PHISH-AWARE

User Manual

SEAN DOWLING
C00246571

Contents

Table of Figures

Introduction

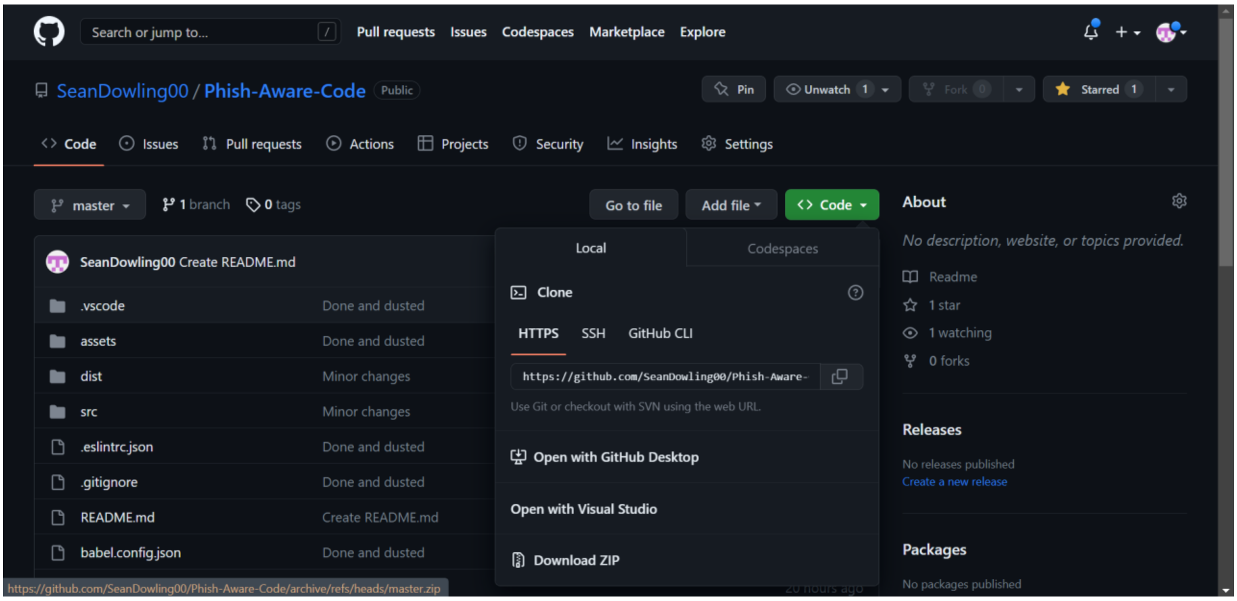
Phish-Aware is an Outlook Add-In designed to assist users in determining a phishing attack using header information analysis, URL analysis and attachment analysis. The tool provides an in-depth compilation of details enabling the user to make informed decisions on whether an email may be malicious or safe. Phish-Aware not onlyruns analysis on header information, URLs and attachments but also provides guidance on common techniques used by attackers. Phish-Aware also provides a reporting feature that will send potentially malicious emails to IT Services, and they will take appropriate action.

Requirements

Phish-Aware will run on any Mac, Windows or Linux machine that has an internet connection. Due to the availability of the browser version of Outlook, any Operating System will be able to provide this service. Phish-Aware is also available in Outlook's desktop version on Windows and Mac, but not Linux.

Installation

Installing the tool is simple. Go to the https://showcase.itcarlow.ie/ website, find“An Outlook Add-In for Detection and Guidance against Phishing Attacks” near the bottom, click on it, scroll to near the end and click “Download the Tool.” This will then open the GitHub repository where the code resides. Click the green “code button on the right-hand side and click download zip.



SeanDowling00 / Phish-Aware-Code

SeanDowling00 Create README.md

.vscode	Done and dusted
assets	Done and dusted
dist	Minor changes
src	Minor changes
.eslintrc.json	Done and dusted
.gitignore	Done and dusted
README.md	Create README.md
babel.config.json	Done and dusted

https://github.com/SeanDowling00/Phish-Aware-

Use Git or checkout with SVN using the web URL.

No description, website, or topics provided.

No releases published

No packages published

https://github.com/SeanDowling00/Phish-Aware-Code/archive/refs/heads/master.zip

Figure 1: Showcase Website

This will install the tool onto your machine. Once you have it installed, right click the folder, and click unzip. Once done, go to your Outlook application, either the desktop version or browser version. The installation process is similar.

Desktop Version

Step 1.

Once you are on your desktop version of Outlook, please click “Get Add-Ins” on the ribbon along the top of your screen.

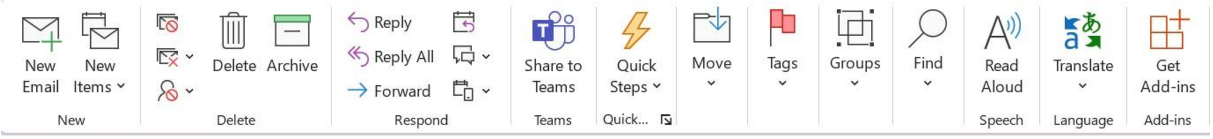
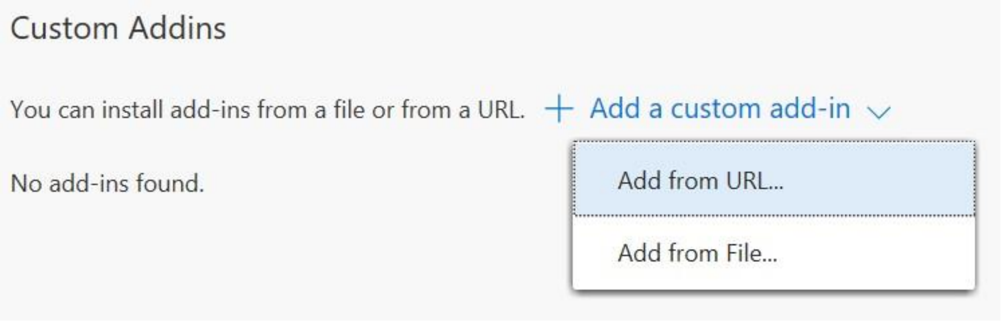


Figure 2: Outlook Ribbon

Step 2.

Once you click that, click on “My Add-Ins” on the list on the left-hand side. Scroll to the bottom of the page and click on “Add a custom add-in.” A drop-down menu will appear, click “Add from File…”


Custom Addins

You can install add-ins from a file or from a URL.

No add-ins found.

Figure 3: Custom Add-In Installation

Step 3.

Once you clicked that a file explorer will pop up. Go to the location that you have downloaded the folder, presumably “Downloads.” Once there click into the folder and click into “Phishing Detection and Guidance” folder. From here, double click on the “manifest.xml” file. A warning will appear after this, just click install.

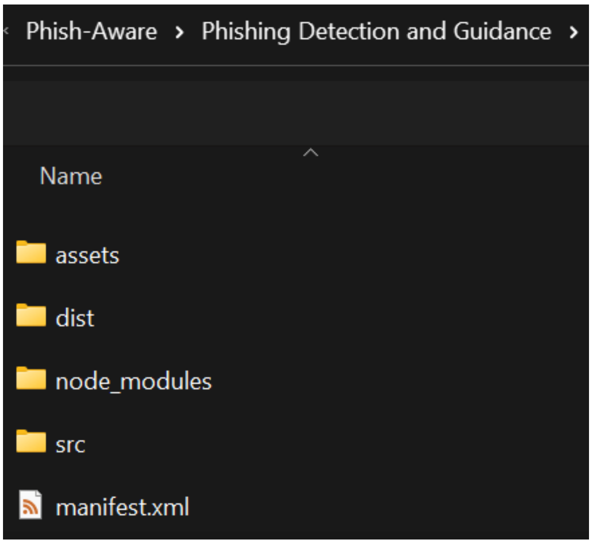


Figure 4: Manifest File

Browser Version

Step 1.

Along the top hand bar, you should see “Get Add-Ins,” like the Desktop version.

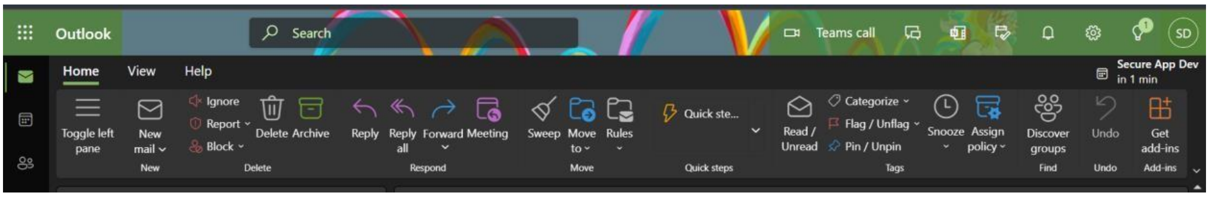
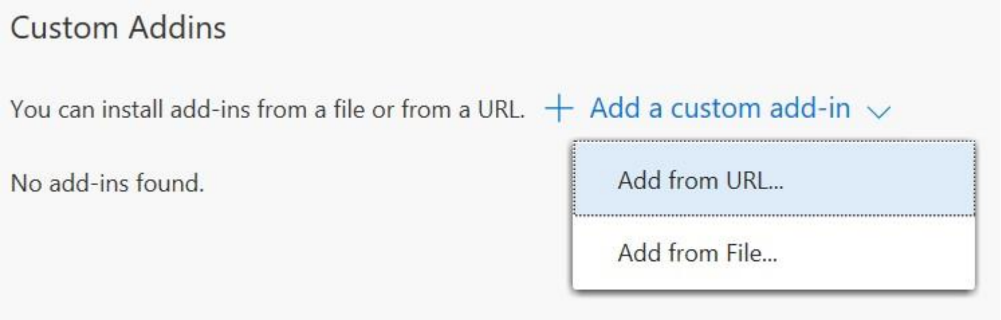


Figure 5: Outlook Ribbon

Step 2.

Once you click that, click on “My Add-Ins” on the list on the left-hand side. Scroll to the bottom of the page and click on “Add a custom add-in.” A drop-down menu will appear, click “Add from File...”



Custom Addins

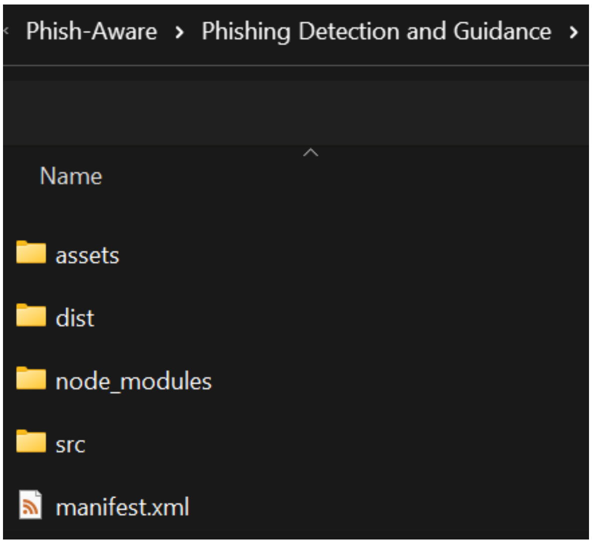
You can install add-ins from a file or from a URL. + Add a custom add-in

No add-ins found.

Figure 6: Custom Add-In Ribbon

Step 3.

Once you clicked that a file explorer will pop up. Go to the location that you have downloaded the folder, presumably “Downloads.” Once there click into the folder and click into “Phishing Detection and Guidance” folder. From here, double click on the “manifest.xml” file. A warning will appear after this, just click install.



Phish-Aware › Phishing Detection and Guidance ›

Name

assets

dist

node_modules

src

manifest.xml

Figure 7: Manifest File

How to Use

When you first click on “Phish-Aware” you will be given two options: “Analyse”and “Guide.”

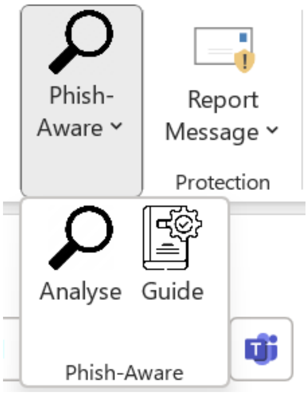
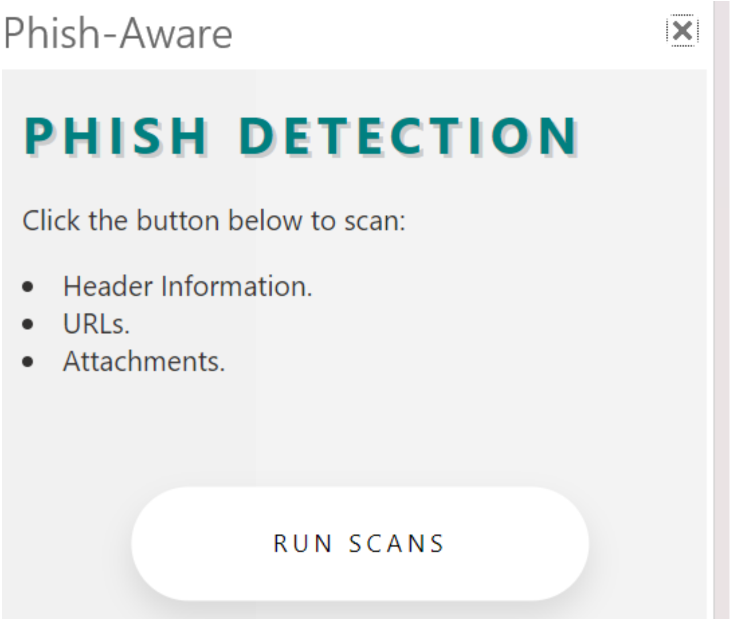


Figure 8: Phish-Aware Tool

- Analyse
  - Analyse header information
  - Analyse URLs
  - Analyse Attachments
  - Report
- Guide
  - Phishing Overview
  - Warnings
  - Common Techniques

Analyse

When you first click on Analyse you will be shown this page:



Phish-Aware

PHISH DETECTION

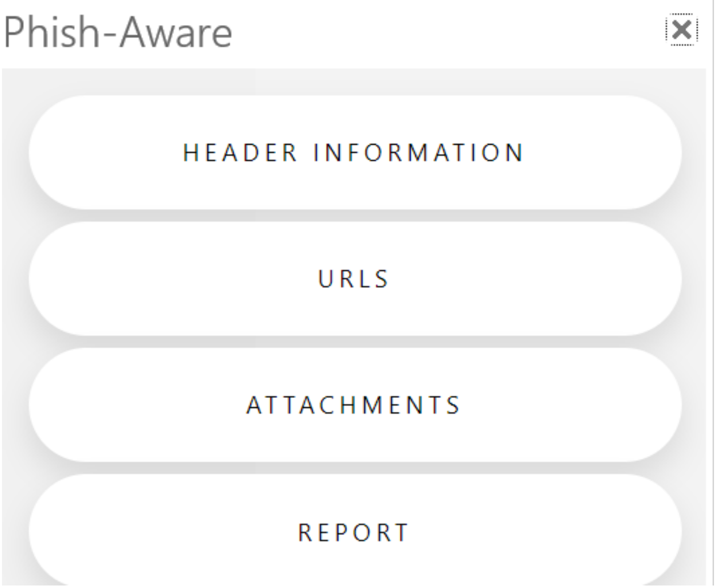
Click the button below to scan:

- Header Information.
- URLs.
- Attachments.

Figure 9: Run Scans Screen

By clicking on "Run Scans," header information and URLs will be automatically scanned for you, attachments will have to manually done later.

You will then get this page:



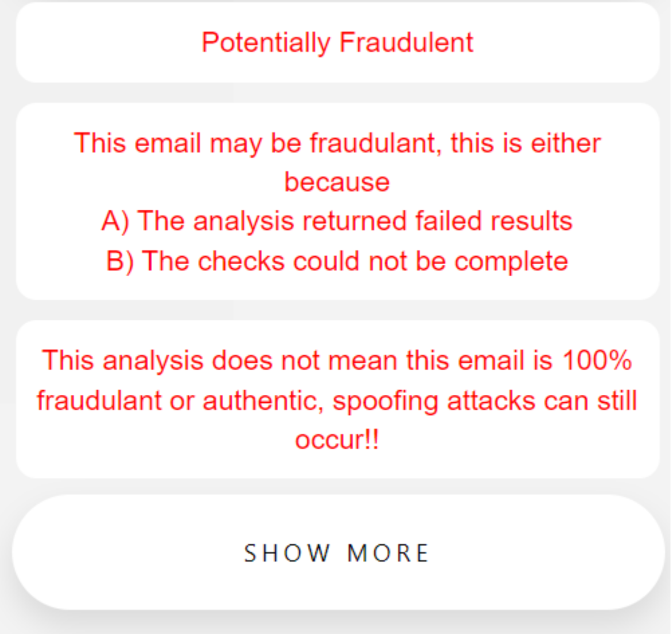
Phish-Aware

Figure 10: Scan Options

By clicking on any of the buttons you will be shown either an in-depth analysis of header information, URLs, attachments, or an option to report the email.

Header Information Analysis

By clicking on the header information button, you will first be shown a quick overview of the header analysis, allowing you to make a quick determination of theemail:



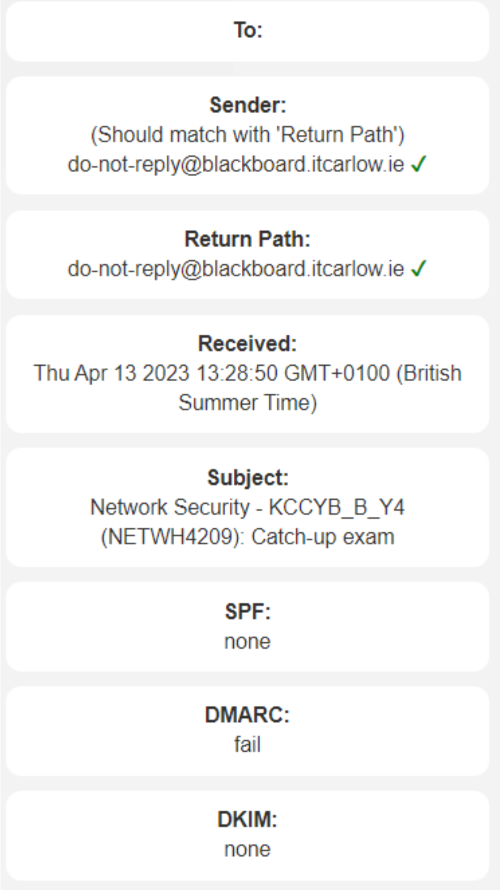
Potentially Fraudulent

This email may be fraudulant, this is either because
A) The analysis returned failed results
B) The checks could not be complete

This analysis does not mean this email is 100% fraudulant or authentic, spoofing attacks can still occur!!

Figure 11: Header Information Overview

You will also be offered a “Show More” button for a more in-depth analysis of the all the checks that were made, from the “To,” “From,” “Subject,” “Date,” “Return Path” and the authentication results: “SPF”, “DKIM” and “DMARC”.



To:

Sender:
(Should match with 'Return Path')
do-not-reply@blackboard.itcarlow.ie ✓

Return Path:
do-not-reply@blackboard.itcarlow.ie ✓

Received:
Thu Apr 13 2023 13:28:50 GMT+0100 (British Summer Time)

Subject:
Network Security - KCCYB_B_Y4 (NETWH4209): Catch-up exam

SPF:
none

DMARC:
fail

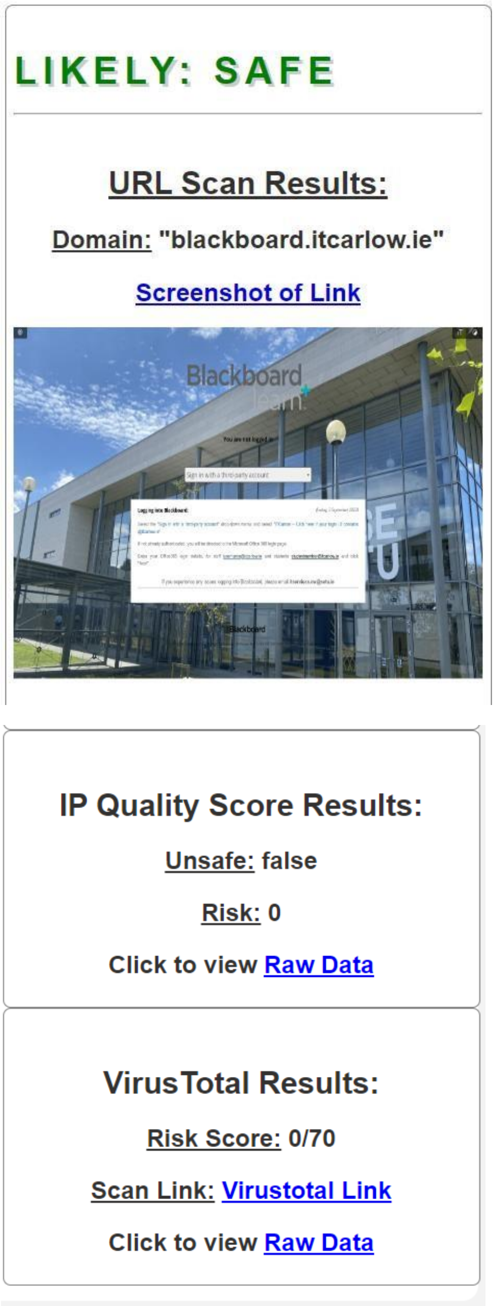
DKIM:
none

Figure 12: In-Depth Header Information

There are also options available at the very bottom to inform users on what SPF, DKIM and DMARC are.

URL Analysis

Next up is URL analysis, by clicking on the “URLs” button at the top, you will get an overview of the scans that have taken place for any URL found within the email body, it gives you “Likely” rating at the very top, based on how malicious each of the API’s have rated the URL. You are also given the option to click on “Raw Data” for each of the APIs to give an even more in-depth view of the URLs and why they were deemed either malicious or safe.



LIKELY: SAFE

URL Scan Results:

Domain: "blackboard.itcarlow.ie"

Screenshot of Link

IP Quality Score Results:

Unsafe: false

Risk: 0

Click to view Raw Data

VirusTotal Results:

Risk Score: 0/70

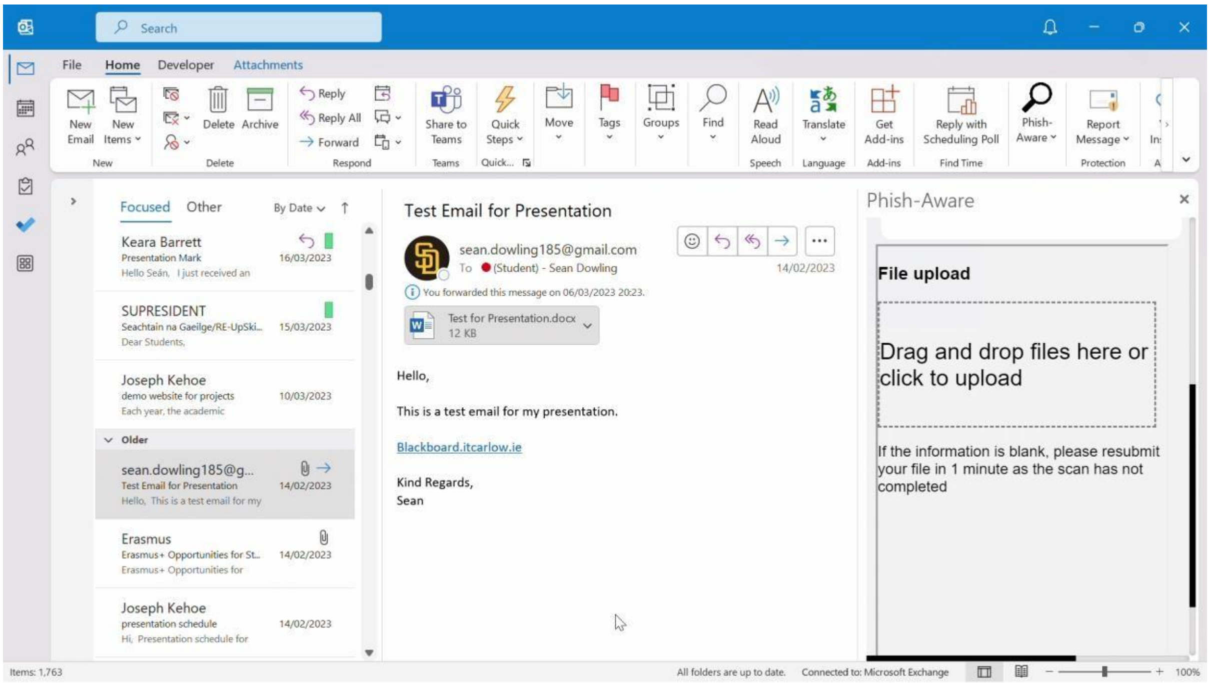
Scan Link: Virustotal Link

Click to view Raw Data

Figure 13: URL Analysis

Attachment Analysis

Attachments unfortunately are managed slightly differently. Due to security, we require users to drag and drop the attachments into the Add-In itself demonstrated below.



Test Email for Presentation

sean.dowling185@gmail.com

To ● (Student) - Sean Dowling

14/02/2023

You forwarded this message on 06/03/2023 20:23.

Test for Presentation.docx
12 KB

Hello,

This is a test email for my presentation.

Blackboard.itcarlow.ie

Kind Regards,
Sean

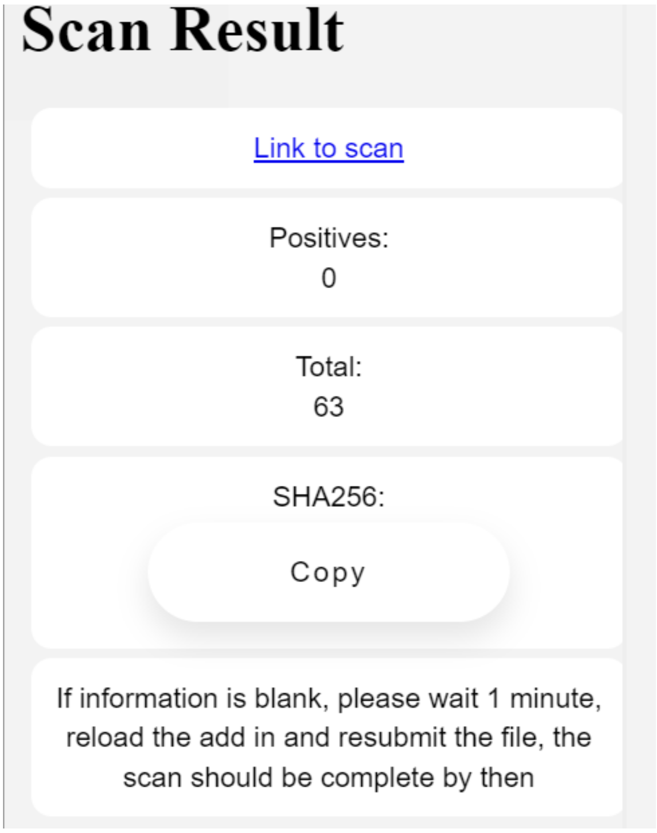
File upload

Drag and drop files here or click to upload

If the information is blank, please resubmit your file in 1 minute as the scan has not completed

Figure 14: Attachment Drag and Drop Area

Once you have done the above step, you can then click the submit button. This will automatically scan the file and return the necessary information for a user to make their determination on whether a file is malicious or not. The first detail that appears is "Link to scan," by clicking on this you will be redirected to the VirusTotal webpage where your scan took place. Here, you can get a more in-depth analysis of your scan. Next you will see positives and total, this is the amount of security vendors marked this file as malicious, the higher the positive mark, the more likely it is to be malicious. As you can see in the example below, there are 0/63 positive results. Finally, you are shown a copy button for the SHA256, by clicking this button you can go to other file scanners online and paste thehash into their scanners to verify if your file is malicious or not if you are still unsure.



Scan Result

Link to scan

Positives:
0

Total:
63

SHA256:

If information is blank, please wait 1 minute, reload the add in and resubmit the file, the scan should be complete by then

Figure 15: Attachment Analysis Overview

Reporting

The final button is “Report.” By clicking this button, a new email will open, with all the details needed. You can review this information before you click send. By clicking send you will send the email to the IT Services team who will review the information and take appropriate action.

Guidance Tool

The final part of this project is the Guidance tool. Found by clicking on Guide, shown below:

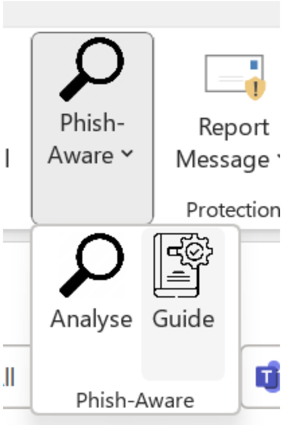
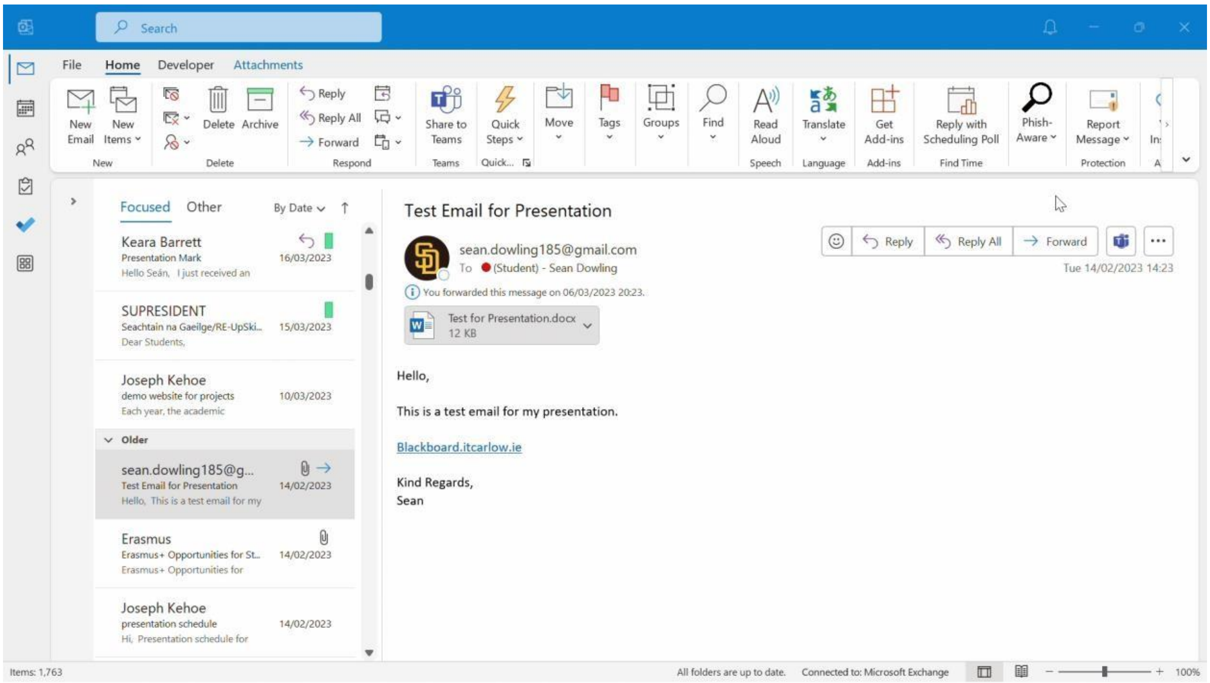


Figure 16: Phish-Aware Guide Location

By clicking this button, you will be given a multitude of information. At the bottom, there are a multitude of clickable buttons that will reveal information on common techniques used by attackers.



Keara Barrett
Presentation Mark 16/03/2023
Hello Seán, I just received an

SUPRESIDENT
Seachtain na Gaeilge/RE-UpSki... 15/03/2023
Dear Students,

Joseph Kehoe
demo website for projects 10/03/2023
Each year, the academic

sean.dowling185@g...
Test Email for Presentation 14/02/2023
Hello, This is a test email for my

Erasmus
Erasmus+ Opportunities for St... 14/02/2023
Erasmus+ Opportunities for

Joseph Kehoe
presentation schedule 14/02/2023
Hi, Presentation schedule for

Test Email for Presentation

sean.dowling185@gmail.com
To (Student) - Sean Dowling
Tue 14/02/2023 14:23
You forwarded this message on 06/03/2023 20:23.
Test for Presentation.docx
12 KB

Hello,

This is a test email for my presentation.

Blackboard.itcarlow.ie

Kind Regards,
Sean

Figure 17: Guide Overview

And that has been a complete guide to my final year project – “Phish-Aware,” an Outlook Add-In tool for phish detection and guidance. I hope you have enjoyed it and please feel free to keep on using this tool to your heart’s content.