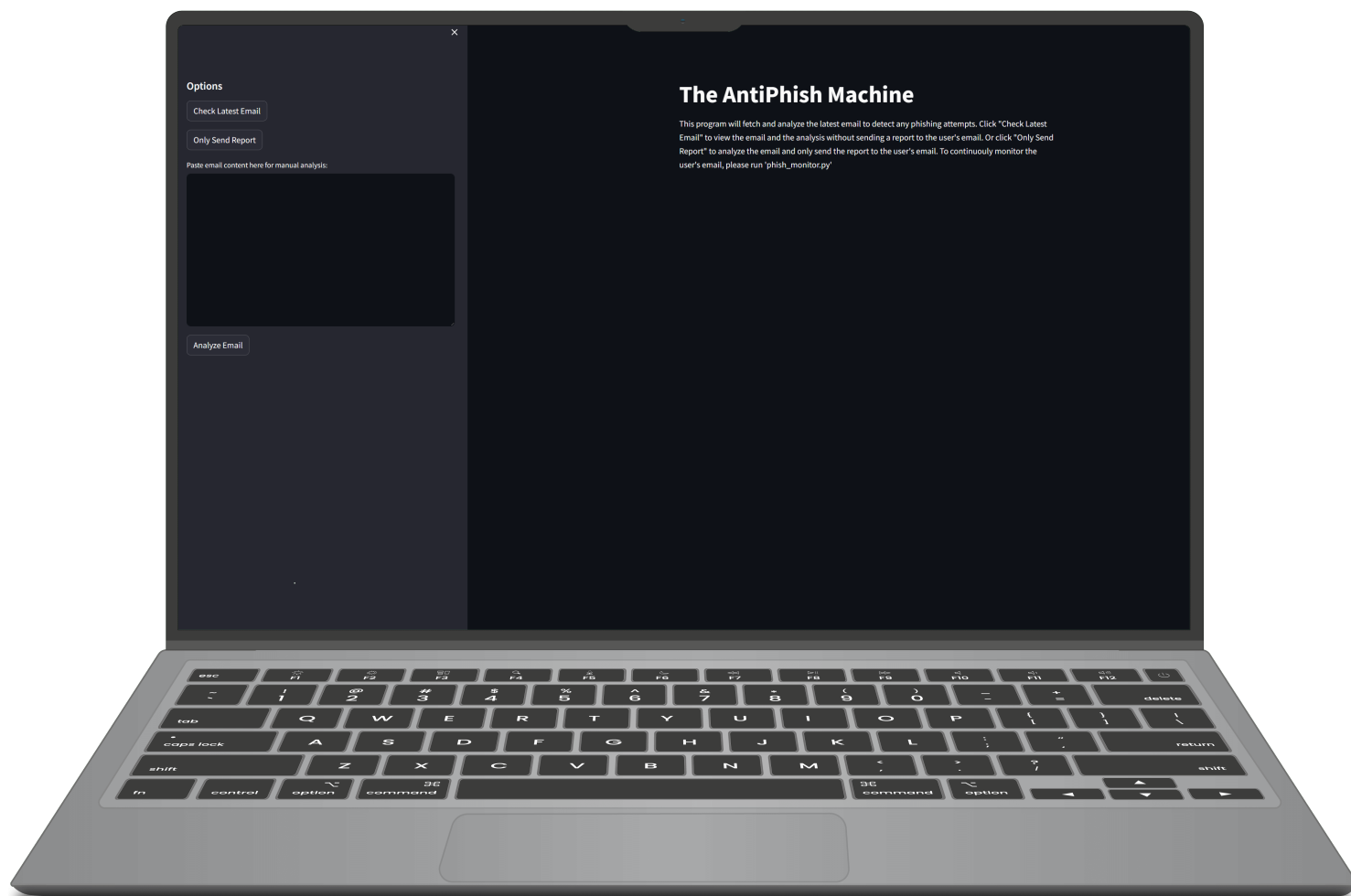


JUSTIN JOY

ADELPHI UNIVERSITY, SPRING 2024

# ANTIIPHISH MACHINE

## SOFTWARE USER MANUAL



# AntiPhish Machine

## REQUIRED LIBRARIES

### Working Files:

- **phish\_monitor.py**
- **phish\_gui.py**
- **phish\_gui\_app.py**

### Third Party Modules (install via pip)

- Requests: Simplifies making HTTP requests.
- Torch: A library for machine learning and tensor computations (PyTorch).
- Transformers: Provides models and tools for many transformer-based models (HuggingFace).
- IMAPClient: Simplifies working with the IMAP protocol.
- OpenAI: Client library to work with and access OpenAI's API.
- Keras (TensorFlow): High-Level neural networks library, used for building and training deep learning models— installed via TensorFlow
- StreamLit: App framework for creating simple (minimal) web apps.
- Plotly: A graphing library to create quality graphs

### Working Files:

- **LSTM\_train.py**
- **transformer\_train.py**

### Third Party Modules (install via pip)

- Pandas: For data manipulation and analysis.
- NLTK: The Natural Language Toolkit used to work with human language data.
- Keras (TensorFlow): High-Level neural networks library, used for building and training deep learning models— installed via TensorFlow
- SciKit-Learn: A Machine Learning library.
- Torch: A library for machine learning and tensor computations (PyTorch).
- Transformers: Provides models and tools for many transformer-based models (HuggingFace).
- Numpy: A library for numerical operations and N-dimensional arrays.
- TQDM: A library for creating progress bars.

## ADDITIONAL SETUP

### Setting Up Environment Variables (for Windows):

To allow API functionality and logging into IMAP/SMTP, API Keys and Password Keys need to be set as the following environment variables. Follow these steps:

1. Open Command Prompt:



```
Microsoft Windows [Version 10.0.22631.3447]
(c) Microsoft Corporation. All rights reserved.

C:\Users\justi>setx REPORT_GENERATOR_PASSWORD "xc[REDACTED]eu"

SUCCESS: Specified value was saved.

C:\Users\justi>setx OPENAI_KEY "sk-T5S[REDACTED]RXk"

SUCCESS: Specified value was saved.

C:\Users\justi>setx GMAIL_APP_PASSWORD "x[REDACTED]ik"

SUCCESS: Specified value was saved.

C:\Users\justi>setx API_VOID "9589b[REDACTED]ef84"

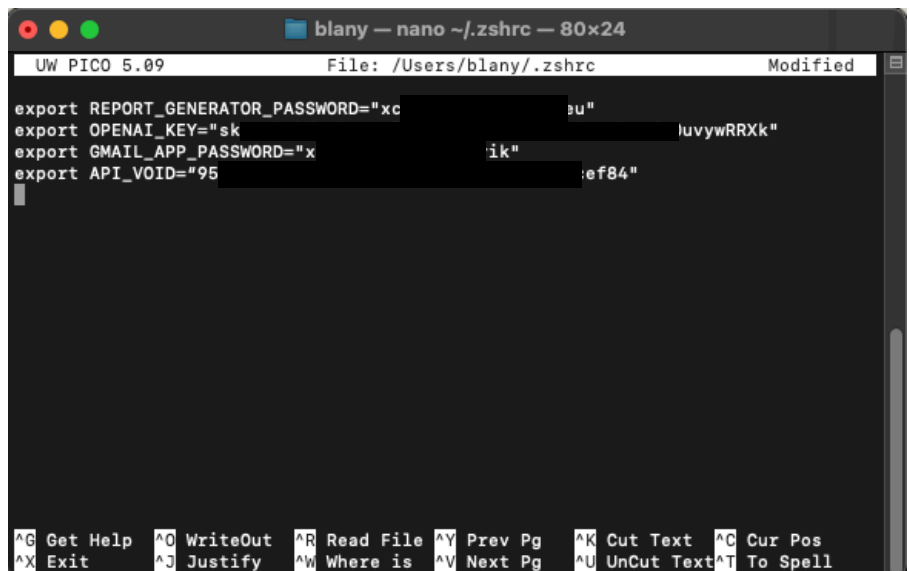
SUCCESS: Specified value was saved.
```

2. Enter the following commands as shown above:

```
setx REPORT_GENERATOR_PASSWORD "PASSWORD HERE"
setx OPENAI_KEY "API KEY HERE"
setx GMAIL_APP_PASSWORD "PASSWORD HERE"
setx API_VOID "API KEY HERE"
```

### Setting Up Environment Variables (for macOS):

1. Open Terminal:
2. Use nano or vim to edit `~/zshrc`
3. "Export" the following environment variables.



```
blany — nano ~/.zshrc — 80x24
UW PICO 5.09 File: /Users/blany/.zshrc Modified
export REPORT_GENERATOR_PASSWORD="xc[REDACTED]bu"
export OPENAI_KEY="sk[REDACTED]luywRRXk"
export GMAIL_APP_PASSWORD="x[REDACTED]ik"
export API_VOID="95[REDACTED]ef84"

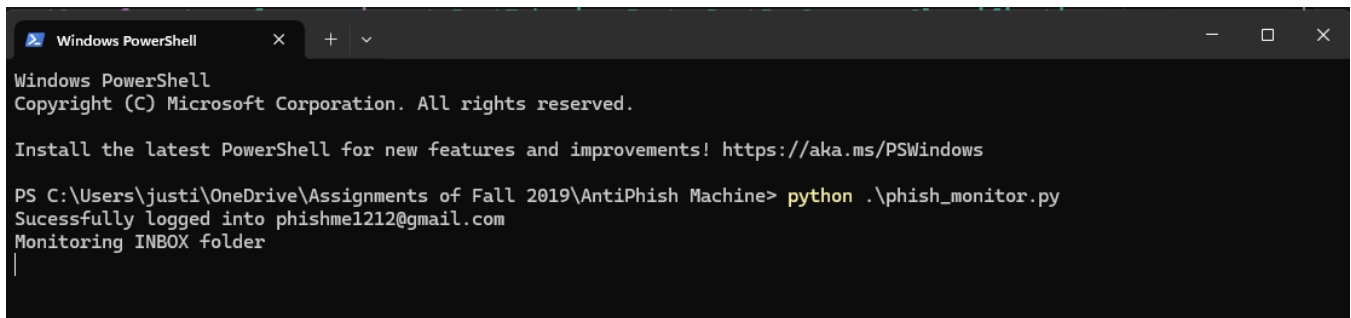
^G Get Help ^O WriteOut ^R Read File ^Y Prev Pg ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where is ^V Next Pg ^U UnCut Text ^T To Spell
```

# Continuous Monitoring

## INITIALIZATION

1. Ensure that you are in the current directory of the program.
2. Start the python program: **phish\_monitor.py**

```
python phish_monitor.py
```



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\justi\OneDrive\Assignments of Fall 2019\AntiPhish Machine> python .\phish_monitor.py
Sucessfully logged into phishme1212@gmail.com
Monitoring INBOX folder
|
```

**macOS users:** The command will be the same, but in terminal.

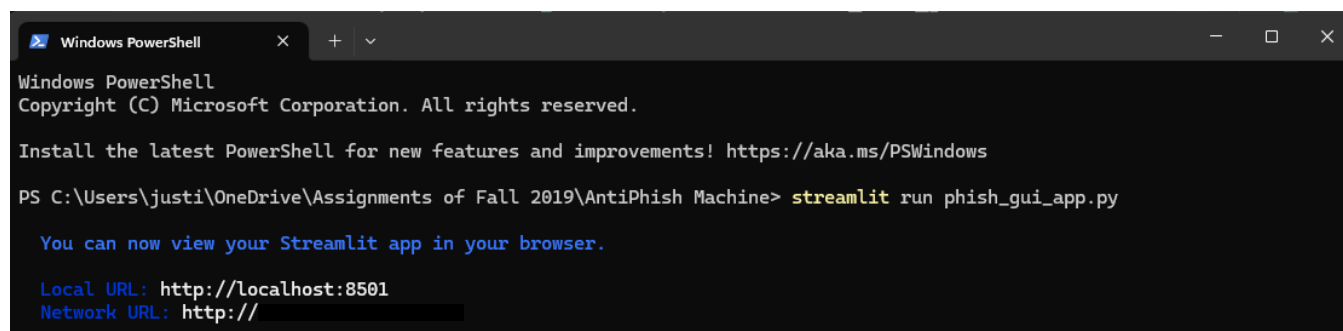
*\*May be "python" or "python3" for some users.*

# Monitoring with GUI

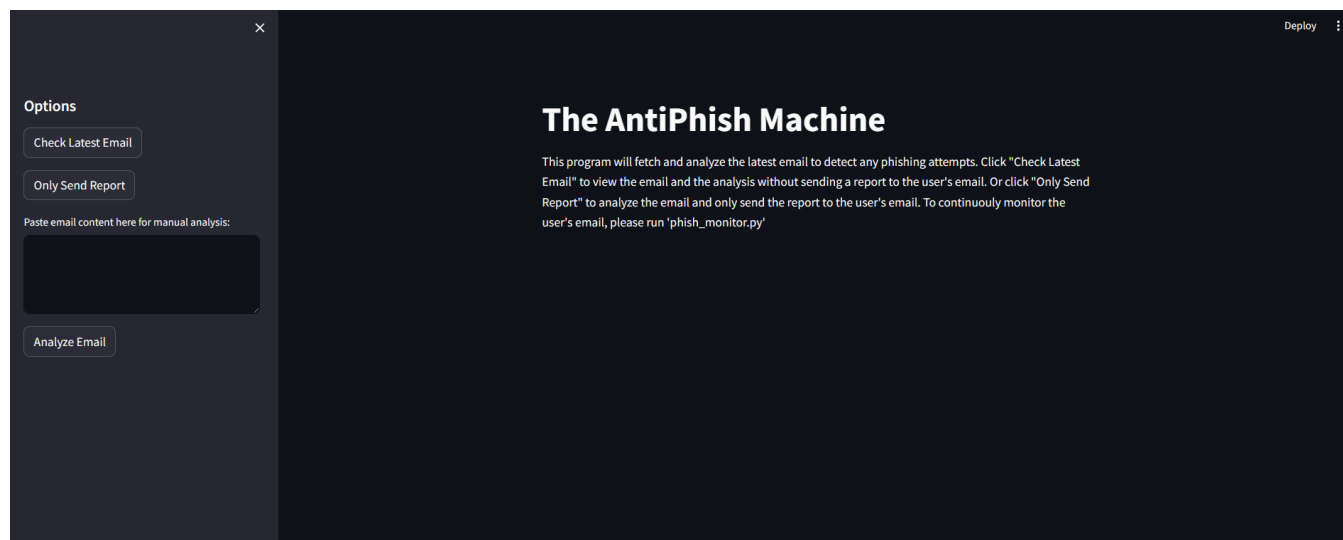
## INITIALIZATION

1. Ensure that you are in the current directory of the program.
2. Run the StreamLit application: `phish_gui_app.py`

```
streamlit run phish_gui_app.py
```



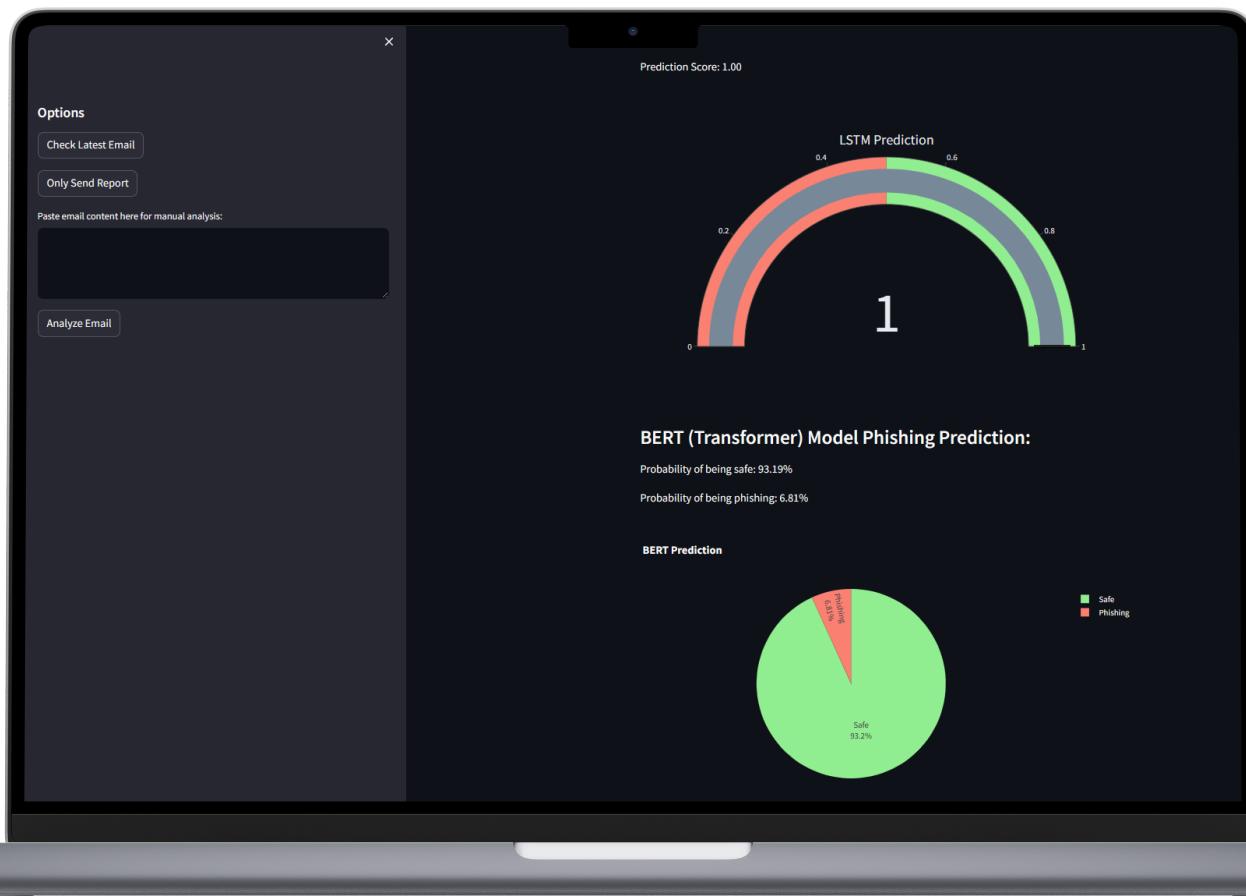
**The browser will open a web application interface for the AntiPhish Machine.**



# Monitoring with GUI

## CHECK LATEST EMAIL

This option will check the latest email and only show the results on the GUI. The Email Content will be shown, OpenAI GPT result, Danger Word Detection result, LSTM Prediction result, BERT Prediction result, URL Analysis Results and Email Analysis Results.



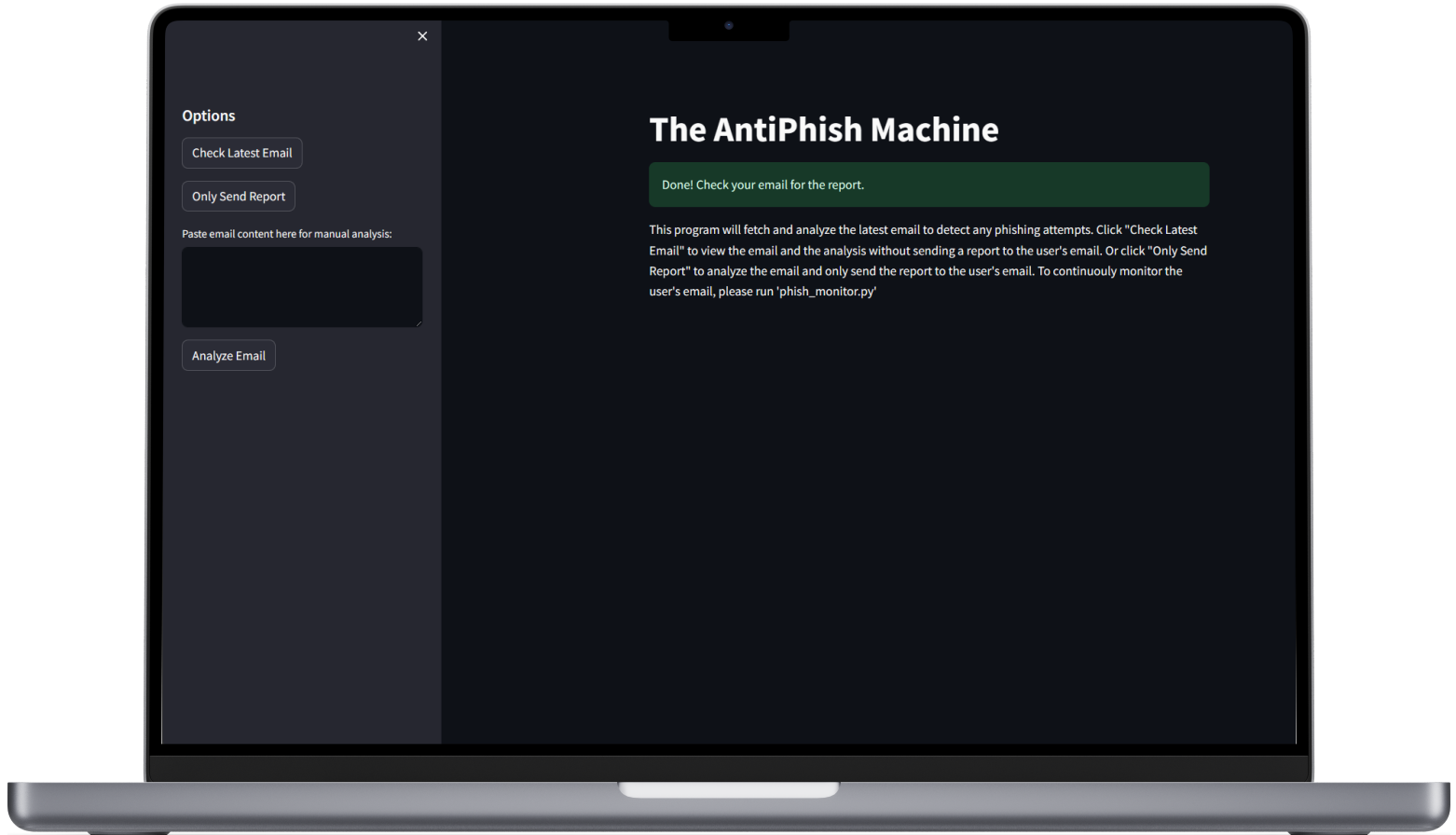
## MANUAL ANALYSIS

The user can also enter their own email plaintext and the AntiPhish Machine will detect any phishing patterns in the manually entered email. This method does not check the users inbox.

# Monitoring with GUI

## ONLY SEND REPORT

This option will only send a report to the user's email and skips the results on the GUI.



# Continuous or GUI Monitoring

## PHISHING REPORTS

- If continuously monitoring, the AntiPhish Machine will continuously monitor the User's email and automatically send a report for any new email.
- If GUI Monitoring, the report will be sent if the user selects "Send Report Only"

