Phishing Email Detection Tool

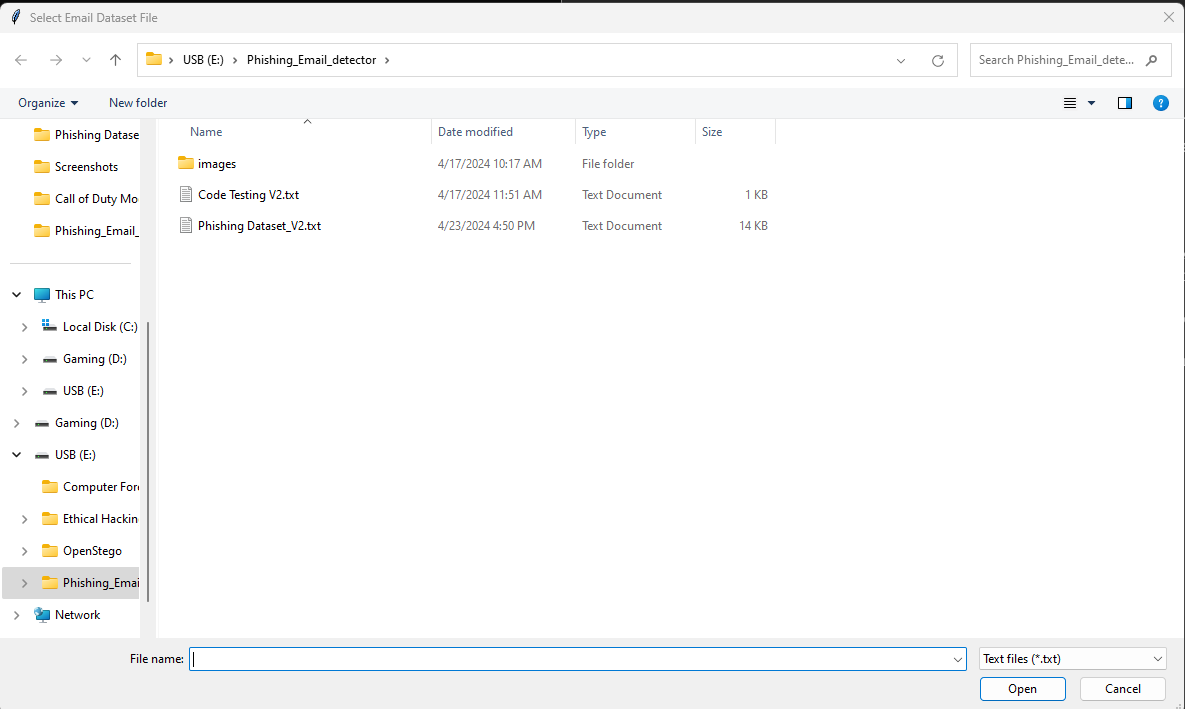
***Usage Guide***

This guide will cover the usage of Phishing Email Detection Tool app. The app is still in development, so it is not a finished product. Please leave a comment for any questions, or feedback.

Windows Version

After installing everything, you should have an “images”, the Phishing app, the “Phishing\_Dataset” txt file, and the code for the app if you chose to install it. The text file is the dataset and is what the app needs to be able to determine whether an email is a phishing email. The folder contains the images the code will be using. Please make sure to keep the images folder within the same folder as the app. You may place the dataset file anywhere you’d like, but I recommend keeping it in the same folder with everything else.

When running the app, you will be prompted to select the dataset file. Here is how it will look like:



Please select the correct file, or the code may not work properly. After selecting the dataset file you will be presented with a GUI like this:

A screenshot of a computer

Description automatically generated

Not very pretty I know, but it’ll get the job done for now. From here, you can input the email you wish to analyze. Below here is how it will look like when an email is a Phishing email and when it is a safe email:

A screenshot of a computer

Description automatically generatedA computer screen with a message

Description automatically generated

After getting your results, you may input another email, or save the email which will create a folder called “user\_emails” which will have the email you saved in a txt file. Here is how it will look:

A screenshot of a computer

Description automatically generated