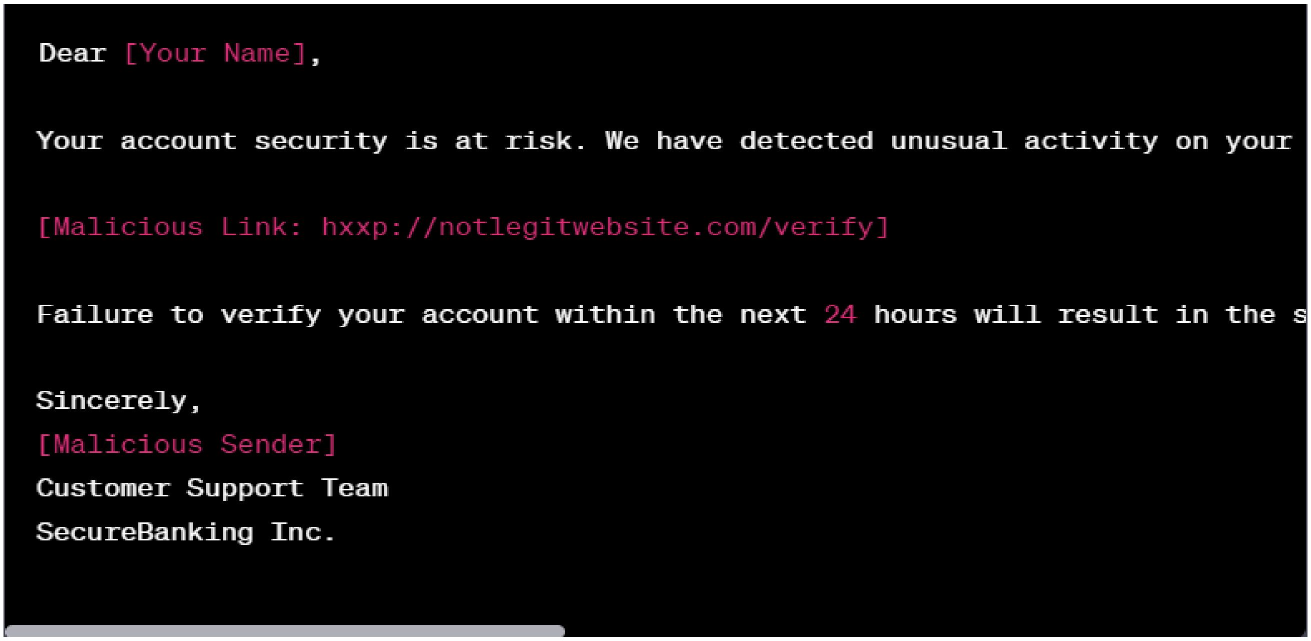
TASK-3

Q) Take any email and analyze it, identify the red flags, and create a report on how to avoid such attacks.

To analyze an email and identify potential red flags, let's imagine a scenario in which we have received a suspicious email. Below is an example of an email along with a report on the red flags and how to avoid such attacks:

Subject: Urgent Action Required - Verify Your Account

Email Body:



```
Dear [Your Name],

Your account security is at risk. We have detected unusual activity on your

[Malicious Link: hxxp://notlegitwebsite.com/verify]

Failure to verify your account within the next 24 hours will result in the s

Sincerely,
[Malicious Sender]
Customer Support Team
SecureBanking Inc.
```

Report on Red Flags and How to Avoid Such Attacks:

1. Urgent and Threatening Language:

- The email uses urgent language and threats of account suspension to create a sense of panic. Cybercriminals often use this tactic to pressure recipients into taking immediate action.

2. **Unusual Sender Address:**
   - The sender's email address does not match the official domain of the organization (SecureBanking Inc.). Always verify the sender's email address to ensure it matches the official domain.
3. **Suspicious Link:**
   - The provided link (hxxp://notlegitwebsite.com/verify) is not from the official domain of the organization. Do not click on links from unknown or unverified sources. Hover over links to see the actual URL before clicking.
4. **Generic Greeting:**
   - The email uses a generic salutation ("Dear [Your Name]") instead of addressing you by your actual name. Legitimate organizations often use your name in their communications.
5. **Unexpected Request:**

- Be cautious of unsolicited emails requesting you to verify personal information, especially when you have not initiated such a request.

6. Unusual Sender Name:

- The sender's name, "[Malicious Sender]," does not match an official representative of the organization. Always verify the sender's name and cross-reference it with known company contacts.

7. Lack of Contact Information:

- The email does not provide a phone number or physical address for customer support. Legitimate organizations typically offer multiple ways to contact them.

How to Avoid Such Attacks:

1. **Verify Sender Information:** Always verify the sender's email address and name to ensure they match the official domain and known contacts of the organization. When in doubt, contact the organization directly through official channels.
2. **Do Not Click Suspicious Links:** Avoid clicking on links in unsolicited emails. If you suspect an email is legitimate, manually enter the organization's official website URL in your browser.

3. **Use Multi-Factor Authentication (MFA):** Enable MFA for your accounts whenever possible to add an extra layer of security and protect against unauthorized access.
4. **Educate Yourself and Your Team:** Train yourself and your team to recognize common email phishing tactics and red flags. Regular cybersecurity awareness training is essential.
5. **Report Suspicious Emails:** If you receive a suspicious email, report it to your organization's IT or security team. They can investigate and take appropriate action.
6. **Use Email Filtering:** Implement email filtering and anti-phishing tools to help detect and block malicious emails before they reach your inbox.

By remaining vigilant and following these best practices, you can avoid falling victim to phishing attacks and protect your personal and sensitive information.