# HACKTIVATE-2k24

24th - 26th JUNE, 2024

# 1. HACKTIVATE Team Details

Problem Statement Title: **AI-Driven Phishing Bot System**

Team name : Binary Bandits

Domain: AI in Cybersecurity

Team Leader Name: Ayush Parkara

Team Member 1 : Heli Nandini

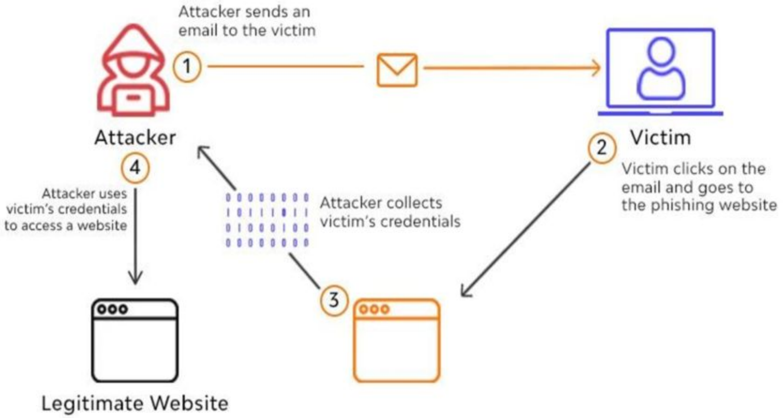
Team Member 2 : Mega Nadar

Team Member 3 : Bhavin Patel

# 2. Our Solution

1. **Reconnaissance and Campaign Management:** Our platform will facilitate detailed reconnaissance to gather active email addresses associated with a target domain. Users can manage campaigns through an interactive dashboard, view past campaigns, and utilize a drop-down list sorted by date. The system will **validate and filter active email addresses**, saving them in the database, with an option to manually upload email lists via CSV.
2. **Profiling and Detailed Analytics:** We provide tools for profiling identified email addresses, collecting data on various parameters such as **full name, age, job title, and social media profiles.** Users can automatically fetch additional information to build comprehensive profiles. This information will be visualized on the dashboard to help organizations understand their targets better.
3. **AI-Driven Phishing Simulations:** Our platform uses AI to generate and send realistic phishing emails, mimicking the communication style of target users. The success of these campaigns is tracked and analyzed. Additionally, AI bots (personas) are developed to simulate real user responses, allowing continuous refinement of phishing attempts until successful, enhancing the organization's preparedness against such threats.

# 3. FlowChart & Tools


Attacker sends an email to the victim
1
Attacker
Victim
2
Victim clicks on the email and goes to the phishing website
4
Attacker uses victim's credentials to access a website
Attacker collects victim's credentials
3
Legitimate Website

spaCy

matplotlib

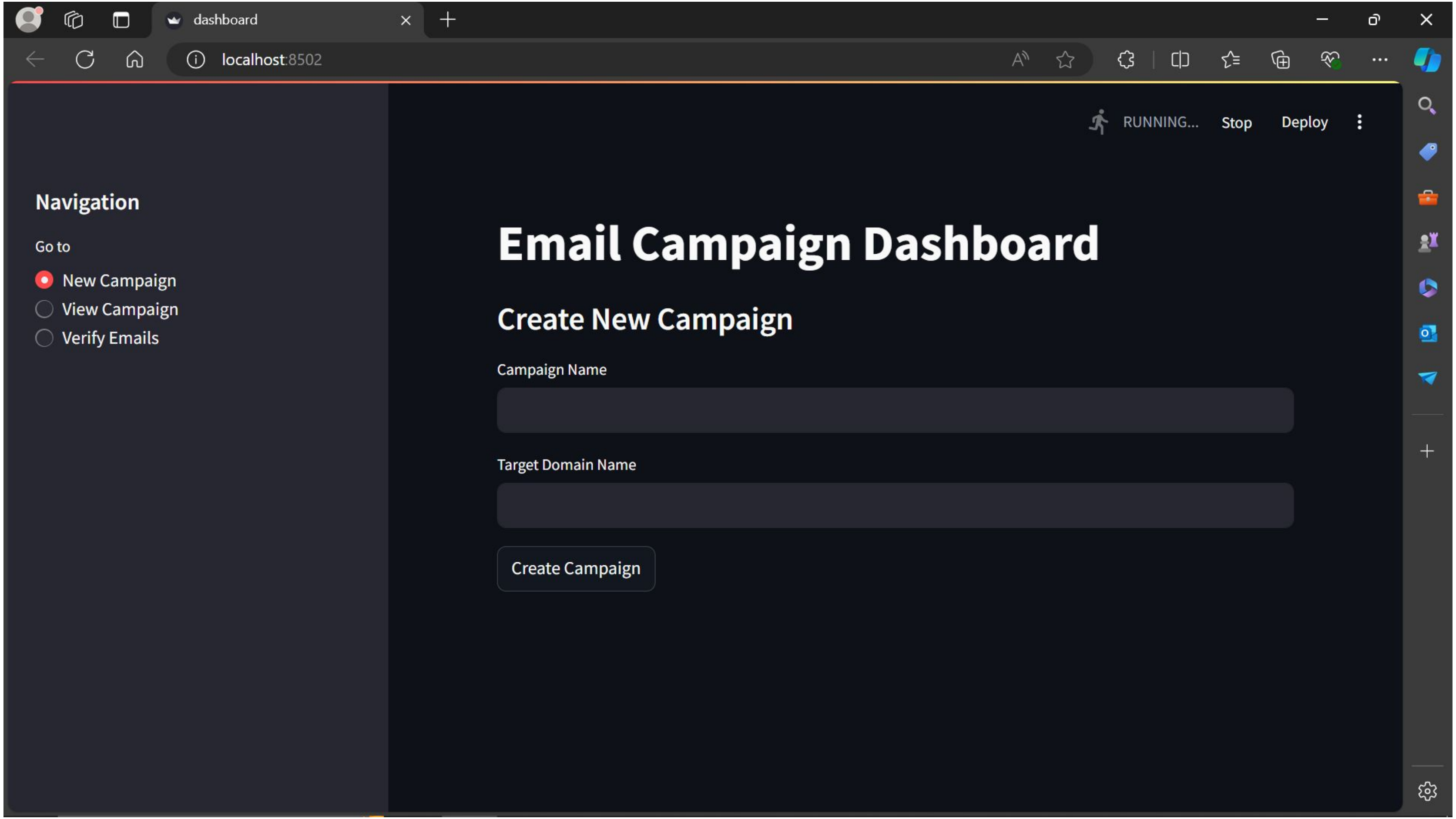
NLTK

FullContact

GENERATIVE PRE-TRAINED TRANSFORMER
GPT

Streamlit

# 3.C. Our interactive dashboard interface



Navigation

Go to

● New Campaign
○ View Campaign
○ Verify Emails

# Email Campaign Dashboard

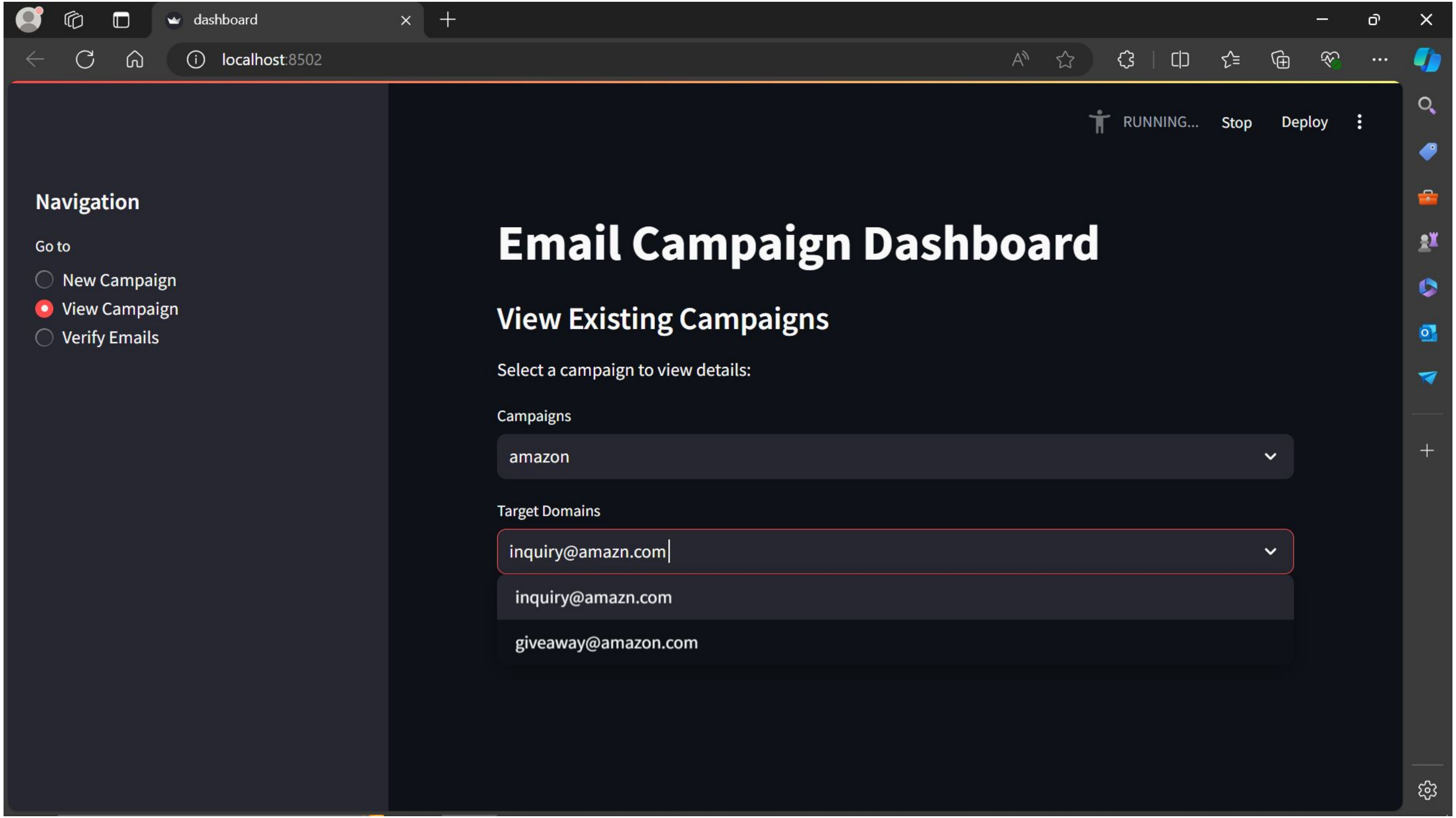
## Create New Campaign

Campaign Name

Target Domain Name

Create Campaign

# 3.D. Our interactive dashboard interface



Navigation

Go to

○ New Campaign
● View Campaign
○ Verify Emails

# Email Campaign Dashboard

## View Existing Campaigns

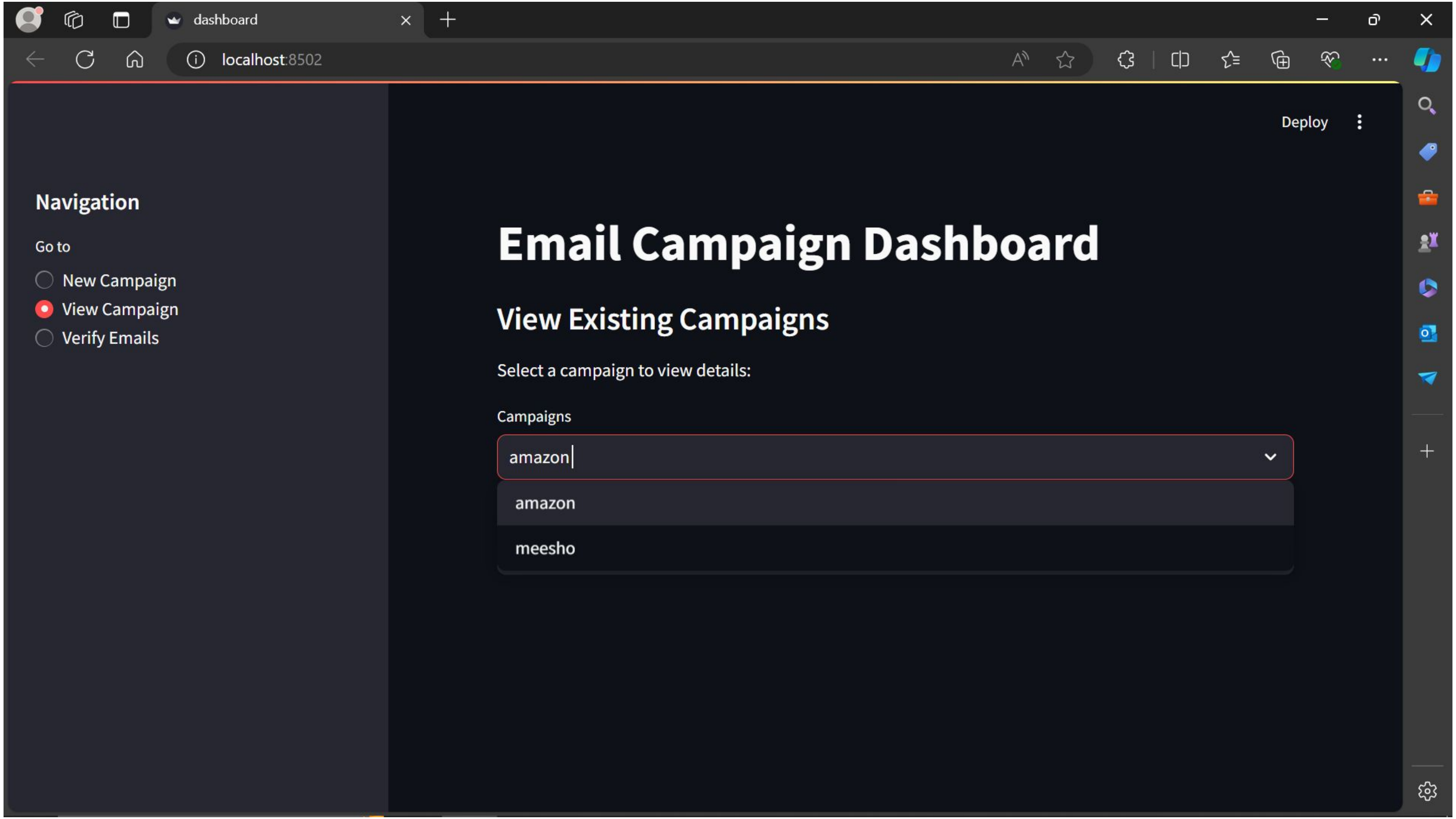
Select a campaign to view details:

Campaigns: amazon

Target Domains: inquiry@amazn.com

inquiry@amazn.com
giveaway@amazon.com

# 3.E. Our interactive dashboard interface



## Navigation

Go to

○ New Campaign
● View Campaign
○ Verify Emails

# Email Campaign Dashboard

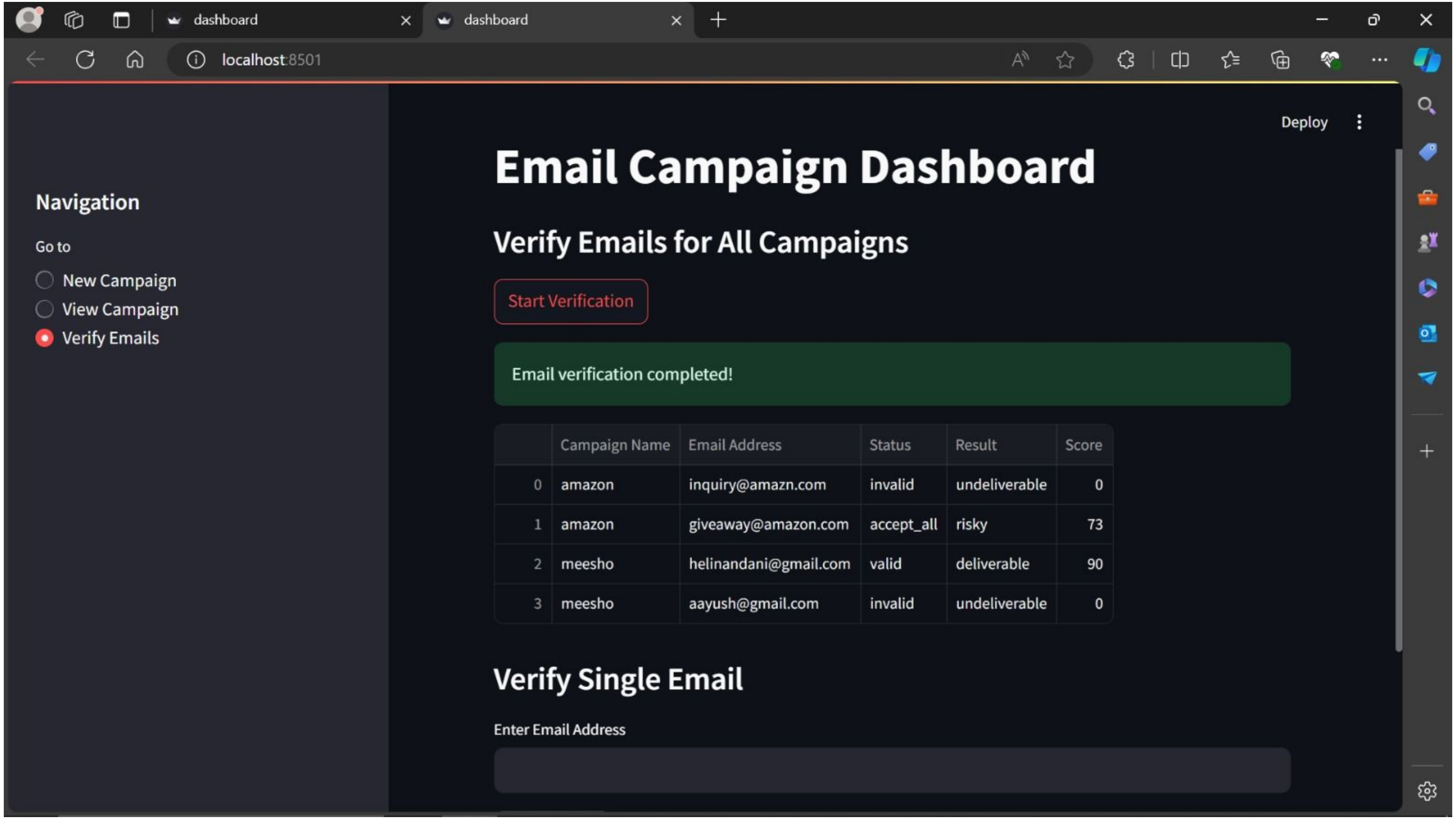
## View Existing Campaigns

Select a campaign to view details:

Campaigns

amazon

# 3.A. Our interactive dashboard interface



## Email Campaign Dashboard

### Verify Emails for All Campaigns

Email verification completed!

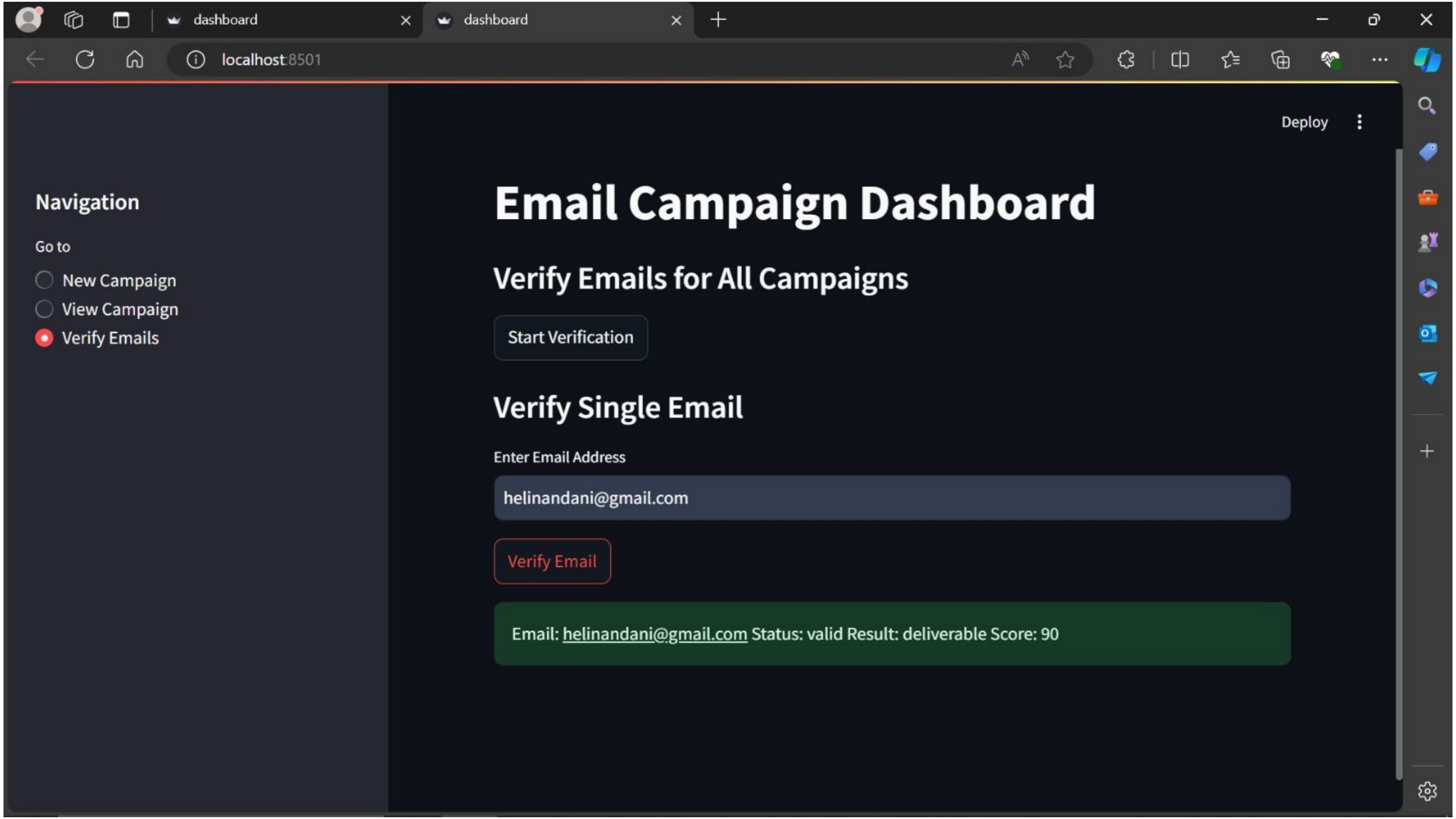
| | Campaign Name | Email Address | Status | Result | Score |
|---|---|---|---|---|---|
| 0 | amazon | inquiry@amazn.com | invalid | undeliverable | 0 |
| 1 | amazon | giveaway@amazon.com | accept_all | risky | 73 |
| 2 | meesho | helinandani@gmail.com | valid | deliverable | 90 |
| 3 | meesho | aayush@gmail.com | invalid | undeliverable | 0 |

### Verify Single Email

Enter Email Address

List of all the verified emails, along with their scores

# 3.B. Our interactive dashboard interface



## Email Campaign Dashboard

### Verify Emails for All Campaigns

### Verify Single Email

Enter Email Address

helinandani@gmail.com

Email: helinandani@gmail.com Status: valid Result: deliverable Score: 90

# 4. AI-Driven Phishing Email Generation

**Dataset:**

- The dataset consists of 60,000 rows, each containing email IDs and the entire email content including the sender (from), recipient (to), and subject.

**Preprocessing:**

- The dataset was preprocessed by converting all text to lowercase and removing special characters.
- Tokenization was performed to break down the text into individual words using a tokenizer.

**LSTM Model:**

- An LSTM (Long Short-Term Memory) model was trained on the preprocessed data for sequence learning.

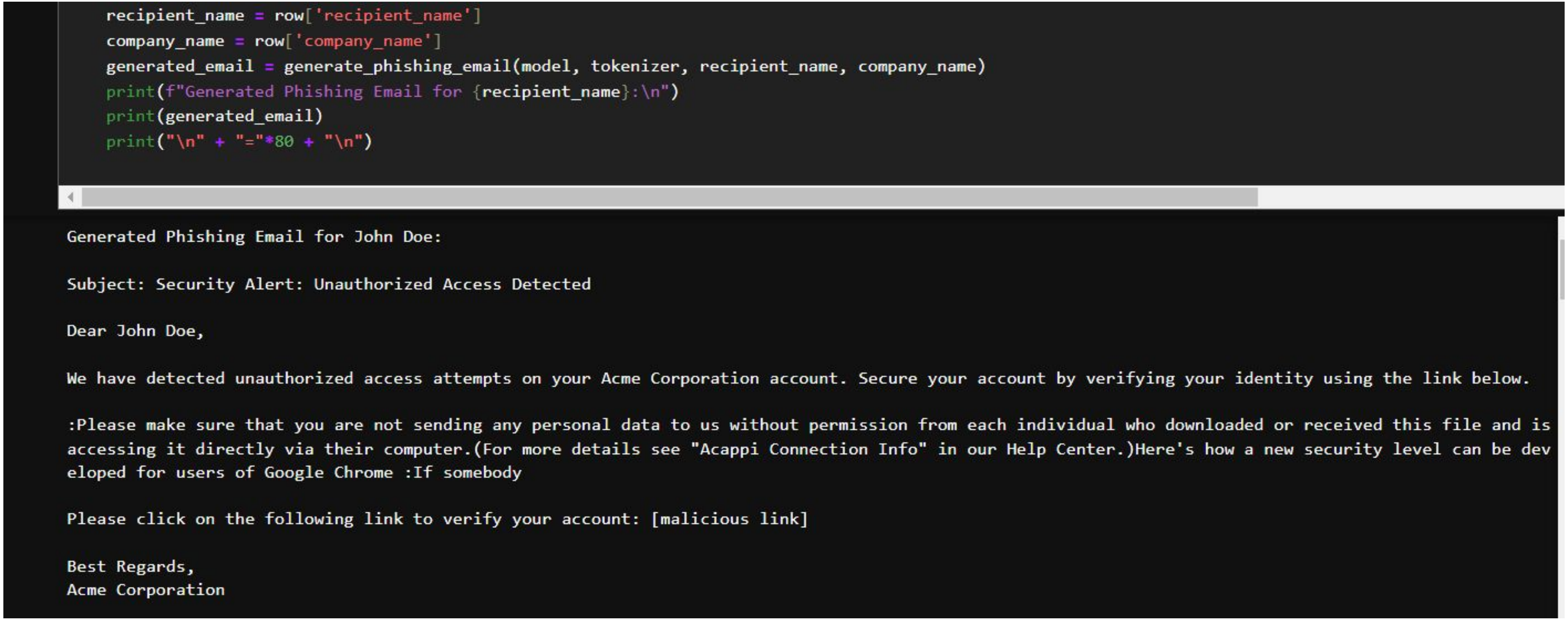
**GPT-2 Model:**

- A pretrained GPT-2 model was used for email generation based on the features extracted from the dataset.

**Automation Script:**

- A Python script was created to automate the process of sending generated emails.
- Bots were utilized to send the generated emails to the specified targets.

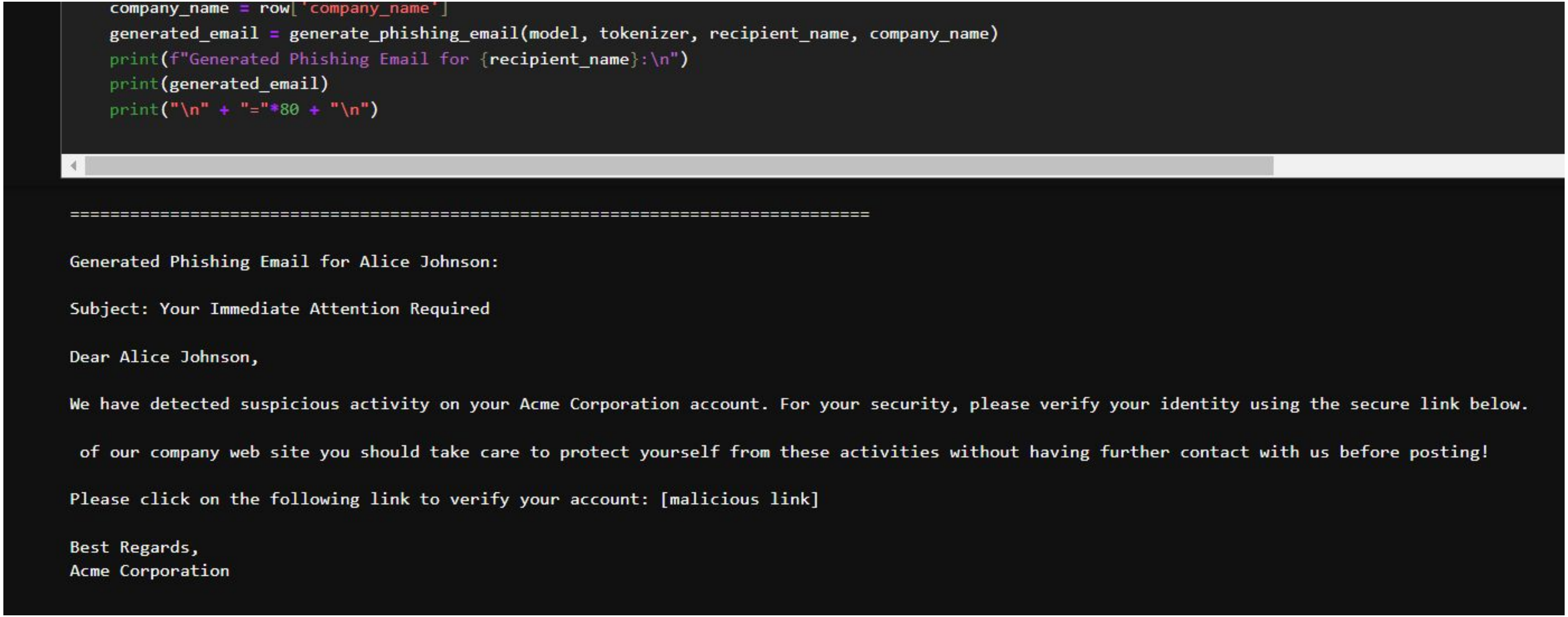
# 4.A  AI-Driven Phishing Email Generation



```
    recipient_name = row['recipient_name']
    company_name = row['company_name']
    generated_email = generate_phishing_email(model, tokenizer, recipient_name, company_name)
    print(f"Generated Phishing Email for {recipient_name}:\n")
    print(generated_email)
    print("\n" + "="*80 + "\n")
```

```
Generated Phishing Email for John Doe:

Subject: Security Alert: Unauthorized Access Detected

Dear John Doe,

We have detected unauthorized access attempts on your Acme Corporation account. Secure your account by verifying your identity using the link below.

:Please make sure that you are not sending any personal data to us without permission from each individual who downloaded or received this file and is
accessing it directly via their computer.(For more details see "Acappi Connection Info" in our Help Center.)Here's how a new security level can be dev
eloped for users of Google Chrome :If somebody

Please click on the following link to verify your account: [malicious link]

Best Regards,
Acme Corporation
```

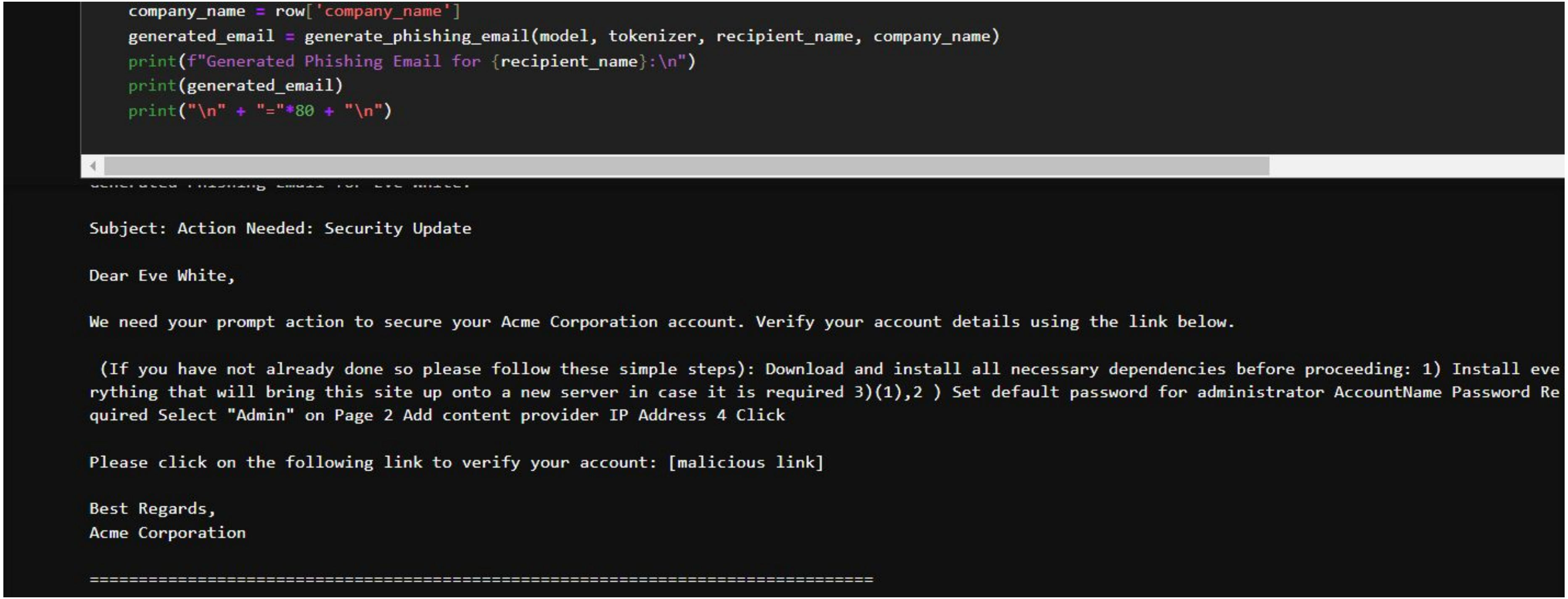
# 4.B  AI-Driven Phishing Email Generation



```python
    company_name = row['company_name']
    generated_email = generate_phishing_email(model, tokenizer, recipient_name, company_name)
    print(f"Generated Phishing Email for {recipient_name}:\n")
    print(generated_email)
    print("\n" + "="*80 + "\n")
```

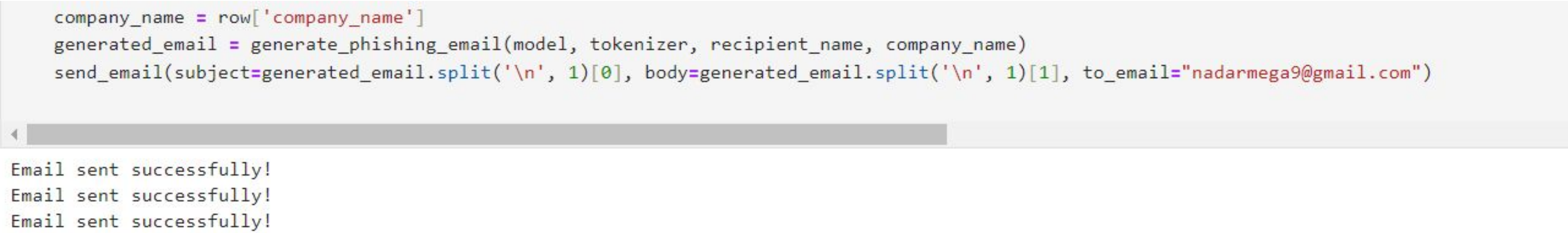
```
================================================================================

Generated Phishing Email for Alice Johnson:

Subject: Your Immediate Attention Required

Dear Alice Johnson,

We have detected suspicious activity on your Acme Corporation account. For your security, please verify your identity using the secure link below.

 of our company web site you should take care to protect yourself from these activities without having further contact with us before posting!

Please click on the following link to verify your account: [malicious link]

Best Regards,
Acme Corporation
```

# 4.B  AI-Driven Phishing Email Generation



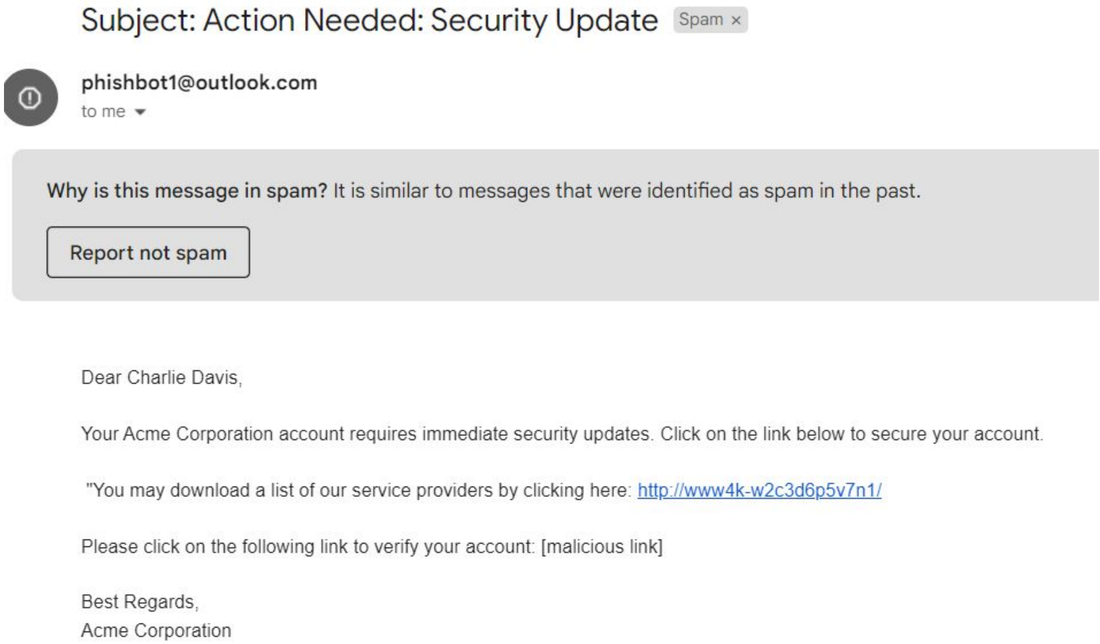
```python
    company_name = row['company_name']
    generated_email = generate_phishing_email(model, tokenizer, recipient_name, company_name)
    print(f"Generated Phishing Email for {recipient_name}:\n")
    print(generated_email)
    print("\n" + "="*80 + "\n")
```

```
Generated Phishing Email for Eve White:

Subject: Action Needed: Security Update

Dear Eve White,

We need your prompt action to secure your Acme Corporation account. Verify your account details using the link below.

 (If you have not already done so please follow these simple steps): Download and install all necessary dependencies before proceeding: 1) Install eve
rything that will bring this site up onto a new server in case it is required 3)(1),2 ) Set default password for administrator AccountName Password Re
quired Select "Admin" on Page 2 Add content provider IP Address 4 Click

Please click on the following link to verify your account: [malicious link]

Best Regards,
Acme Corporation

================================================================================
```



```
    company_name = row['company_name']
    generated_email = generate_phishing_email(model, tokenizer, recipient_name, company_name)
    send_email(subject=generated_email.split('\n', 1)[0], body=generated_email.split('\n', 1)[1], to_email="nadarmega9@gmail.com")
```

```
Email sent successfully!
Email sent successfully!
Email sent successfully!
```



Subject: Action Needed: Security Update

phishbot1@outlook.com

**Why is this message in spam?** It is similar to messages that were identified as spam in the past.

Dear Charlie Davis,

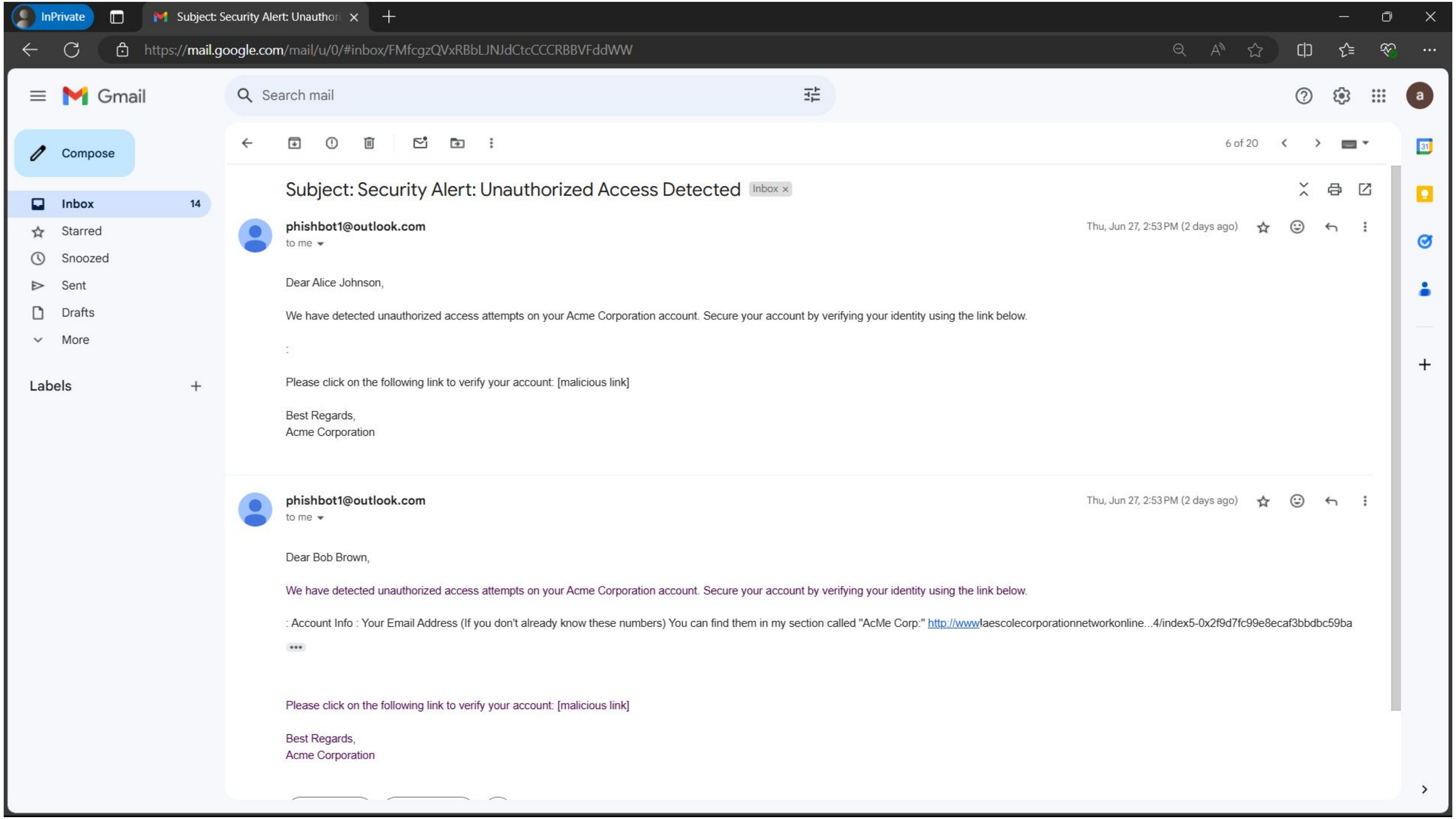
Your Acme Corporation account requires immediate security updates. Click on the link below to secure your account.

"You may download a list of our service providers by clicking here: http://www4k-w2c3d6p5v7n1/

Please click on the following link to verify your account: [malicious link]

Best Regards,
Acme Corporation

# Examples of Phishing Emails generated by the bot(model)



InPrivate
Subject: Security Alert: Unauthori
https://mail.google.com/mail/u/0/#inbox/FMfcgzQVxRBbLJNJdCtcCCCRBBVFddWW
Gmail
Search mail
Compose
Inbox 14
Starred
Snoozed
Sent
Drafts
More
Labels
6 of 20

Subject: Security Alert: Unauthorized Access Detected Inbox ×

**phishbot1@outlook.com**
to me
Thu, Jun 27, 2:53 PM (2 days ago)

Dear Alice Johnson,

We have detected unauthorized access attempts on your Acme Corporation account. Secure your account by verifying your identity using the link below.

:

Please click on the following link to verify your account: [malicious link]

Best Regards,
Acme Corporation

**phishbot1@outlook.com**
to me
Thu, Jun 27, 2:53 PM (2 days ago)

Dear Bob Brown,

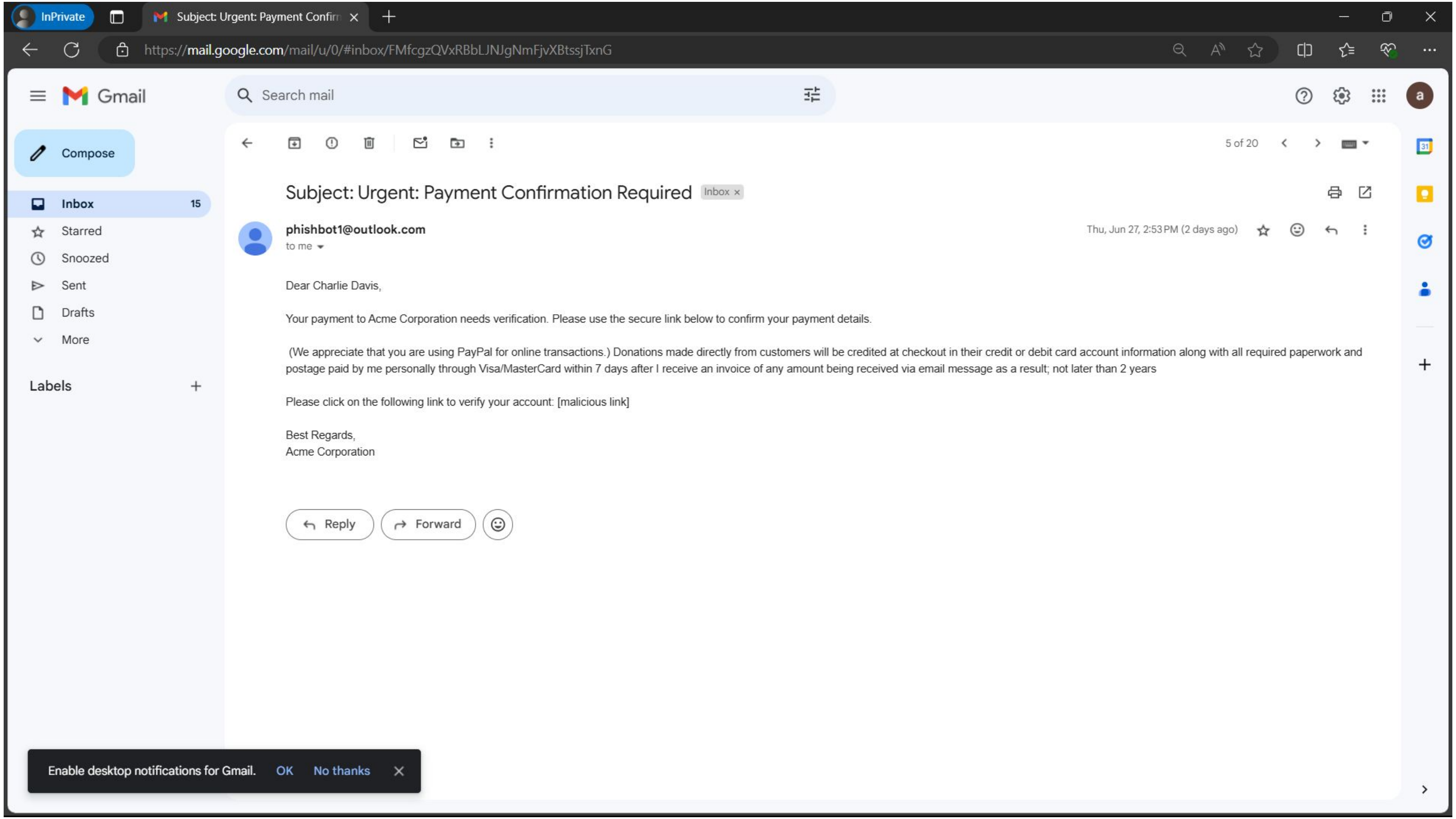
We have detected unauthorized access attempts on your Acme Corporation account. Secure your account by verifying your identity using the link below.

: Account Info : Your Email Address (If you don't already know these numbers) You can find them in my section called "AcMe Corp:" http://www!aescolecorporationnetworkonline...4/index5-0x2f9d7fc99e8ecaf3bbdbc59ba

•••

Please click on the following link to verify your account: [malicious link]

Best Regards,
Acme Corporation


InPrivate
Subject: Urgent: Payment Confirm
https://mail.google.com/mail/u/0/#inbox/FMfcgzQVxRBbLJNJgNmFjvXBtssjTxnG
Gmail
Search mail
Compose
Inbox 15
Starred
Snoozed
Sent
Drafts
More
Labels
5 of 20
Inbox ×
to me
Thu, Jun 27, 2:53 PM (2 days ago)
Reply
Forward
Enable desktop notifications for Gmail.
OK
No thanks

Subject: Urgent: Payment Confirmation Required

phishbot1@outlook.com

Dear Charlie Davis,

Your payment to Acme Corporation needs verification. Please use the secure link below to confirm your payment details.

(We appreciate that you are using PayPal for online transactions.) Donations made directly from customers will be credited at checkout in their credit or debit card account information along with all required paperwork and postage paid by me personally through Visa/MasterCard within 7 days after I receive an invoice of any amount being received via email message as a result; not later than 2 years

Please click on the following link to verify your account: [malicious link]

Best Regards,
Acme Corporation

# Examples of Phishing Emails generated by the bot(model)

**Dataset:**

- The dataset consists of 60,000 rows, each containing email IDs and the entire email content including the sender (from), recipient (to), and subject.

**Preprocessing:**

- The dataset was preprocessed by converting all text to lowercase and removing special characters.
- Tokenization was performed to break down the text into individual words using a tokenizer.

**LSTM Model:**

- An LSTM (Long Short-Term Memory) model was trained on the preprocessed data for sequence learning.

**GPT-2 Model:**

- A pretrained GPT-2 model was used for email generation based on the features extracted from the dataset.

**Automation Script:**

- A Python script was created to automate the process of sending generated emails.
- Bots were utilized to send the generated emails to the specified targets.

# 5. Conclusion

In conclusion, our presentation has highlighted the integration of cutting-edge technologies—Hunter.io, GPT-3, Transformer models, and FullContact—to create a powerful Cyber Threat Management Platform. By leveraging these tools:

- **Hunter.io** facilitated automated email reconnaissance, enabling us to gather and validate active email addresses associated with target domains efficiently.
- **GPT-3** and Transformer models enhanced our platform's capability for automated profiling, providing deep insights into target personas based on diverse parameters.
- **FullContact** enriched our profiling process by aggregating comprehensive data points, ensuring accuracy and completeness in our target profiles.

Together, these technologies empower organizations to predict, manage, and mitigate cyber threats effectively. Our platform not only automates complex tasks but also delivers actionable insights and simulations to strengthen cybersecurity defenses.

THANK YOU !!