CYBER SECURITY INTERNSHIP

Task 2: Phishing Email Analysis

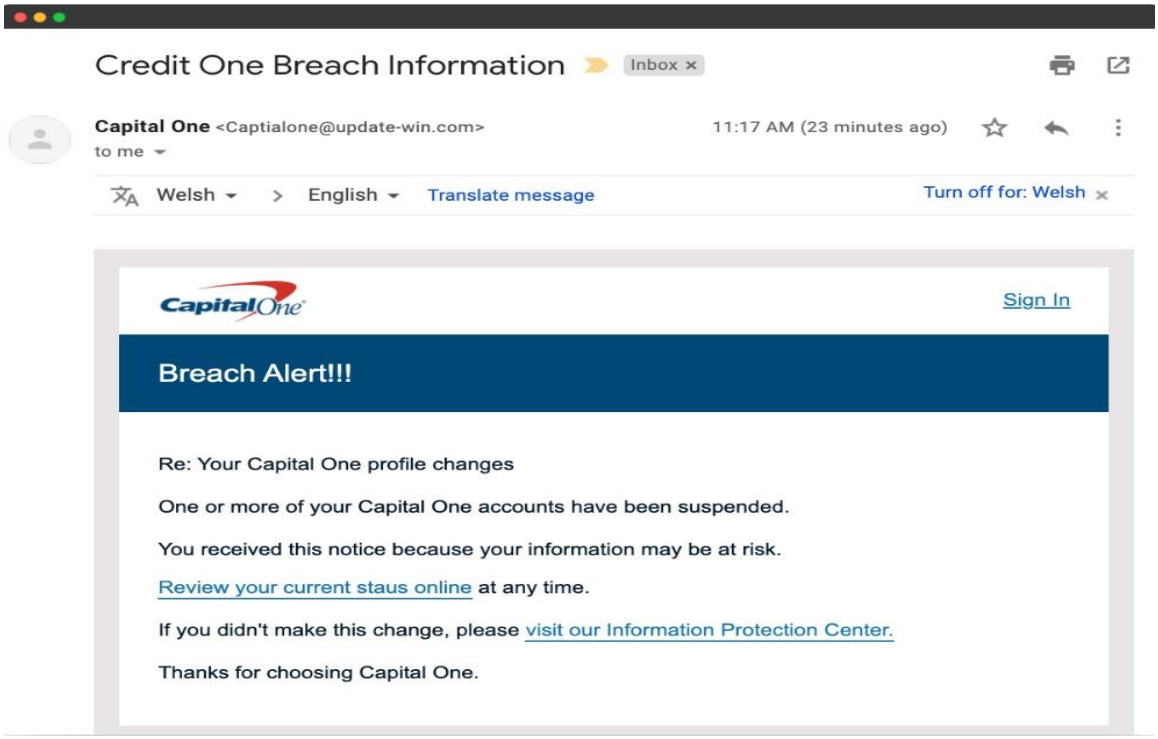
Submitted by: Kommuri Chaitanya
Date: 05-08-2025

1. Introduction

Phishing attacks are fraudulent messages designed to trick recipients into revealing confidential information. They often impersonate trusted brands or institutions. This report analyzes a suspicious email pretending to be from Capital One, warning the user about a potential breach and prompting them to verify account details through a malicious link.

2. Email Overview

Subject: Credit One Breach Information
Sender: Captialone@update-win.com
Claimed Authority: Capital One
Message: Claims user's Capital One account was changed/suspended and instructs them to verify their status online through embedded links.



3. Detailed Suspicious Indicators

• Fake Sender Email:
  - Domain `update-win.com` is unrelated to Capital One.

• Brand Impersonation:
  - Email uses the Capital One logo and brand style to gain trust.

• Urgency and Fear Tactics:
  - Claims account has been suspended and information is at risk.

• Suspicious Links:
  - Hyperlinks like “Review your current staus online” may lead to phishing sites.

• Spelling Error:
  - 'Staus' instead of 'Status' indicates poor quality or fake content.

• No Personalization:
  - Email doesn’t address the recipient by name.

• Unusual Grammar and Tone:
  - Use of excessive exclamation marks and informal language.

• No Legitimate Footer or Contact Info:
  - Official Capital One emails contain legal disclaimers and support details.

4. Email Header Analysis

A header analysis using tools like MXToolbox would reveal that the email is not sent from Capital One servers. The domain and IP address used would not align with official Capital One infrastructure, confirming spoofing.

5. Why This Email is a Phishing Attempt

• Spoofed sender and fake domain.
• Urgent tone to force immediate action.
• Hyperlinks likely lead to credential harvesting pages.
• Grammar and spelling mistakes suggest fraud.

6. Potential Risks if Link is Clicked

• Stolen login credentials.
• Unauthorized access to Capital One accounts.
• Identity theft and financial fraud.
• Malware installation.

7. Preventive Measures

✓ Check sender email addresses carefully.
✓ Hover over links before clicking to verify legitimacy.
✓ Avoid clicking links in suspicious emails.
✓ Enable alerts and MFA on financial accounts.
✓ Report phishing emails to the company being impersonated.

8. Conclusion

This email impersonates Capital One to create a false sense of urgency and trick recipients into revealing their credentials. It uses a spoofed sender domain, suspicious links, and poor grammar—classic signs of a phishing attempt. Awareness and careful analysis of such emails are essential to prevent cyber threats.