# USER MANUAL

## Aegis Shield Phishing Detection Extension

| | |
|---|---|
| Sudam Pullaperuma | - 10660248 |
| Tharuka Gunasekara | - 10659483 |
| Tanushka Elvitigala | - 10663914 |
| Dulaj Walgama | - 10659489 |

# INTRODUCTION

Welcome to the Aegis Shield Phishing Detection Extension. This manual provides step-by-step instructions for installing, configuring, and using the extension to safeguard your browsing experience against phishing threats. This extension offers real-time URL monitoring, email phishing detection, and customizable whitelist/blacklist management to enhance your security online.

The goal of the "Aegis Shield - Phishing Detection Extension" is to protect users from phishing and malware threats by offering real-time URL monitoring, phishing detection, and actionable alerts to enhance online security. The extension leverages VirusTotal APIs and machine learning for advanced threat detection while providing user-friendly features like whitelist/blacklist management

# SYSTEM REQUIREMENTS

To ensure smooth installation and operation, the following components are required

## Browser

Google Chrome (latest version recommended)

## Backend Requirements

**Python**: Version 3.8 or higher

## Development Tools

**Visual Studio Code (VS Code)**: Recommended for running the backend server and editing configuration files.

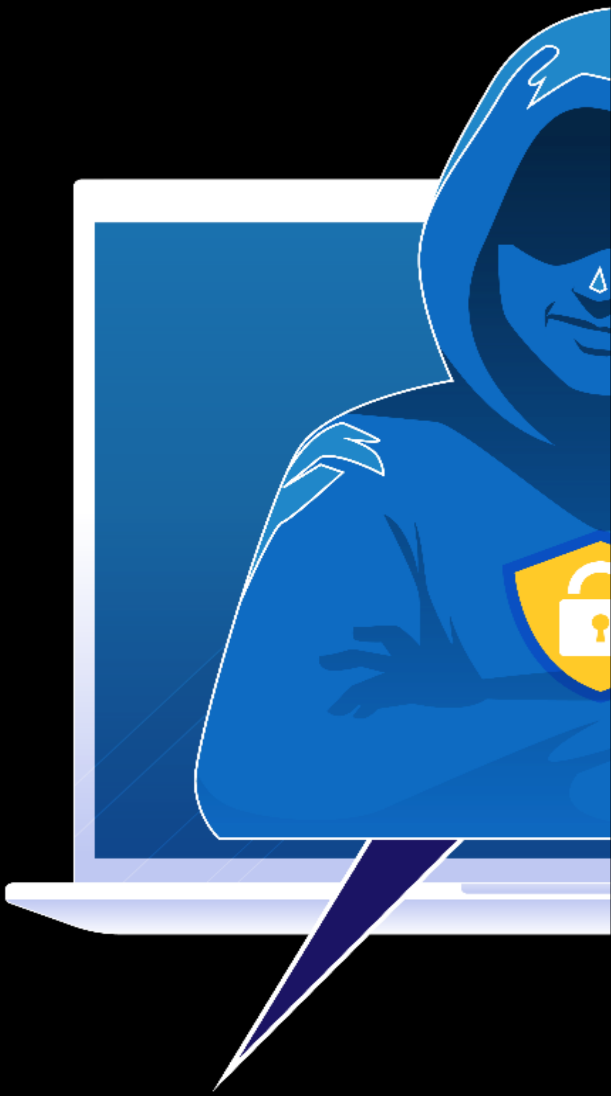
## Internet Connection

Required for Run the Extension

## System Specifications

Minimum of 4GB RAM and 2GHz processor.

At least 100MB of free disk space for extension and backend installation



# Installation Guide

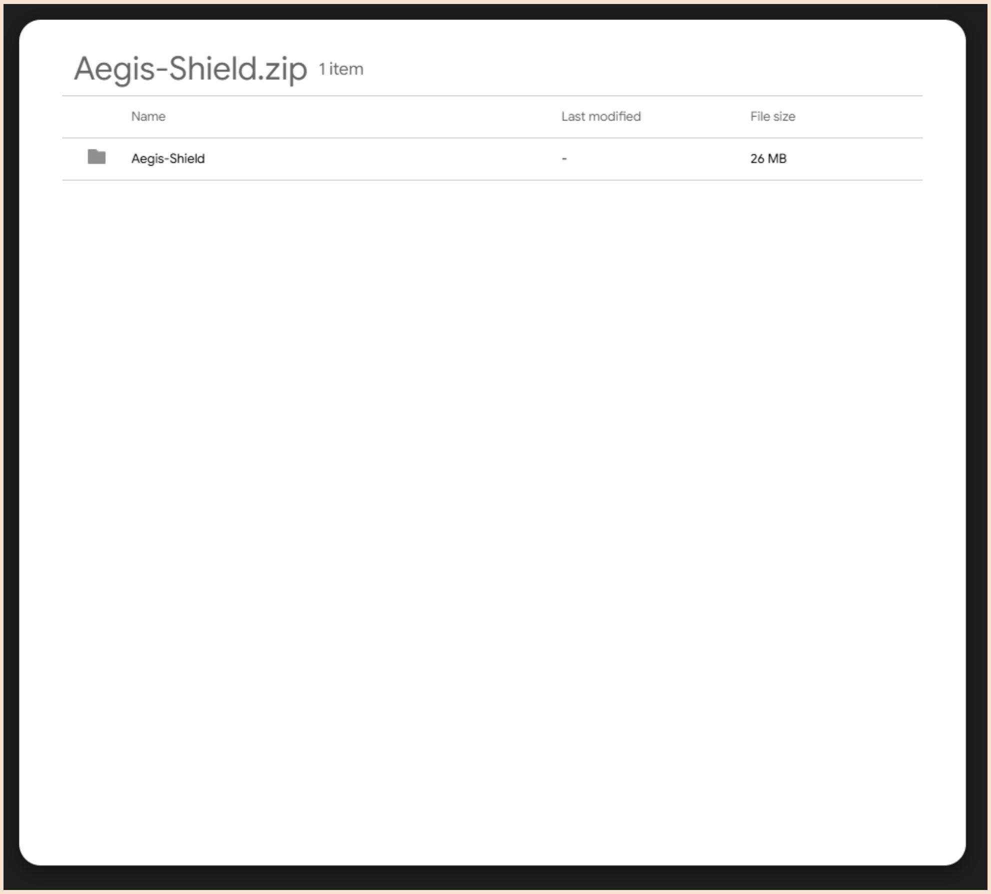
## Step 1: Download and Load the Extension

**1.Download the Extension**

Use the following link to directly download the extension package:

https://drive.google.com/file/d/11j5r2mvqBWo93WosYblIHNkwJgG7ea9I/view?usp=sharing

After loading to this page with this interface click download

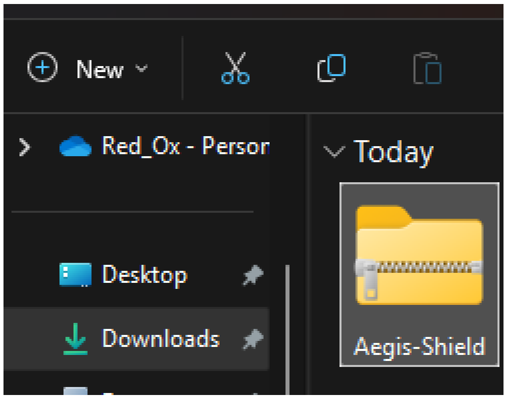


Aegis-Shield.zip 1 item

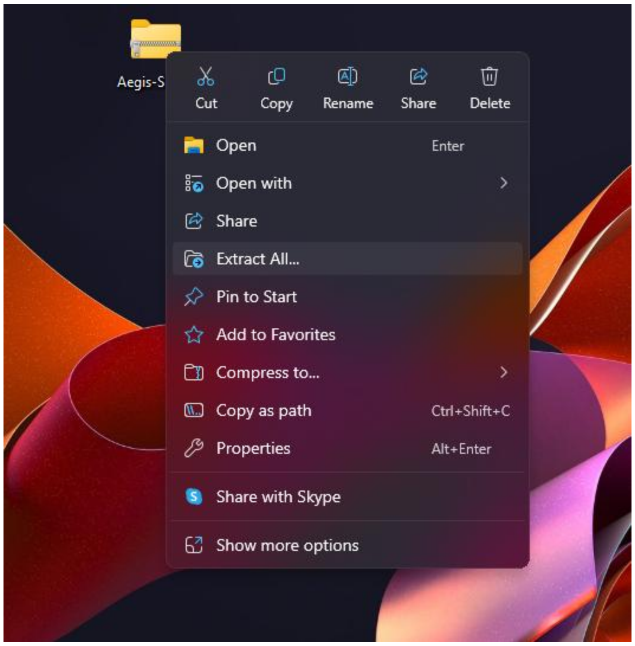
| Name | Last modified | File size |
|---|---|---|
| Aegis-Shield | - | 26 MB |

## 2.Extract the Extension File

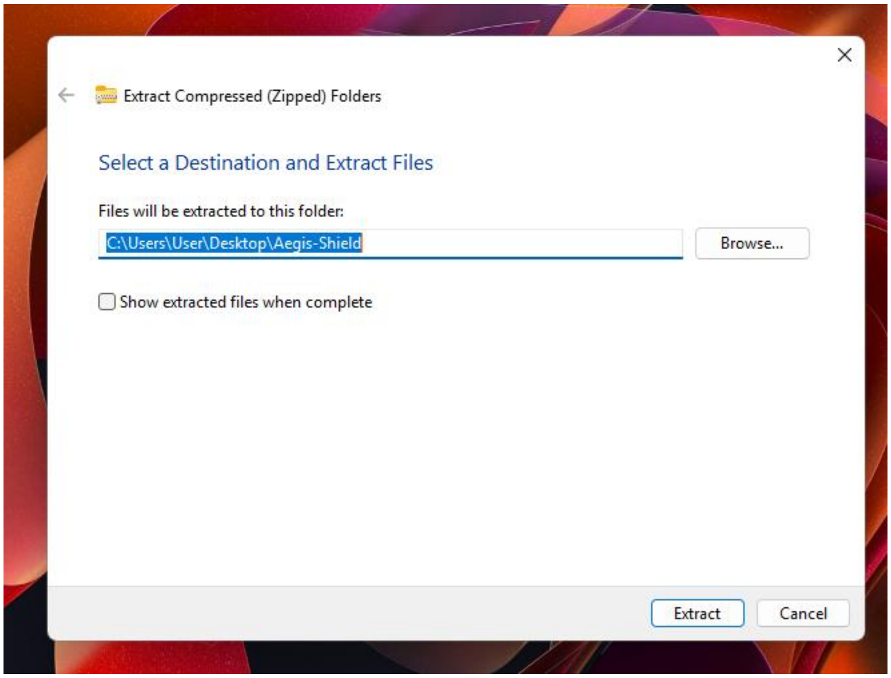
Extract the contents of the downloaded file to a convenient location on your computer. (Ex: Desktop)



1. (For further process change the directory to desktop)



2. (Select Extract all)

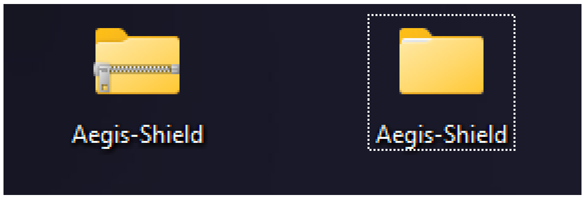

Extract Compressed (Zipped) Folders

Select a Destination and Extract Files

Files will be extracted to this folder:

C:\Users\User\Desktop\Aegis-Shield

□ Show extracted files when complete

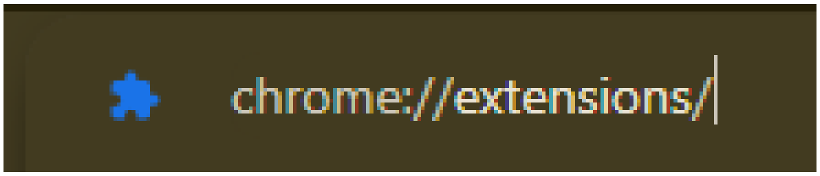


3. Select the path to extract the file

4. Extracted Folder

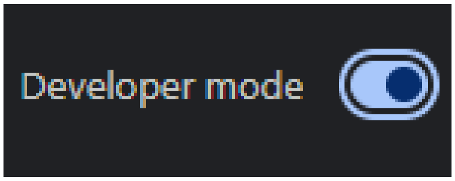
### 3.Enable Developer Mode in Chrome

Open Chrome and navigate to chrome://extensions/.



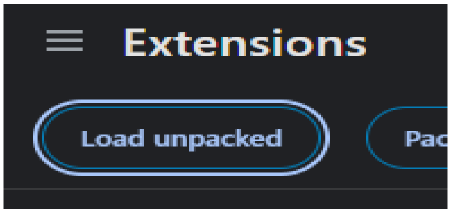
chrome://extensions/

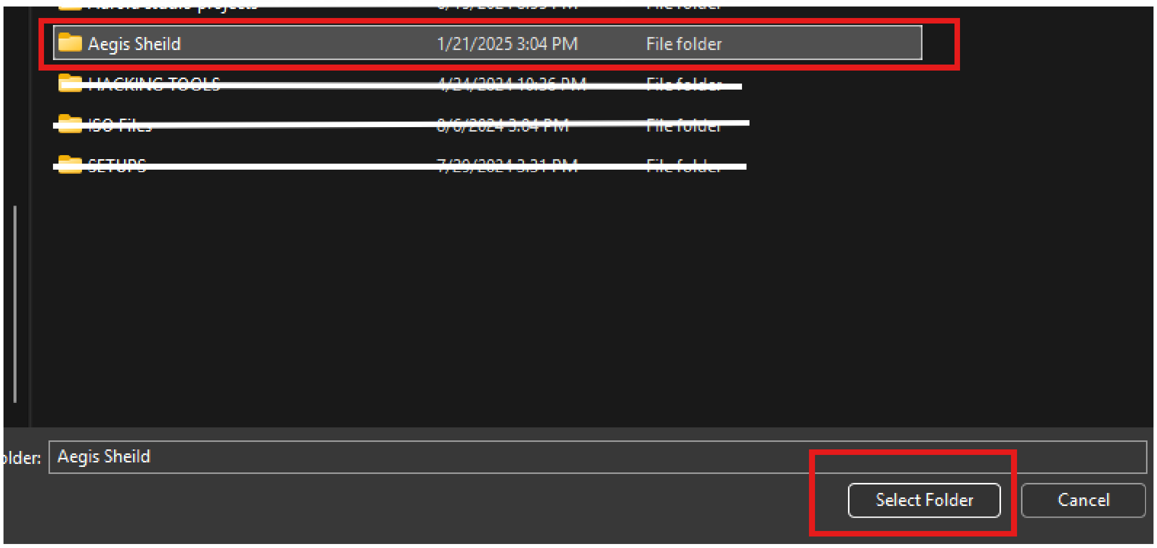
Toggle the **Developer mode** switch in the top-right corner.



### 4. Load Unpacked Extension:

Click **Load unpacked**., Select the folder where you extracted the extension files.





Aegis Sheild 1/21/2025 3:04 PM File folder

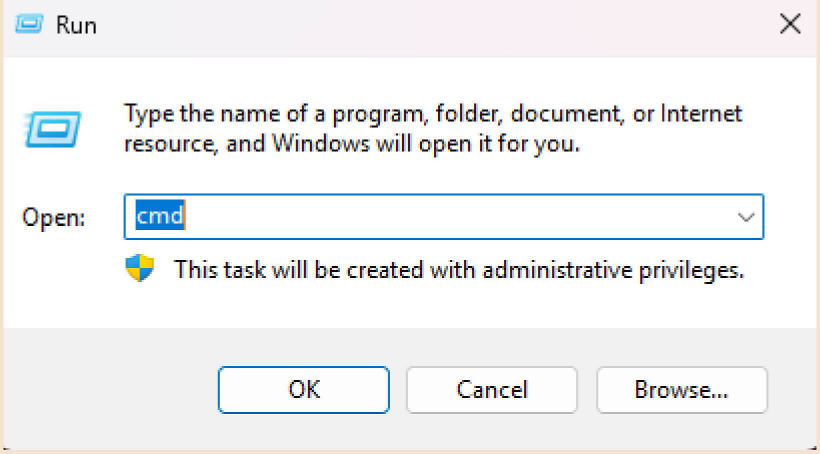
[redacted]

older: Aegis Sheild

# Step 2: Setting Up the Backend Server

## 1. Check if Python is Already Installed

Open a terminal or command prompt on your computer.



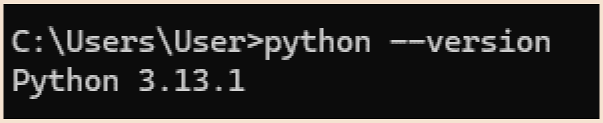
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: cmd

This task will be created with administrative privileges.

(Win + R > cmd > OK)

Type the following command and press Enter: **python --version**



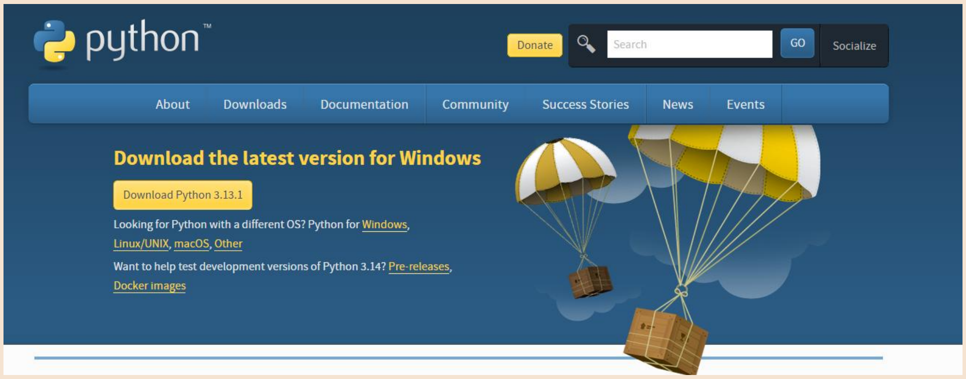
```
C:\Users\User>python --version
Python 3.13.1
```

If Python is installed, the version number will be displayed

**If Python is not installed or the version is below 3.8, proceed to the next step to download and install it.**

## 1.1. Ensure Python is Installed

Download Python from [python.org](python.org)



Download the latest version for Windows

Looking for Python with a different OS? Python for Windows, Linux/UNIX, macOS, Other

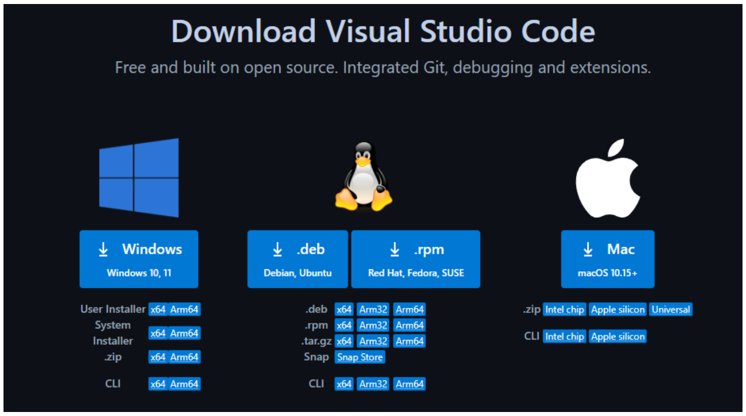
Want to help test development versions of Python 3.14? Pre-releases, Docker images

During installation, ensure you check the box to add Python to the system PATH.

After ensuring Python is installed, follow these steps to set up the backend for the "Aegis Shield - Phishing Detection Extension"

## 2. Install Visual Studio Code (VS Code)

Download and install VS Code from code.visualstudio.com.

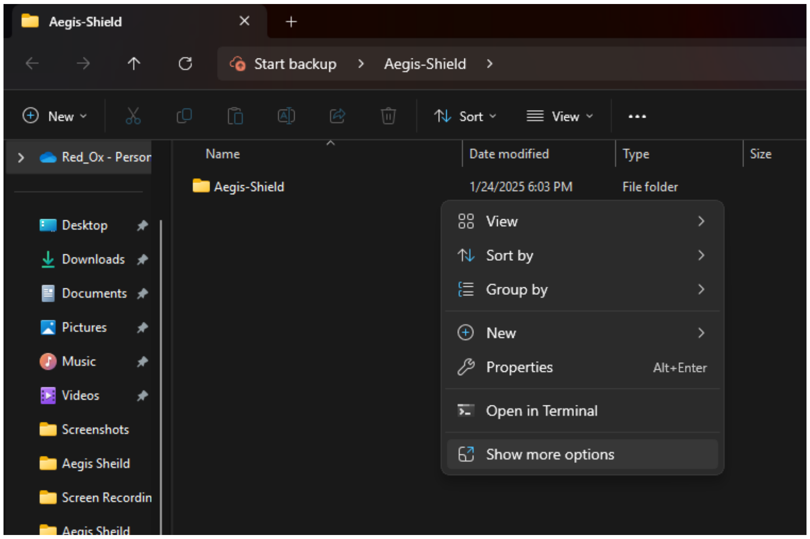


Download Visual Studio Code

Free and built on open source. Integrated Git, debugging and extensions.

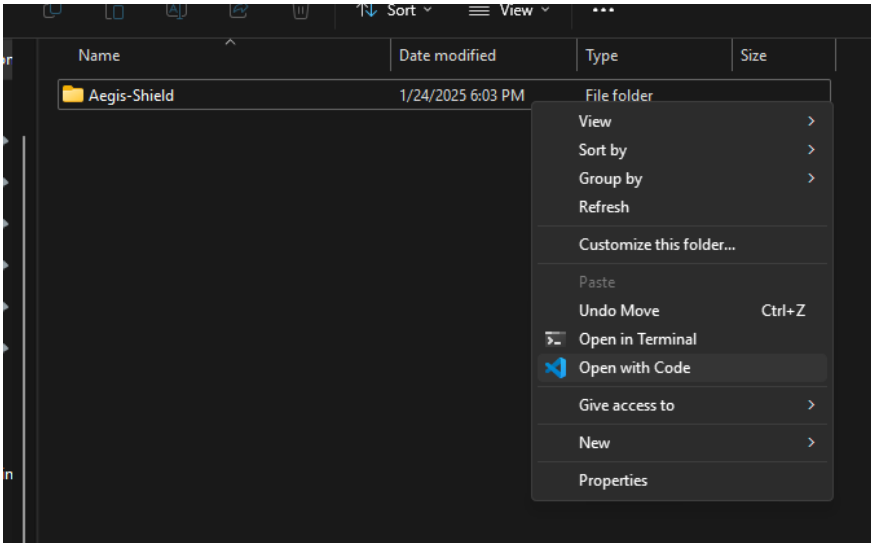
## 3. Install Required Dependencies

Load the VS Code

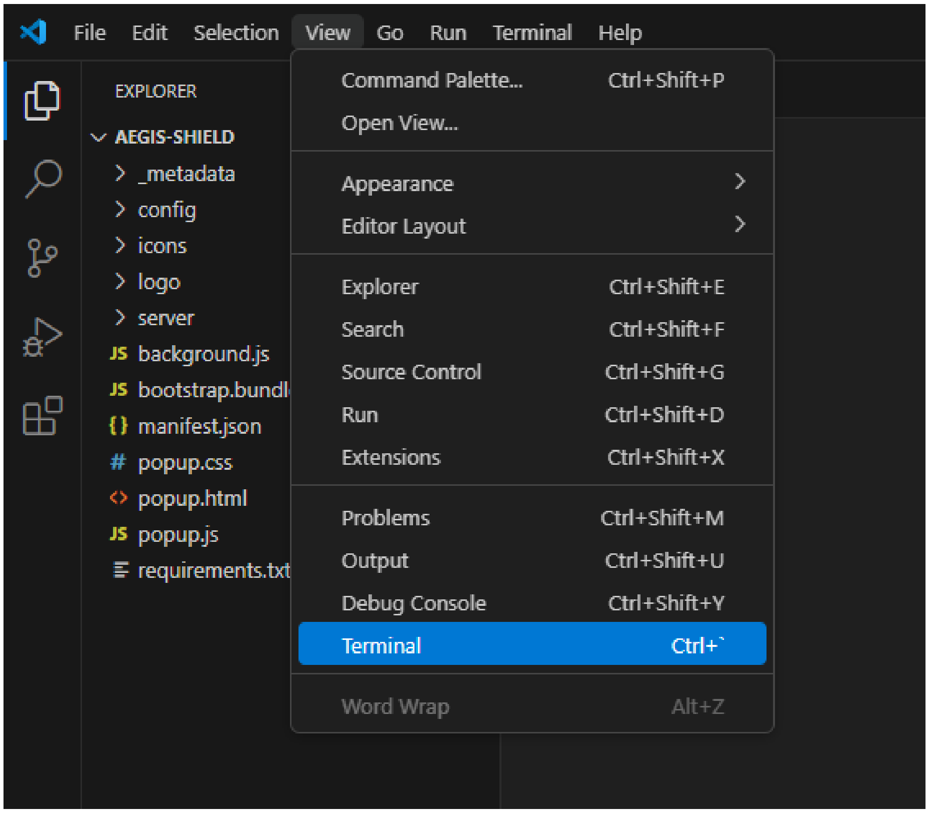


1. Double click the Aegis-Shield folder and right click the folder "Aegis Shield" and select the shore more options

6. select the "Open with code"



Open a terminal in VS Code.

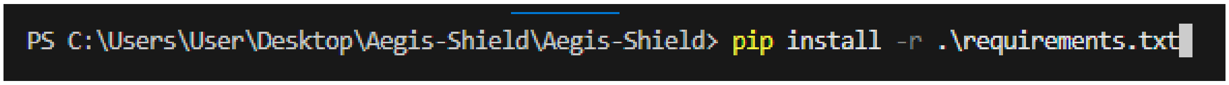


Open the terminal by selecting **View > Terminal** or using the shortcut `Ctrl+``.

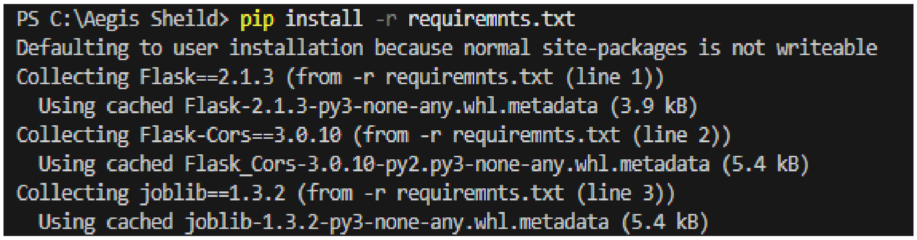
Ensure the terminal path matches the project folder. If it does not, navigate to the correct directory using:
**cd /path/to/your/project**

Run the following command to install all necessary libraries.

**pip install -r requirements.txt**



```
PS C:\Users\User\Desktop\Aegis-Shield\Aegis-Shield> pip install -r .\requirements.txt
```

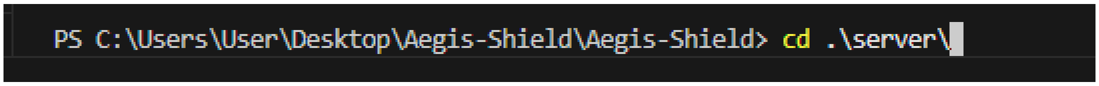


```
PS C:\Aegis Sheild> pip install -r requiremnts.txt
Defaulting to user installation because normal site-packages is not writeable
Collecting Flask==2.1.3 (from -r requiremnts.txt (line 1))
  Using cached Flask-2.1.3-py3-none-any.whl.metadata (3.9 kB)
Collecting Flask-Cors==3.0.10 (from -r requiremnts.txt (line 2))
  Using cached Flask_Cors-3.0.10-py2.py3-none-any.whl.metadata (5.4 kB)
Collecting joblib==1.3.2 (from -r requiremnts.txt (line 3))
  Using cached joblib-1.3.2-py3-none-any.whl.metadata (5.4 kB)
```

## 4. Run the Flask Backend Server

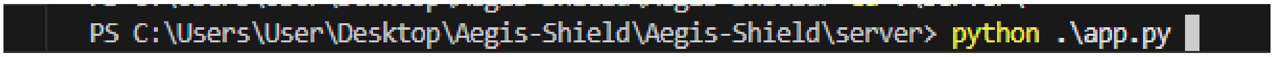
In the terminal, execute the following command **python app.py**

1. Direct the Path into server folder



```
PS C:\Users\User\Desktop\Aegis-Shield\Aegis-Shield> cd .\server\
```

2. Run the server



```
PS C:\Users\User\Desktop\Aegis-Shield\Aegis-Shield\server> python .\app.py
```

Ensure the server is running and accessible at http://127.0.0.1:5000/

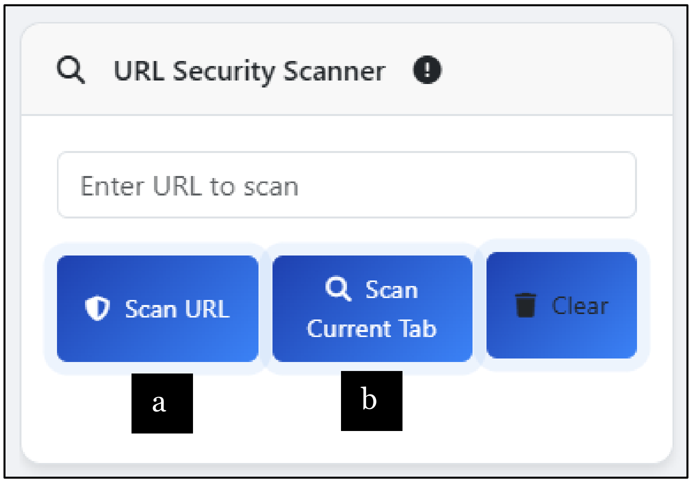
**You can refer to the following demo video for a detailed walkthrough of the installation process and to gain a better understanding of how to set up the extension.**

Click here: Demo Video

Welcome to the Aegis Shield Phishing Detector de

# Using the Extension

1. **Real-Time URL Monitoring**



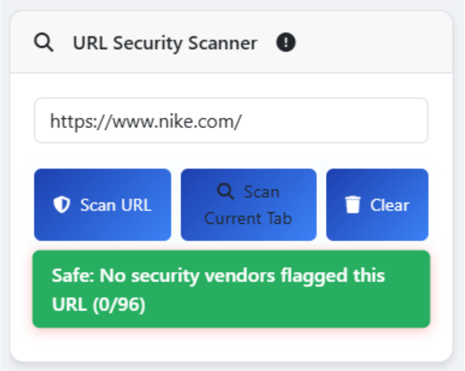
The extension continuously monitors the URLs you visit in your browser.

Threat levels are categorized as:

| 🟩 | 🟥 |
|---|---|
| **Safe** | **Malicious** |
| - | alert with recommendations to block access |

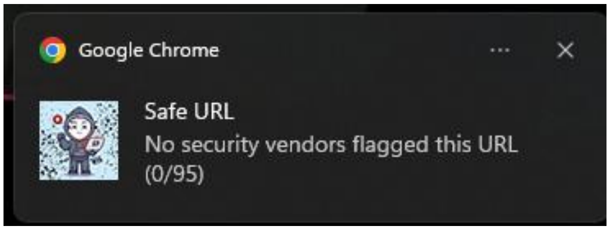
a. **Manual URL Scan -** Paste a URL into the input field within the popup, Click the **Scan URL** button to analyze the entered

b. Scan Current Tab – Click the **Scan Current Tab** button in the popup interface, the extension scans the active tab and displays the safety status.

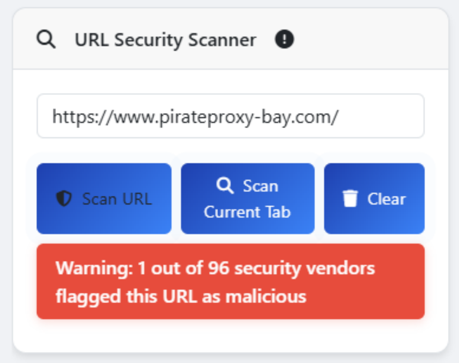


https://www.nike.com/

Safe: No security vendors flagged this URL (0/96)

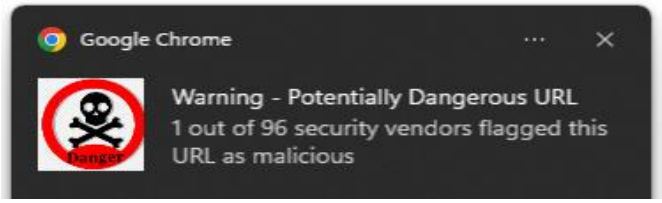


Safe URL
No security vendors flagged this URL (0/95)



https://www.pirateproxy-bay.com/

Warning: 1 out of 96 security vendors flagged this URL as malicious



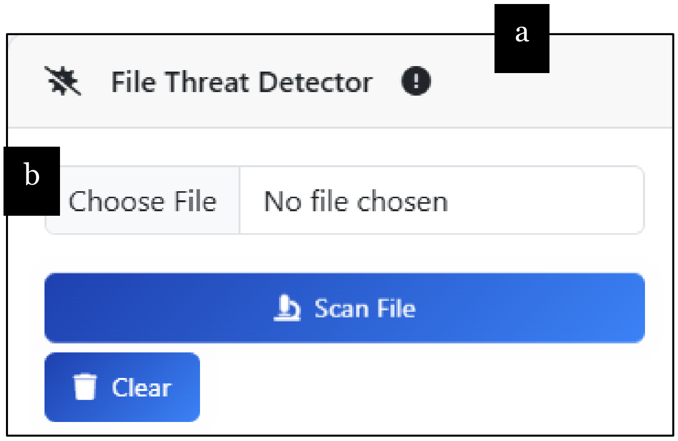
Warning - Potentially Dangerous URL
1 out of 96 security vendors flagged this URL as malicious

## 2. File Threat Detector

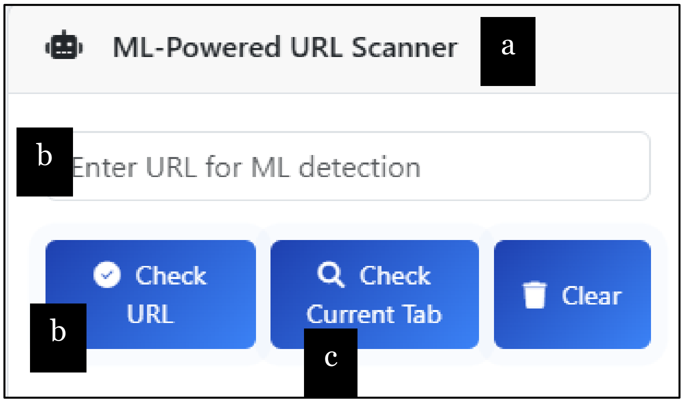
a. Navigate to the **File Scanner** section in the popup.

b. Click the **Choose File** button to select the file you want to analyze.

The system will evaluate the file for potential threats and display the results in the interface.



No file chosen



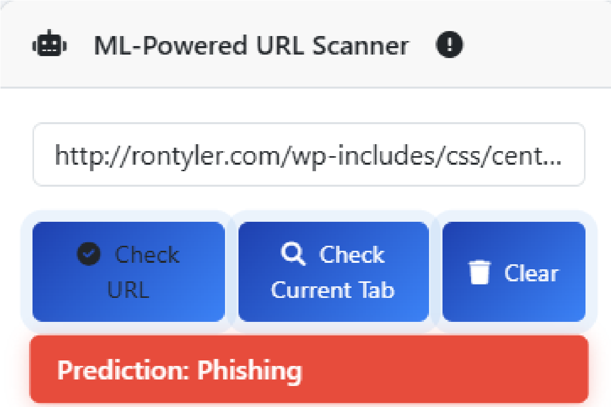
## 3. ML-Powered URL Scanner

a. Navigate to the **ML URL Scanner** section in the popup.

b. Paste the URL to be analyzed and click **Check URL**

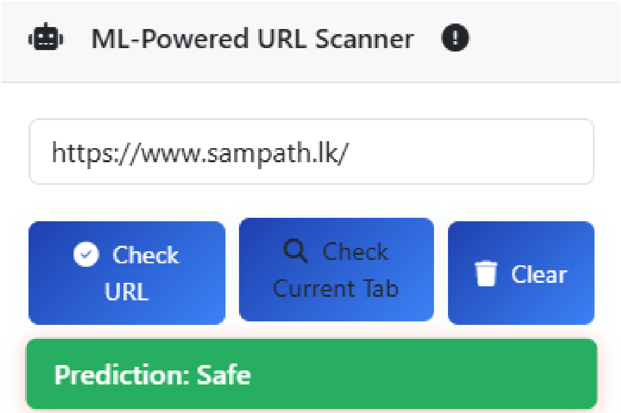
c. **Scan Current Tab** button in the popup interface, the extension scans the active tab and displays the safety status.

The scanner uses advanced machine learning techniques to determine whether the URL is malicious.



http://rontyler.com/wp-includes/css/cent...

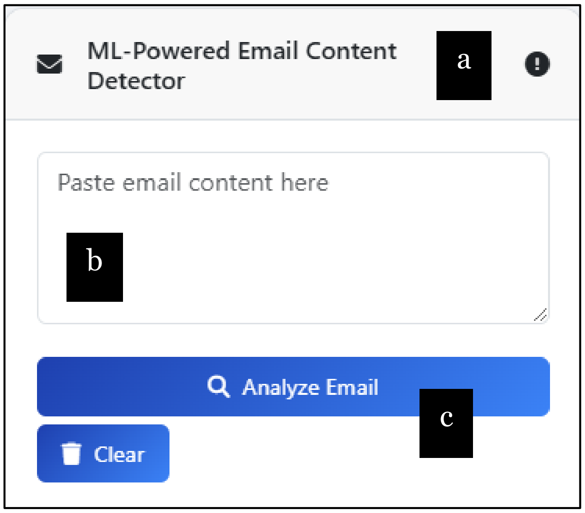
Prediction: Phishing



https://www.sampath.lk/

Prediction: Safe

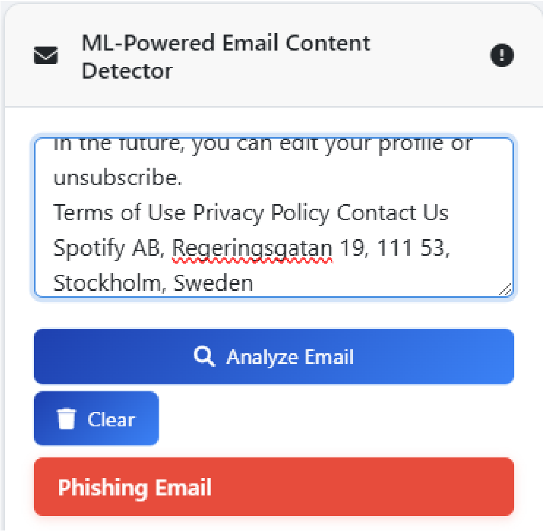
## 4. Email Phishing Detection



a. Navigate to the **Email Content Detector** section in the popup.

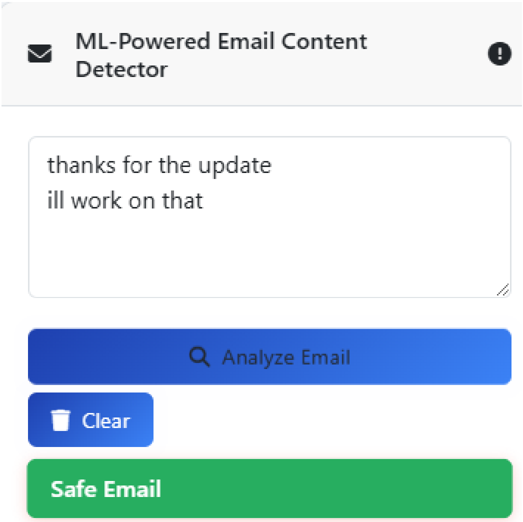
b. Paste the email text or header into the provided text box.

c. Click **Analyze Email** to check for potential phishing indicators.



In the future, you can edit your profile or unsubscribe.
Terms of Use Privacy Policy Contact Us
Spotify AB, Regeringsgatan 19, 111 53, Stockholm, Sweden

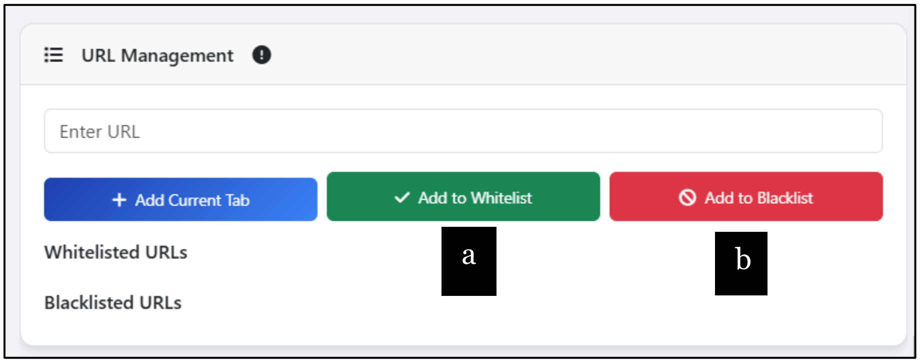
Phishing Email



thanks for the update
ill work on that

Safe Email

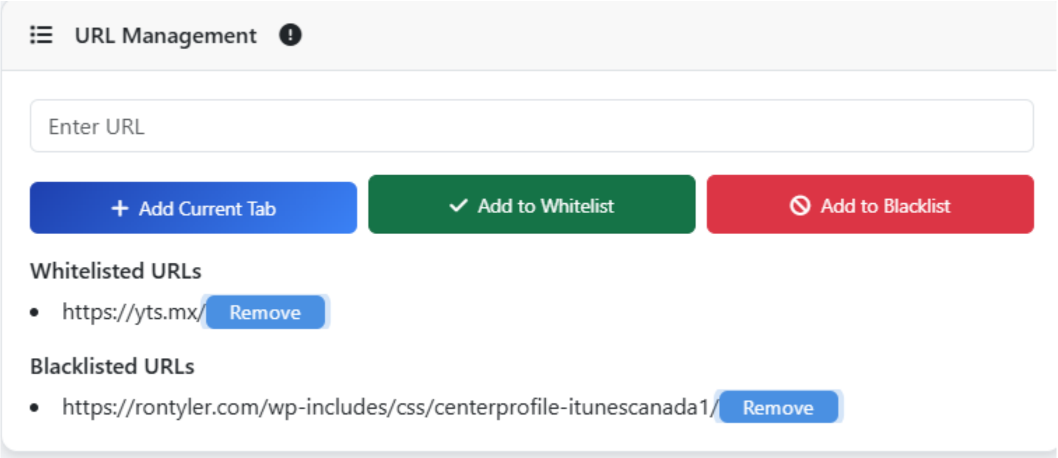
## 5. Whitelist/Blacklist Management



**a. Add to Whitelist** - Use the whitelist feature to mark trusted URLs and bypass analysis.

**b. Add to Blacklist** - Block specific URLs by adding them to the blacklist.

Manage whitelist and blacklist entries from the popup interface.



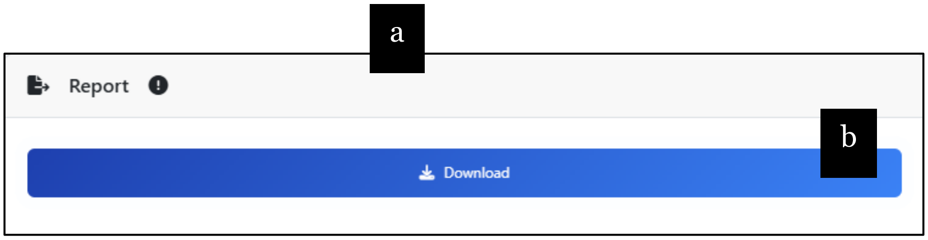
Whitelisted URLs

- https://yts.mx/ Remove

Blacklisted URLs

- https://rontyler.com/wp-includes/css/centerprofile-itunescanada1/ Remove

## 6. Report



a. Navigate to the Reports section in the extension popup.

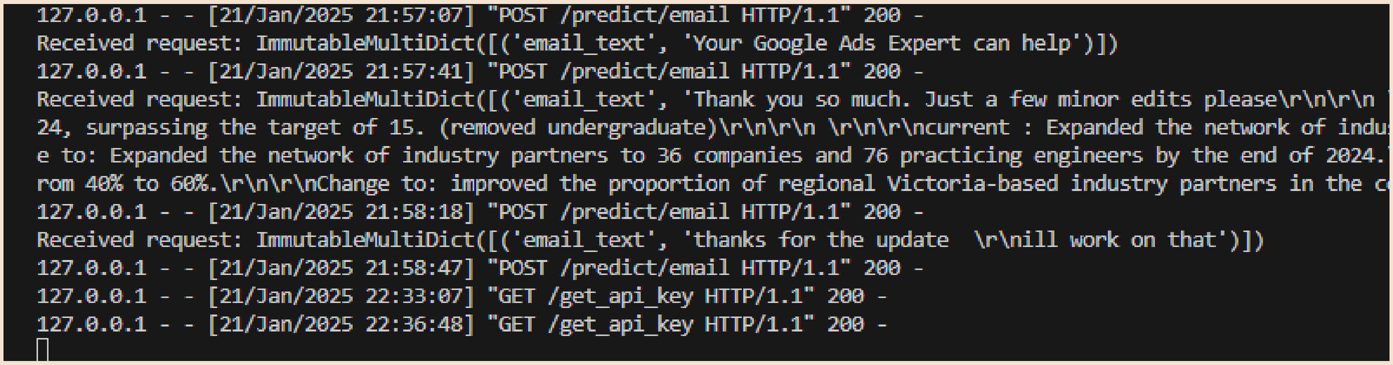
b. Click Download Report to save the report as a .csv file.

# Troubleshooting

## Common Issues

### *Backend Server Not Running*

Ensure **app.py** is running without errors. Check the terminal or console for any specific error messages and resolve them accordingly.



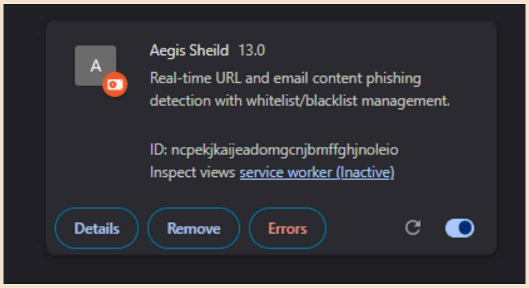
```
127.0.0.1 - - [21/Jan/2025 21:57:07] "POST /predict/email HTTP/1.1" 200 -
Received request: ImmutableMultiDict([('email_text', 'Your Google Ads Expert can help')])
127.0.0.1 - - [21/Jan/2025 21:57:41] "POST /predict/email HTTP/1.1" 200 -
Received request: ImmutableMultiDict([('email_text', 'Thank you so much. Just a few minor edits please\r\n\r\n
24, surpassing the target of 15. (removed undergraduate)\r\n\r\n \r\n\r\ncurrent : Expanded the network of indu
e to: Expanded the network of industry partners to 36 companies and 76 practicing engineers by the end of 2024.
rom 40% to 60%.\r\n\r\nChange to: improved the proportion of regional Victoria-based industry partners in the c
127.0.0.1 - - [21/Jan/2025 21:58:18] "POST /predict/email HTTP/1.1" 200 -
Received request: ImmutableMultiDict([('email_text', 'thanks for the update  \r\nill work on that')])
127.0.0.1 - - [21/Jan/2025 21:58:47] "POST /predict/email HTTP/1.1" 200 -
127.0.0.1 - - [21/Jan/2025 22:33:07] "GET /get_api_key HTTP/1.1" 200 -
127.0.0.1 - - [21/Jan/2025 22:36:48] "GET /get_api_key HTTP/1.1" 200 -
```

Verify that Python and required dependencies are installed correctly. If necessary, re-run the command:

pip install -r requirements.txt

### *Extension Not Loading*

Ensure Developer Mode is enabled in Chrome by navigating to **chrome://extensions/** and toggling the switch in the top-right corner.



Aegis Sheild 13.0

Real-time URL and email content phishing detection with whitelist/blacklist management.

ID: ncpekjkaijeadomgcnjbmffghjnoleio

Inspect views service worker (Inactive)

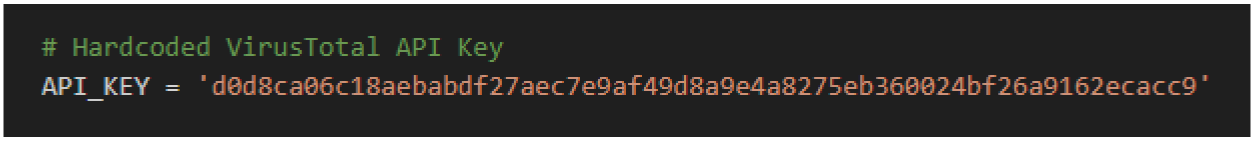
Verify that the correct folder containing the extracted extension files is selected during the load process.

Check for any errors in the Chrome Developer Console under the Extensions tab.

## *API Errors*

Check your internet connection and ensure it is stable.

Verify that the VirusTotal API key is configured correctly in the backend by reviewing the **app.py** file.



```
# Hardcoded VirusTotal API Key
API_KEY = 'd0d8ca06c18aebabdf27aec7e9af49d8a9e4a8275eb360024bf26a9162ecacc9'
```

If the API rate limit is exceeded, wait for a reset period or use a different API key.

## *Contact Support*

For persistent issues, collect relevant logs or screenshots and contact the development team. Provide details such as:

Exact error messages encountered.

Steps to reproduce the issue.

Logs from the terminal or browser console.

You can reach the team via the following emails:

- SPULLAPE@our.ecu.edu.au
- TELVITIG@our.ecu.edu.au
- dwalgama@our.ecu.edu.au
- PTGUNASE@our.ecu.edu.au

# Security and Privacy

**Data Processing:** All user data is processed securely and never stored persistently. Temporary data is cleared immediately after analysis to minimize the risk of unauthorized access. The extension employs strict security protocols to ensure sensitive information is protected throughout its lifecycle.

**Encrypted Communication:** All API requests are secured using HTTPS protocols, providing end-to-end encryption for data transmission. This ensures that any data exchanged between the extension and external services, such as VirusTotal, remains confidential and secure from interception or tampering.

**Local Storage:** User preferences and settings, such as whitelists and blacklists, are stored locally within the browser. This local-only storage method prevents external entities from accessing these settings, further enhancing privacy and security.

**No Tracking:** The extension does not monitor, record, or share user activity or browsing behavior beyond its intended functionality. This commitment to non-tracking ensures that users can browse with confidence, knowing their actions are private and not being monitored.

**Privacy Compliance:** The extension adheres to international privacy standards and guidelines, ensuring that user data is handled in accordance with regulations such as GDPR (General Data Protection Regulation) where applicable.

**Regular Audits:** The extension undergoes periodic security reviews and updates to ensure it remains compliant with the latest security best practices and addresses potential vulnerabilities proactively.

**Data Processing:** All user data is processed securely and never stored persistently. Temporary data is cleared immediately after analysis.

**Encrypted Communication:** All API requests are secured using HTTPS protocols to protect data during transmission.

**Local Storage:** User preferences and settings, such as whitelists and blacklists, are stored locally in the browser for enhanced privacy.

**No Tracking:** The extension does not track user activity or behavior beyond its core functionality, ensuring complete user confidentiality.

.

# Acknowledgments

**The success of the Aegis Shield Phishing Detection Extension would not have been possible without the invaluable contributions of key resources and dedicated efforts. The integration of the VirusTotal API has been instrumental in enabling real-time threat analysis and enhancing the security capabilities of the extension. The development team has worked tirelessly to ensure the extension delivers reliable, up-to-date protection against phishing and malware threats, showcasing their commitment to user safety and cybersecurity excellence.**

**Development Team: The team is dedicated to maintaining and improving the Aegis Shield extension to provide reliable, up-to-date protection against phishing and malware threats**