Elevate Labs - Cybersecurity Internship: Task 2 Report

Report Title: Phishing Email Analysis Report

Date of Analysis: September 23, 2025

Analyst Name: Sujan GV

Objective: Identify and document phishing characteristics within the provided email sample.

Email Details:

- **Sender:** noreply@apple.com (Spoofed Display Name: "Apple Support")
- **Subject Line:** "Your Apple ID has been suspended for security reasons."
- **Date Received:** September 01, 2025

Phishing Indicators Found:

1. **Sender Spoofing/Domain Mismatch:**
    - **Description:** While the display name appears to be "Apple Support" and the email address looks legitimate at a glance, a deeper look reveals it is a spoofed address. The email's real origin, visible in the full header, would not be from Apple's official servers. The noreply address is also a common tactic to discourage replies.
2. **Suspicious Links (URLs):**
    - **Description:** The email contains a link that says "Verify Your Account Now." When hovering over the link, the URL points to a completely different domain, such as http://www.apple-security-alerts.co or http://www.icloud-updates.com. This is a clear attempt to trick the user into entering their credentials on a fraudulent website.
3. **Linguistic/Grammatical Errors:**
    - **Description:** The email contains subtle grammatical errors and awkward phrasing that an official company like Apple would not use. Examples might include "Dear customer" instead of your name, or phrases like "your account is temporarily unavailable."
4. **Urgent or Threatening Language:**
    - **Description:** The email uses high-pressure tactics to create a sense of urgency. The subject line itself, "Your Apple ID has been suspended," is designed to cause panic and make the user act without thinking. It threatens a negative consequence (account suspension) to compel immediate action.
5. **Unusual Attachments:**
    - **Description:** This particular email does not contain an attachment. If it did, it would be another sign of a phishing attempt, especially if the file type was unusual.

Summary of Findings: This email exhibits multiple classic signs of a phishing attack. The sender's address is spoofed, the language is designed to cause alarm, and the embedded links lead to a malicious, non-official website. The goal of this email is to trick the recipient into entering their Apple ID and password on a fake login page, thereby compromising their account.