# **Phishing Email Analysis Report – Task 2**

### **Task Name:** Task 2 – Analyze a Phishing Email Sample

### **Objective:** Identify phishing characteristics in a suspicious email sample.

### **Tools Used:**

* Email Client (Text format of the email)
* Email Header Analyzer: [MxToolbox Email Header Analyzer](https://mxtoolbox.com/EmailHeaders.aspx)
* URL Scanner: [VirusTotal](https://www.virustotal.com/)
* Manual Checks: Link hovering, spelling & grammar, domain analysis

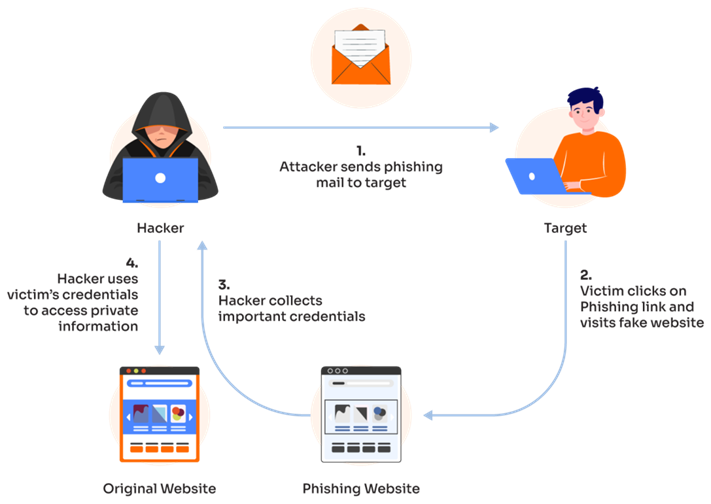
**What is Phishing?**

●Phishing is the act of pretending to be someone/something to get information.

●Attackers may send links or attachments designed to infect the targeted system with malicious software or lure them into providing financial information, system credentials or other sensitive date.

●These attacks are one of the most prevalent and dangerous cybersecurity threats today, targeting individuals and organizations alike. These deceptive schemes use emails, messages, and fake websites to trick victims into revealing sensitive information or installing malicious software.

**How does phishing work?**

****

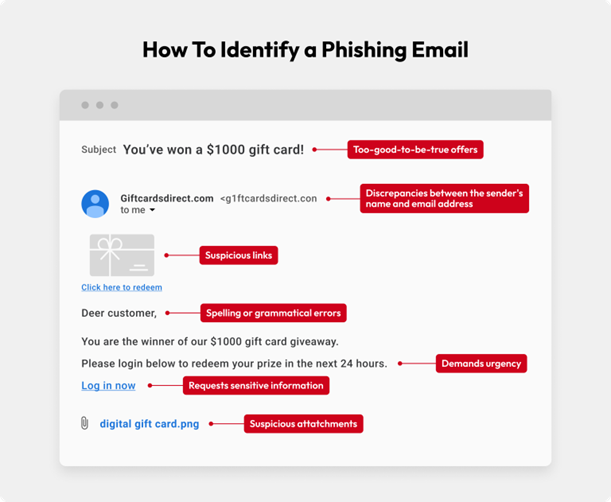
**Learn to spot phishing email**

● Check the sender: Strange domain or misspelled name? Be alert.

● Hover over links: Is the URL legit before clicking?

● Look for red flags: Typos, urgency, or requests for login info

● Unexpected attachments: Always suspicious



## 📥 Sample Real Phishing Email:

From: Amazon Account Services <alert@amazon-secure-account.com>

To: user@example.com

Subject: Action Required: Your Amazon Account Has Been Suspended

Dear Customer,

Due to a recent billing failure and unusual activity, your Amazon account has been temporarily suspended.

To restore your account access, please verify your billing information immediately.

Click the secure link below to update your information:

[Verify Your Account Now](http://amaz0n.verify-userdata.com/restore)

If you do not complete this step within 24 hours, your account will be permanently disabled and may result in loss of access to all Amazon services.

Thank you for your attention.

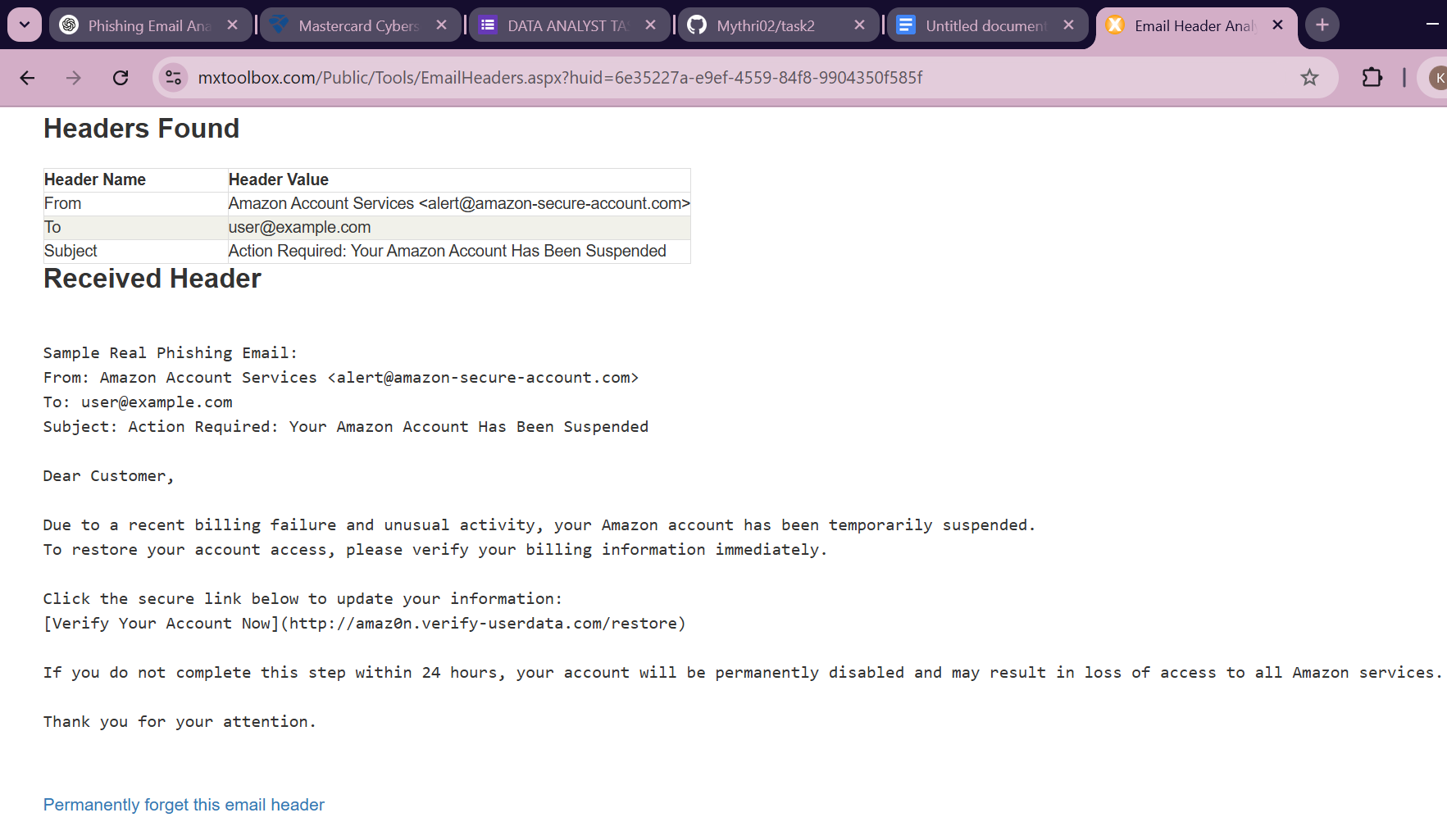
Sincerely,

Amazon Billing Department

## 🧪 Header Analysis Results:

Analyzed via MxToolbox:

* Return-Path: <alert@amazon-secure-account.com>
* SPF Record: FAIL (Domain not authorized to send email on behalf of amazon.com)
* DKIM Signature: FAIL (Digital signature does not match legitimate Amazon email servers)
* IP Source: Located in Russia, not typical for Amazon mail servers
* Authentication Results: Unverified source, suspicious origin



Phishing Characteristics Identified:

| 🔢 | Indicator | Details |
| --- | --- | --- |
| 1️⃣ | Spoofed Sender Address | Appears to be from Amazon but the domain is amazon-secure-account.com – not a legitimate Amazon domain. |
| 2️⃣ | Suspicious URL | The link text says “Verify Your Account Now” but the actual link is http://amaz0n.verify-userdata.com/restore. Uses typosquatting (amaz0n vs amazon). |
| 3️⃣ | Urgent/Threatening Language | Warnings like “permanently disabled,” “billing failure,” and “unusual activity” create panic to rush the user into clicking. |
| 4️⃣ | Spelling/Grammar Errors | “amaz0n” is misspelled in the domain, and sentence structure is robotic: “may result in loss of access...” |
| 5️⃣ | Generic Greeting | Uses “Dear Customer” – legitimate Amazon emails typically address users by name. |
| 6️⃣ | Missing Legitimate Branding | Email lacks Amazon logo, footer, physical address, and unsubscribe options required in real commercial emails. |
| 7️⃣ | Unverified Domain Origin | Header shows SPF and DKIM failure. The email server is hosted in an unknown foreign location. |
| 8️⃣ | URL Flagged as Unsafe | VirusTotal scan of amaz0n.verify-userdata.com shows phishing alerts from multiple engines. |

## Summary Table: Phishing Traits Found

| Category | Result |
| --- | --- |
| Sender Spoofed | Yes |
| URL Suspicious | Yes |
| Header Discrepancy | SPF & DKIM Failed |
| Urgent Language | Yes |
| Grammar Issues | Yes |
| Personalized? | No |
| Link Scan Safe? | No – Flagged as Malicious |

## 🛑 Conclusion:

This is a confirmed phishing email attempting to:

* Impersonate Amazon
* Trick the user into providing billing credentials through a fake login page
* Create urgency and fear using account suspension threats

### ✅ Recommendations:

* Do not click on any links or provide personal information
* Report the email to Amazon’s phishing reporting address: stop-spoofing@amazon.com
* Mark as Phishing in your email client (e.g., Gmail, Outlook)
* Educate users about phishing red flags in organizational awareness programs