**Project Title**

**Detection of Phishing Links on Web Applications Using AI**

**✅ Step-by-Step Setup Guide**

**🔧 Step 1: Install Python**

1. Go to: <https://www.python.org/downloads>
2. Download the latest **Python 3.x**
3. Run the installer, and **CHECK this box**:

pgsql

CopyEdit

✅ Add Python to PATH

1. Click **Install Now**

**📦 Step 2: Unzip the Project Files**

1. Extract the ZIP file: phishing-detector-project.zip
2. You’ll get a folder like:

CopyEdit

phishing-detector-project

**💻 Step 3: Open CMD or Terminal in That Folder**

1. Go into the folder in File Explorer
2. Type cmd in the folder path bar and press **Enter**
3. Now you're inside the project directory

**📥 Step 4: Install Required Packages**

In Command Prompt, run:

bash

CopyEdit

pip install -r requirements.txt

✅ This installs:

* Flask
* Scikit-learn
* Pandas
* Joblib

**🧠 Step 5: Train the AI Model**

Run:

bash

CopyEdit

python train\_model.py

This will:

* Read dataset.csv
* Extract features
* Train a Random Forest model
* Save it as phishing\_model.pkl

✅ You only need to do this **once**, or when adding more data.

**🚀 Step 6: Run the Web App**

Run:

bash

CopyEdit

python app.py

Then open your browser and visit:

cpp

CopyEdit

http://127.0.0.1:5000

✅ Enter any URL to check if it's phishing or safe.

**➕ How to Add More Sample URLs**

**🔄 Step 1: Open dataset.csv**

* Use Excel or any text editor.
* Format:

csv

CopyEdit

url,label

http://example.com,0

http://phishy-site.ru/login,1

Where:

* 0 = Safe
* 1 = Phishing

✅ Add as many rows as you want.

**🔄 Step 2: Retrain the Model**

After updating dataset.csv, run:

bash

CopyEdit

python train\_model.py

✅ This updates the phishing\_model.pkl with the new data.

**📌 Summary**

| **Step** | **Command** |
| --- | --- |
| Install packages | pip install -r requirements.txt |
| Train model | python train\_model.py |
| Run app | python app.py |
| Open in browser | http://127.0.0.1:5000 |