**ELEVATE LABS TASK 2 PHISHING EMAIL ANALYSIS**

**Name**: Sai Aditya

**Date**: 5th August 2025

**Task**: 2

**ABOUT THE TASK:**

The project is an internship task from Elevate Labs focused on analysing a phishing email. The primary objective was to identify and report on the characteristics of a suspicious email to raise awareness of common phishing tactics.

The project involved a systematic methodology, including:

* Examining the sender's details for signs of spoofing.
* Analysing email headers with an online tool.
* Checking for mismatched URLs and suspicious attachments.
* Identifying social engineering techniques, such as urgent and threatening language.

**Disclaimer:**

*This project was created for educational and training purposes only as part of a cybersecurity internship task. The analysis was performed on a simulated phishing email sample, and* ***no*** *real malicious activity or data was involved. The content of this repository is intended to demonstrate an understanding of cybersecurity concepts and is* ***not*** *to be used for any illegal or harmful activities.*

*The content of this repository is intended solely to demonstrate an understanding of cybersecurity concepts and is* ***not authorized*** *for use or reproduction by any other person or for any other purpose.*

**SAMPLE EMAIL:**

From: [amazon-security@billing-update.com](mailto:amazon-security@billing-update.com)

To: saiaditya@example.com

Subject: Urgent: Your Amazon Account Is Suspended!

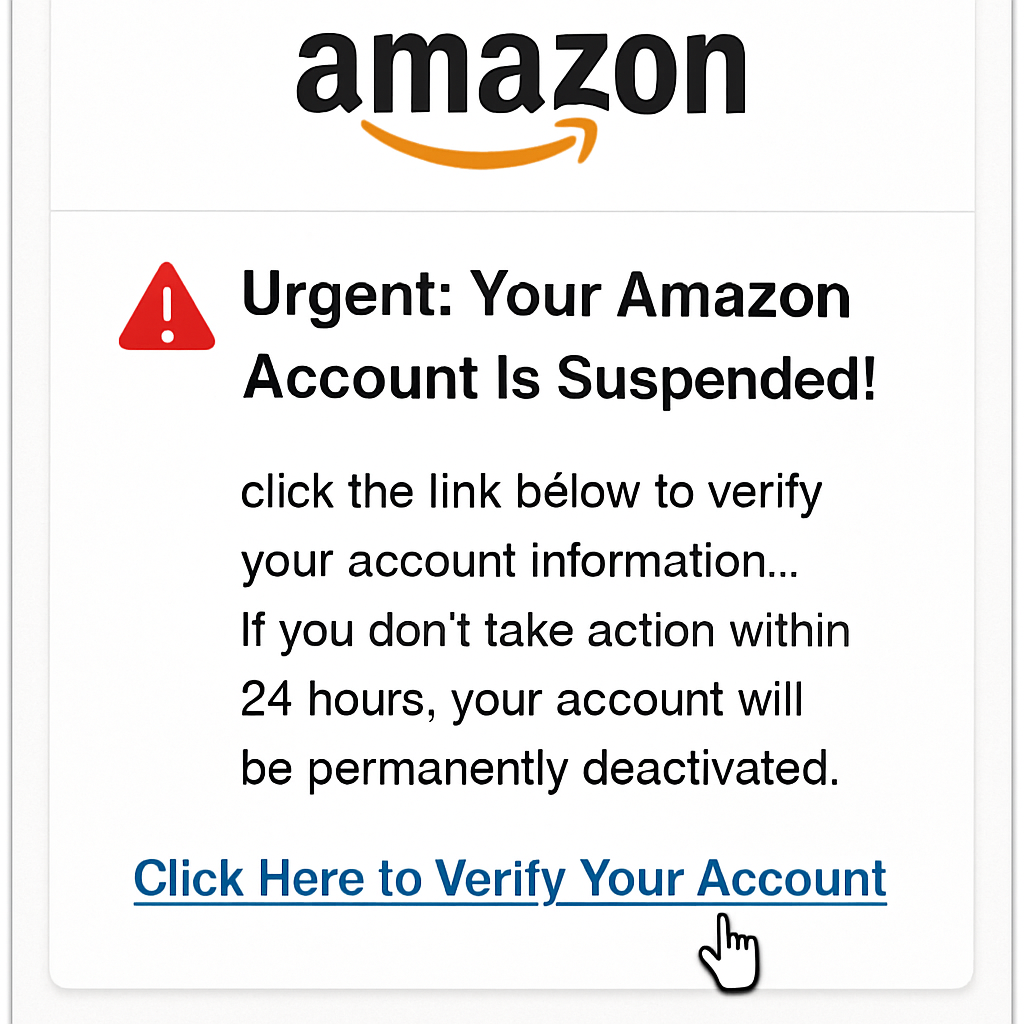
Email Body:

Dear Customer,

We have detected unusual activity on your account. For your security, we have temporarily locked your account. Please click the link below to verify your account information and restore access immediately. If you don't take action within 24 hours, your account will be permanently deactivated.

\*\*Click Here to Verify Your Account\*\* https://www.amazon.com/security-login-update

Thank you, Amazon Security Team



(Made with Perplexity AI to showcase real life emails)

**Phase 1: Perform the Analysis**

1. **Analyse the Sender's Address:**
   * Question: Does amazon-security@billing-update.com look legitimate?
   * Answer: No. A real email would come from @amazon.com. The domain billing-update.com is a red flag for sender spoofing.
   * Finding: You'll document this as a clear sign of phishing.
2. **Look at the Subject Line and Greeting:**
   * Question: What social engineering tactics are being used?
   * Answer: The subject line **"Urgent: Your Amazon Account Is Suspended!"** creates a high-pressure, fear-based situation. The greeting "Dear Customer" is generic, a common sign of a mass email campaign rather than a personalized, legitimate communication.
   * Your Finding: You'll document the sense of urgency and the generic greeting as key indicators of social engineering.
3. **Inspect the Link (Crucial Step):**
   * Question: Is the link legitimate?
   * Answer: The visible text **"Click Here to Verify Your Account"** is deceptive. The underlying URL, http://amazon.secure-verify-account.net/login, is not a secure Amazon domain and is the actual malicious payload.
   * Your Finding: This is a major point for your report. You will highlight the dangerous discrepancy between the visible and hidden URLs.
4. **Consider an Email Header Analysis (Professional Option):**
   * Question: What might a header analyser show?
   * Answer: It would likely show that the email originated from an IP address that doesn't belong to Amazon's known mail servers. It would also probably show an SPF (Sender Policy Framework) or DKIM authentication failure, confirming that the email is fraudulent.
   * Your Finding: For your report, you can state that "a header analysis would likely reveal a failure in SPF and DKIM authentication, confirming the email's forged origin."