## ****Instructions to Run AI/ML Phishing Email Framework****

### ****Step 1: Activate the Environment****

Run the following command to activate the virtual environment:

# Replace 'your\_env' with the actual environment name

source your\_env/bin/activate # For Linux/macOS

your\_env\Scripts\activate # For Windows (Command Prompt)

### ****Step 2: Train the ML Models on Target Data****

Execute the following command to train the models:

python ai\_ml\_phishing\_framework.py --train-models

### ****Step 3: Analyze a Target's Vulnerability****

Run the following command to analyze a specific target (change the target index as needed):

python ai\_ml\_phishing\_framework.py --analyze-target --target-index 0

### ****Step 4: Generate a Phishing Email****

Use AI/ML components to craft a phishing email for a specific target:

python ai\_ml\_phishing\_framework.py --generate-email --target-index 0

### ****Step 5: Evaluate and Analyze the Generated Email****

Review the generated phishing email in output directory and assess its effectiveneness.