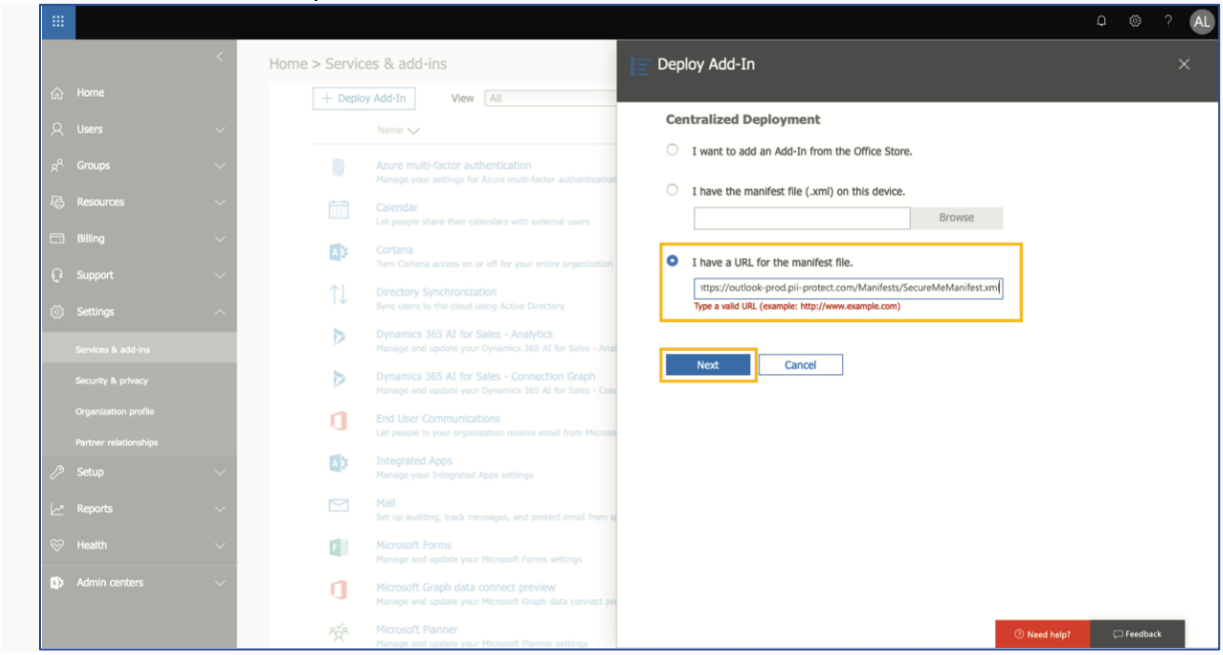


   a. You can also use the following URL to navigate directly there: https://admin.microsoft.com/AdminPortal/Home#/Settings/AddIns

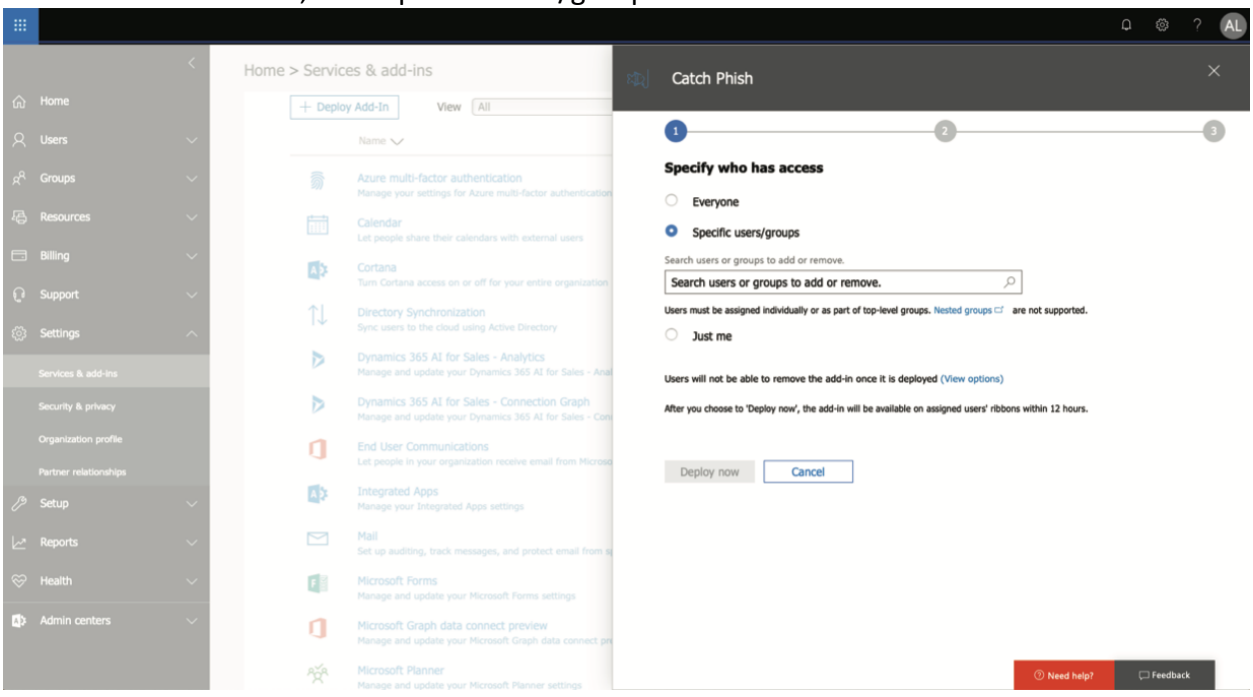
3. Click the **“Deploy Add-in”** button.



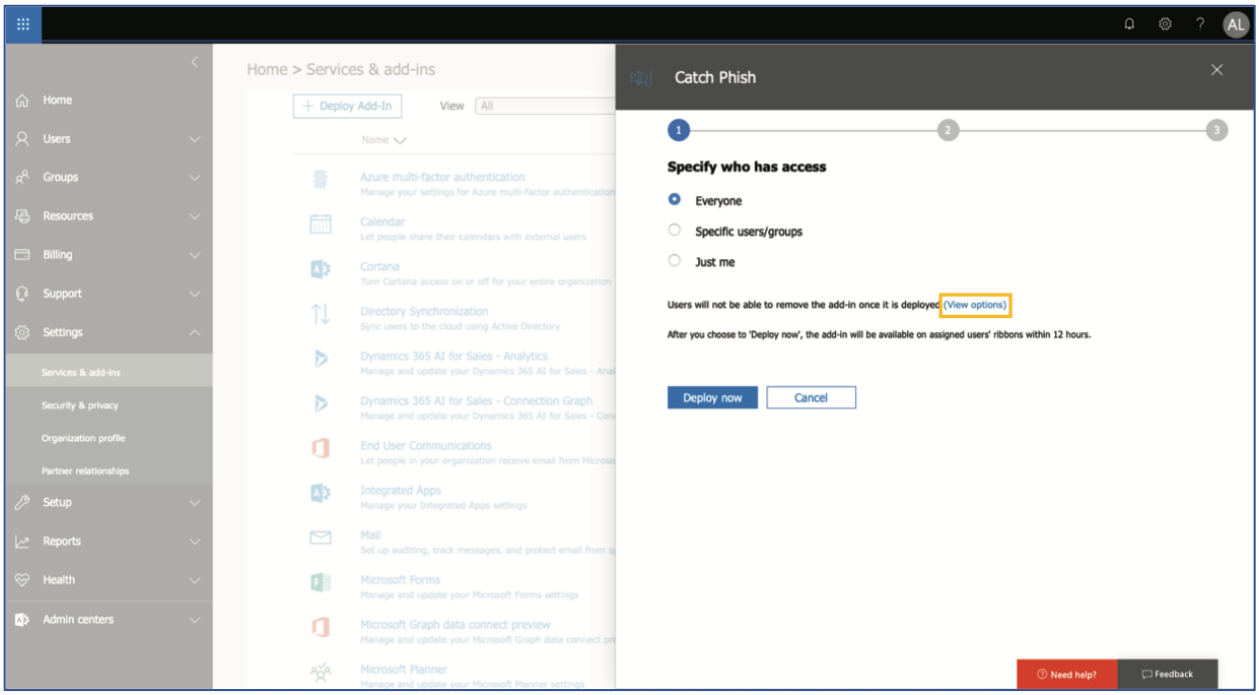
4. Review the overview for Centralized Deployment and hit: **“Next”**
5. Select the URL option for the manifest file



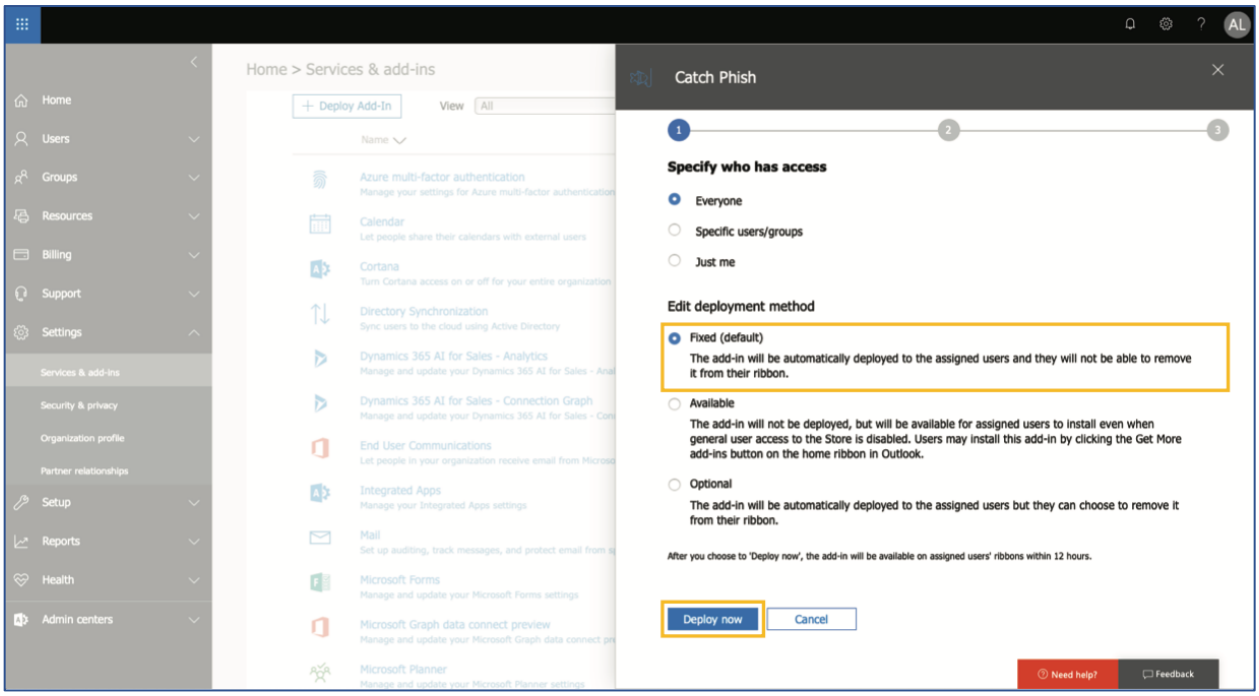
6. Paste the URL for the manifest file inside the textbox: https://catchphish.email/SecureMeManifest.xml
    a. Note: https:// must be in the URL even if https:// is already displayed in grey on the left-hand side
7. Then hit **“Next”** to continue
8. Specify access to the email analysis tool
    a. Configure access to the Catch Phish Outlook Plug-In. You can choose to deploy to all users, or to specific users/groups.



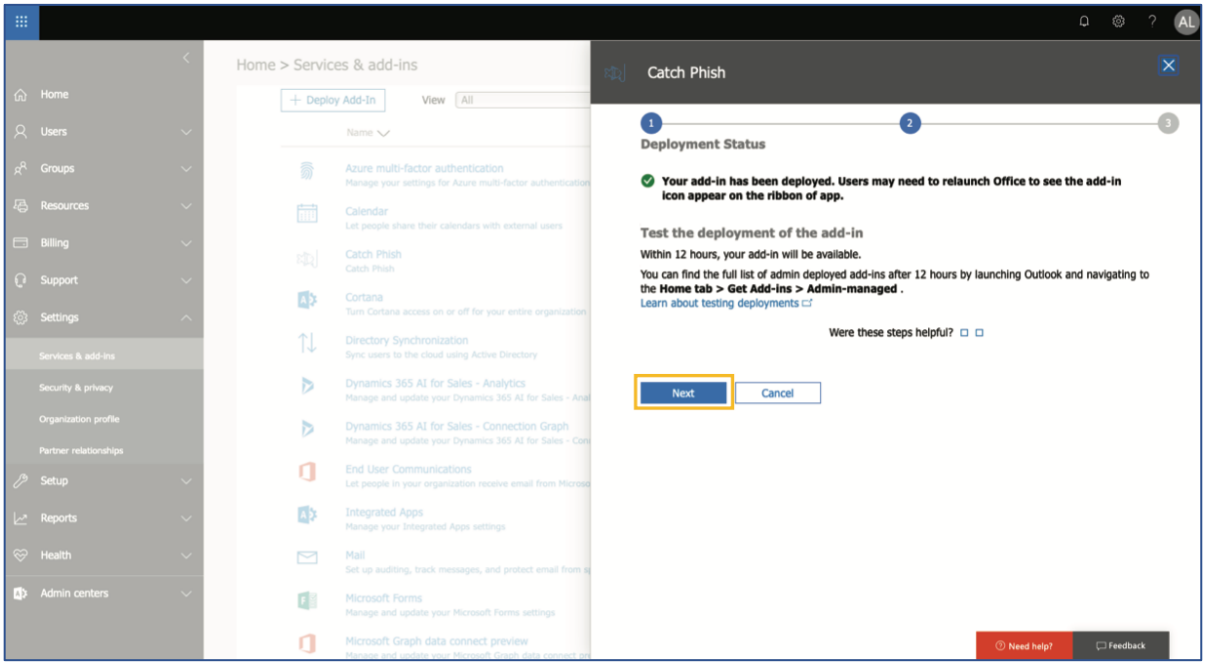
9. Edit the deployment settings by clicking “View Options”



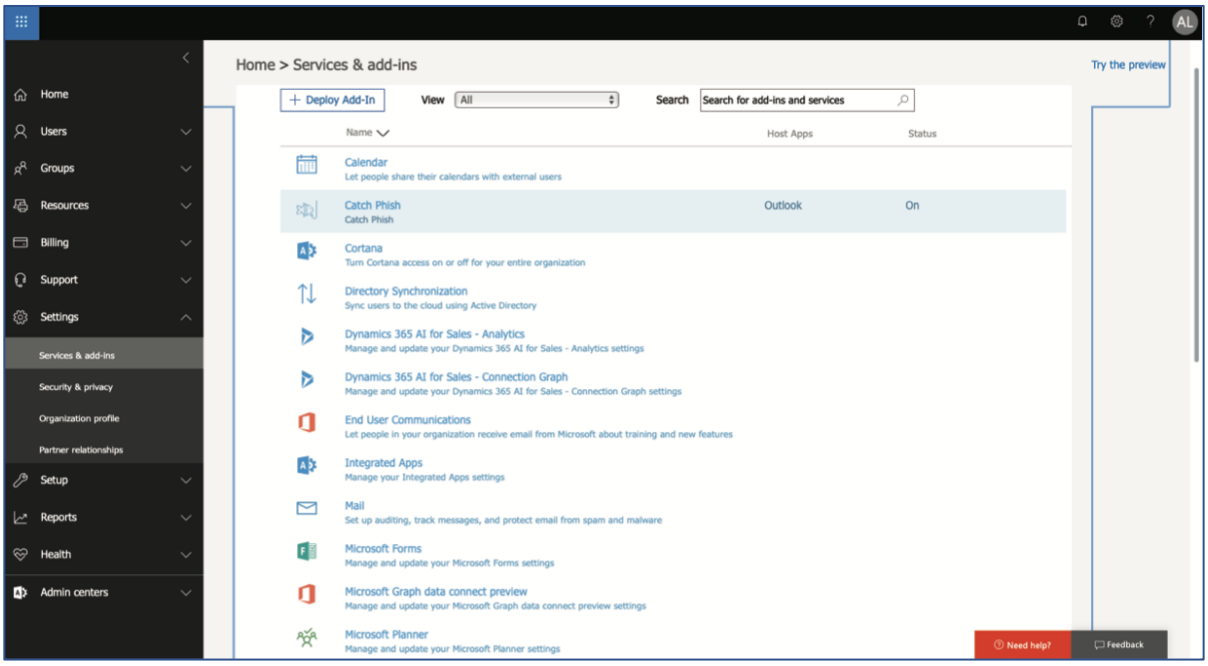
10. Ensure the **“Fixed (default)”** option is selected. Click the **“Deploy now”** button to deploy the Catch Phish Email Analysis Tool to all desired users



11. Review your deployment status



12. Click the **"Next"** button after reviewing the delay notice.
13. Navigate to the **Services & add-ins** dashboard
14. Confirm that Catch Phish Email Analysis Tool is accurate:
    a. Host Apps: Outlook
    b. Status: On



You’re All Set!

You’ve successfully deployed the Catch Phish Outlook Plug-In!