OXEN Security Portal

Catch Phish Email Analysis Tool

WHAT IS CATCH PHISH?

Catch Phish is an Outlook plugin or add-on that allows your users to mark emails as possible phishing attempts and send them in for analysis. If users correctly submit a phishing simulation email using Catch Phish, they can gain points towards their EVA score in the security training portal. This is a great tool for teaching users how to spot a phishing email.

Currently this plugin is for **Outlook only** and is deployed through the Office 365 Admin Center. It is available for Outlook web, mobile, and desktop version of 1.5 and newer.

FREQUENTLY ASKED QUESTIONS

How do users gain or lose points?

Employee Secure Score (ESS): If a user lost ESS points by falling for a previous phishing simulation, they will gain back a portion of their lost points for positive identification.

Phish Caught Count: Each time a user positively identifies a phishing simulation their phish count will increase! This does not affect their ESS score.

What about an external email that is not part of a phishing simulation?

A warning message is returned alerting users to proceed with caution. Users can click “Send for analysis” to learn more or move to an automatically created phishing folder.

Where do the emails go?

Emails are securely captured and processed by a machine learning service. The analyzed email is sent back to the user and never stored.

Will I receive a notification?

You will not be notified when a user sends an email for analysis. There is currently no reporting for managers and data is not stored for emails submitted for analysis.

What's analyzed?

The system uses Machine Learning and Aritificial Intelligence to analyze the links, language, attachments, and hidden elements and identifies any red flags. The email is assigned a phishing threat level indicating the likelihood of the email being a legitimate phishing message. Users can click on the identified components in the analysis to learn more about why the area was identified and if it contains any potential red flags. This real-time analysis trains users on what to look for, identifies any possibly malicious links, and reduces tickets that take up your tech's time!

DEPLOYMENT INSTRUCTIONS

1. Log in to the Microsoft O365 Admin Center and navigate to **Settings > Services & add-ins**.
2. Click the **Deploy Add-in** button.
3. Review the overview for Centralized Development and then hit **Next**.
4. Select the **URL** option for the manifest file.
5. Paste the URL for the manifest file inside the textbox: https://catchphish.email/SecureMeManifest.xml
6. Then hit **Next** to continue.
7. Configure access to the Catch Phish Email Analysis Tool. You can choose to deploy to all users or specific users/groups.
8. Edit the deployment settings by clicking View **Options**. Ensure the **Fixed (default)** option is selected.
9. Click the **Deploy Now** button to deploy the tool to all desired users.
10. Click **Next** after reviewing the delay notice.
11. Navigate to the S**ervices & add-ins** dashboard, and confirm the Catch Phish Email Analysis Tool is accurate:
    Host Apps: Outlook
    Status: On
12. Click **Close** to exit the window.

Then, it's time to announce the plugin to your users! You can use this announcement email as a starting point (.docx file).