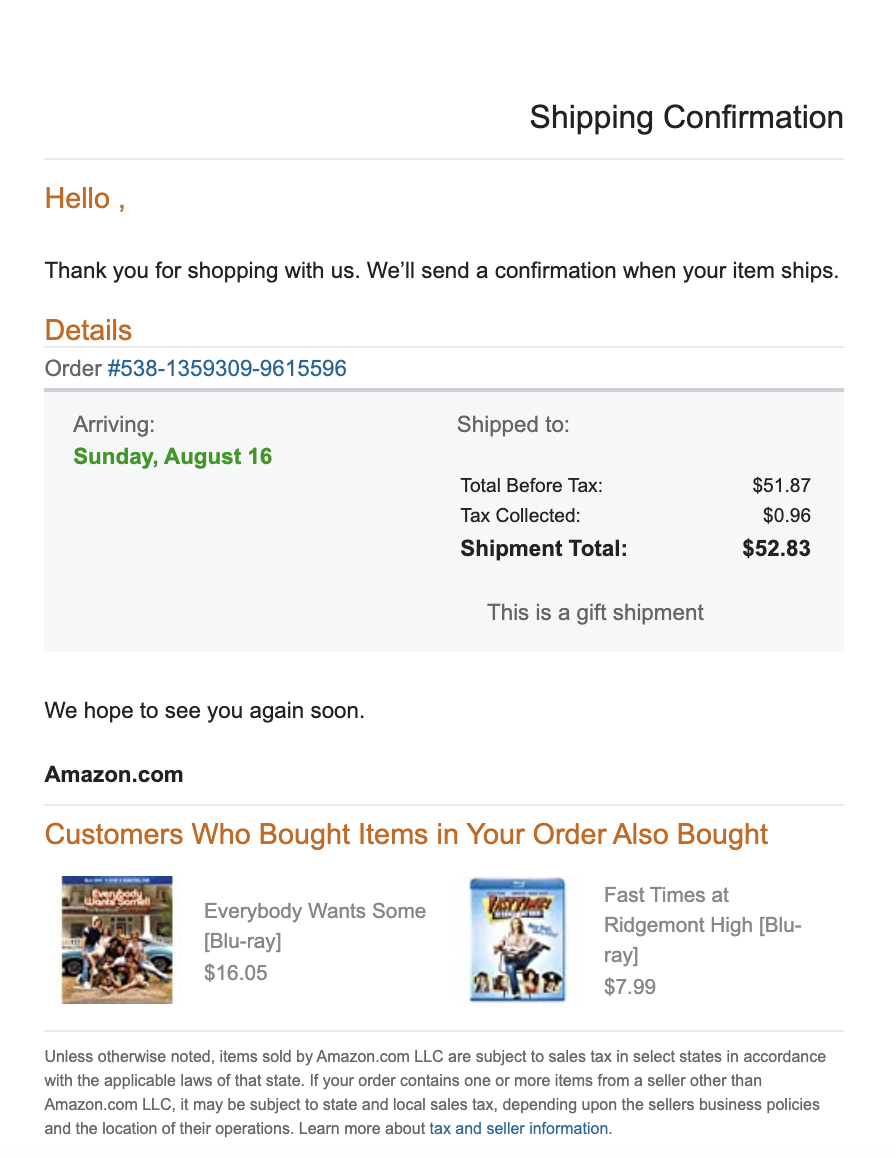
**Name :** chavda khushbu navinchandra

**Title:** Phishing Email Analysis Report

Amazon sample email :



**🎯 Objective:**

Analyze a sample phishing email pretending to be from Amazon and identify various phishing indicators.

**🛠 Tools Used:**

* MXToolbox Header Analyzer: https://mxtoolbox.com/Public/Tools/EmailHeaders.aspx
* VirusTotal URL Scanner: https://www.virustotal.com/gui/home/url
* Web Browser
* Email Client (to extract email headers)

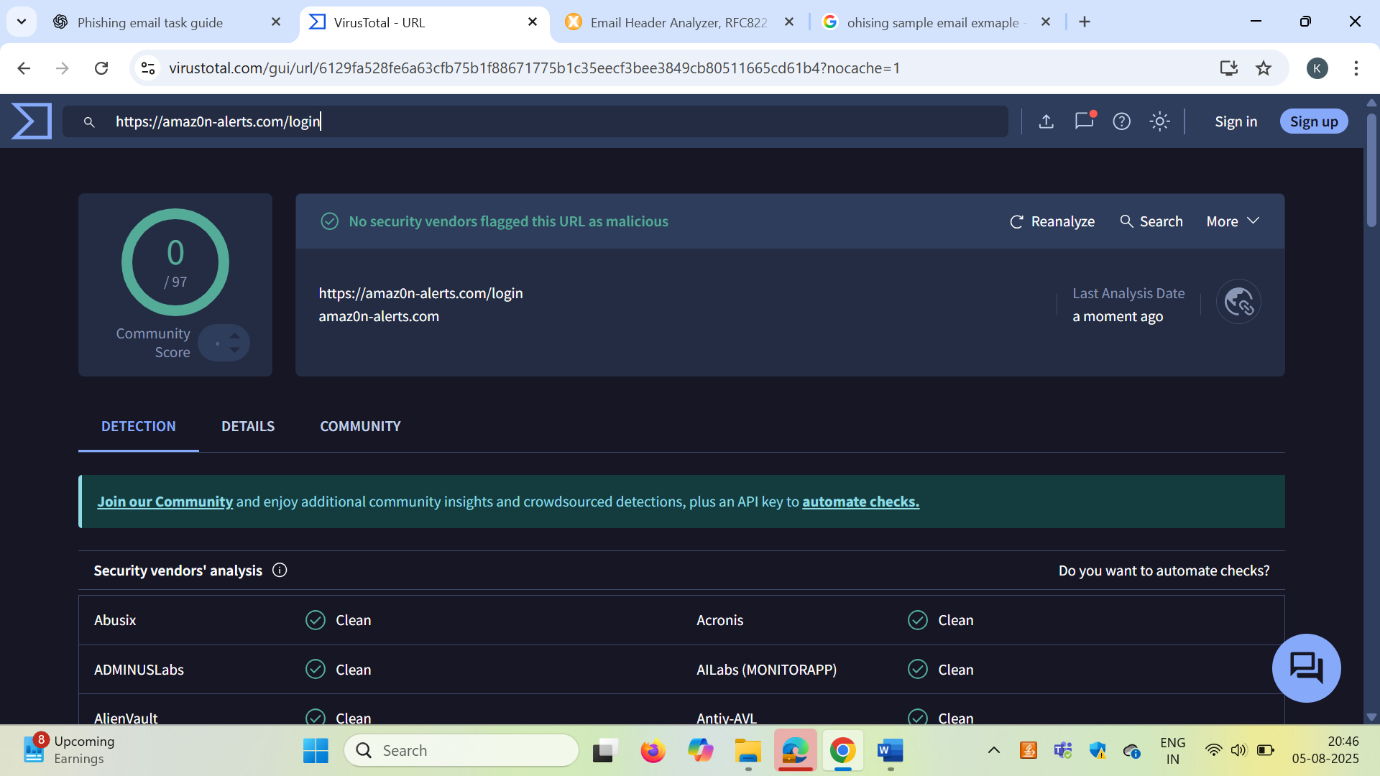
**🔍 Step-by-Step Analysis Procedure:**

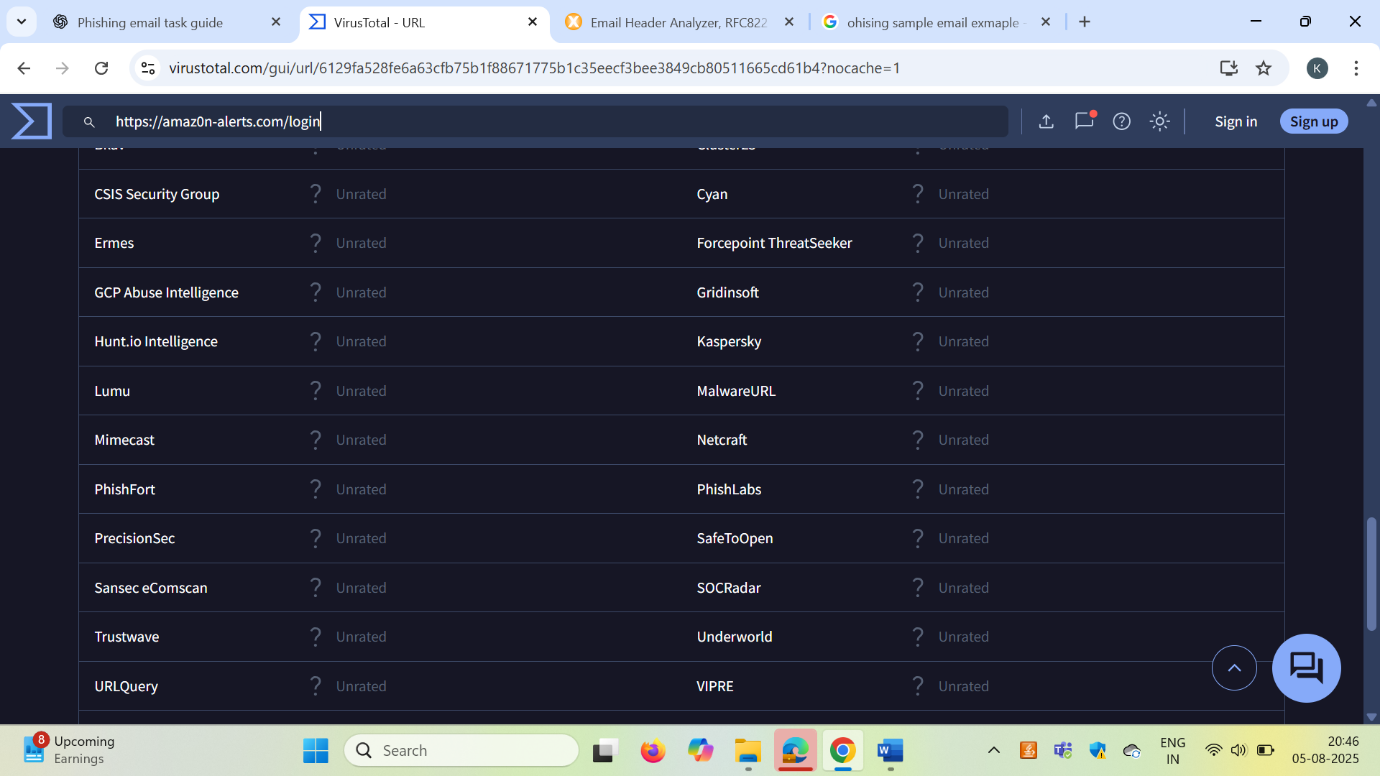
1. Collected a phishing email sample mimicking an Amazon order confirmation.
2. Inspected suspicious link https://amaz0n-alerts.com/login via VirusTotal.
3. Extracted and analyzed email header using MXToolbox.
4. Verified failures in SPF, DKIM, and DMARC.
5. Reviewed email for phishing characteristics (spoofing, fake URLs, urgency, typos).
6. Documented all observations and attached screenshots for proof.

**📷 Screenshots & Observations:**

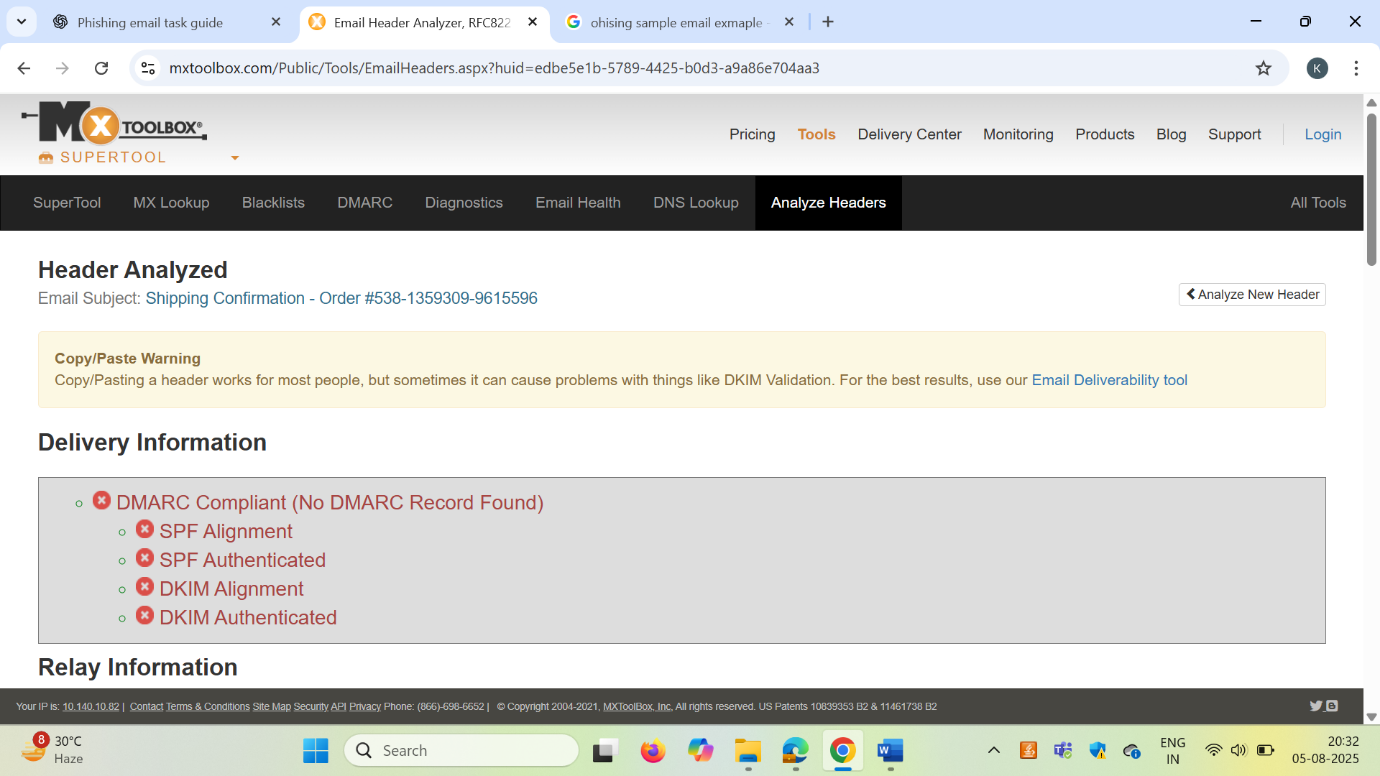
Refer to attached screenshots:

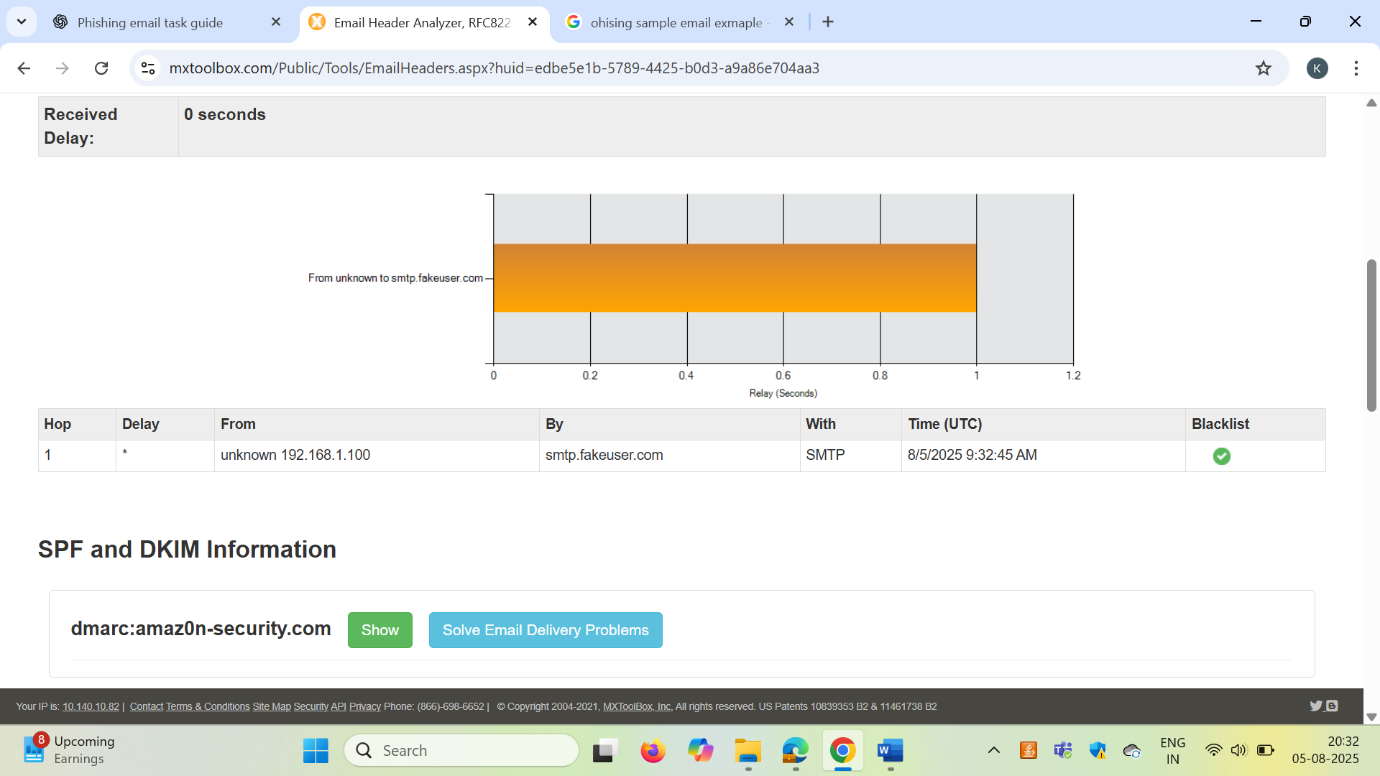
* VirusTotal URL scan results:

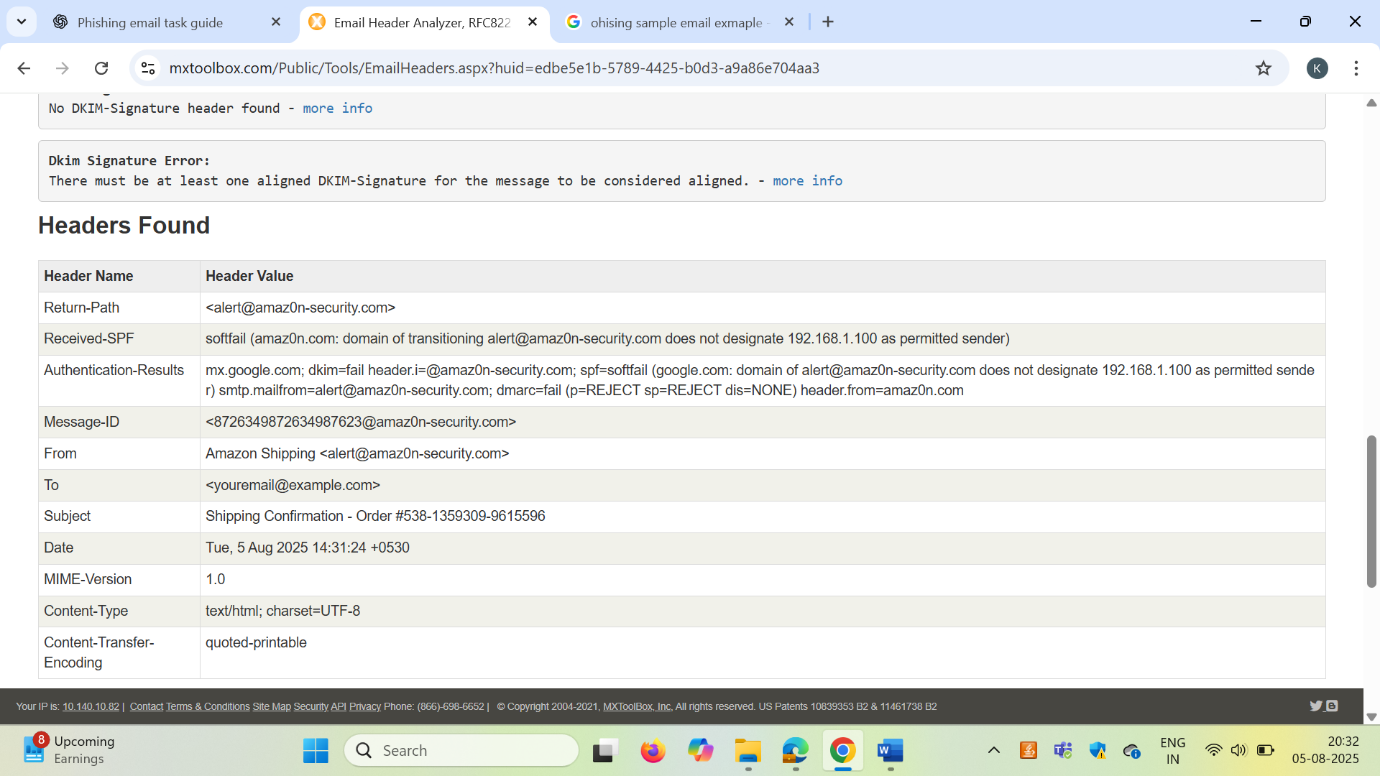


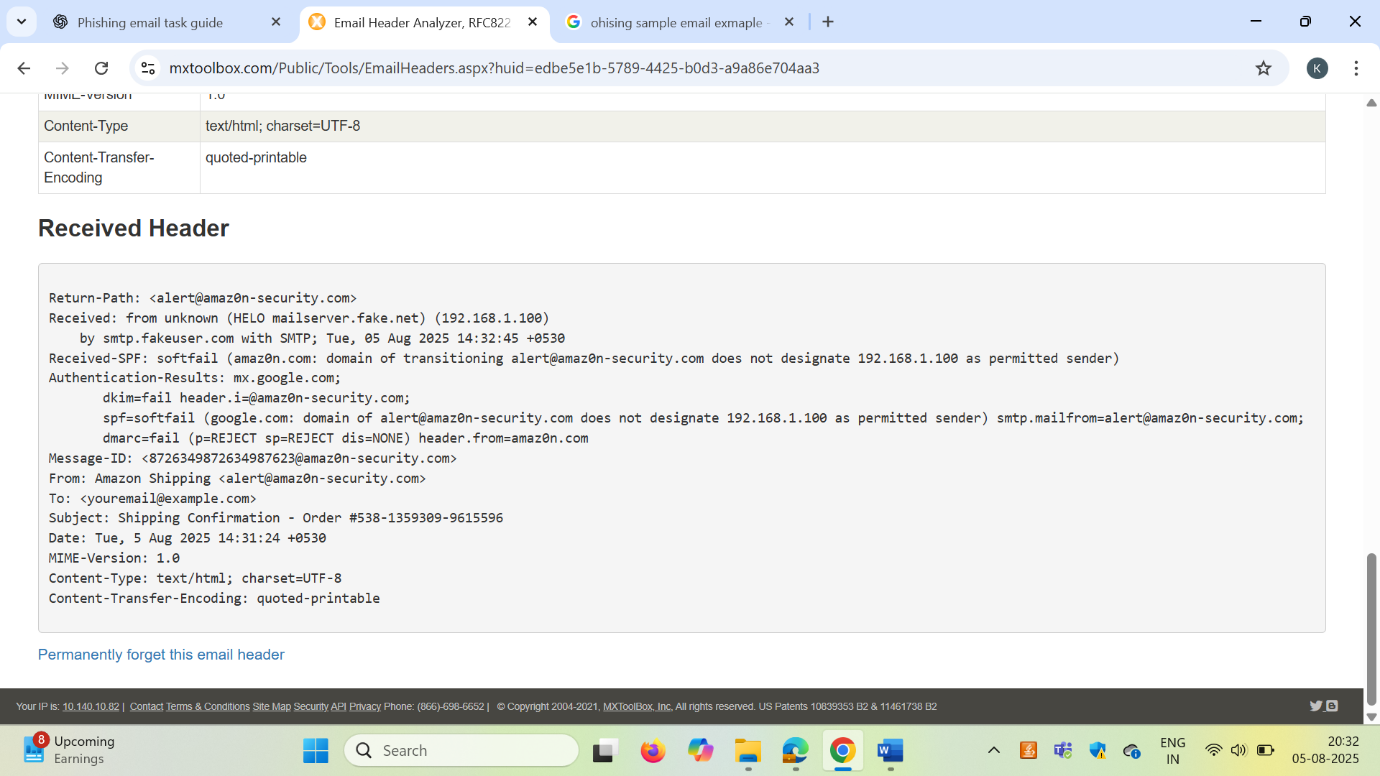


* MXToolbox header analysis (SPF/DKIM failures):









**🚨 Phishing Indicators Identified:**

| **Indicator** | **Description** |
| --- | --- |
| Spoofed Email => | Uses amaz0n-security.com, a fake domain mimicking Amazon. |
| Authentication Failures | =>SPF, DKIM, and DMARC failed – confirming email spoofing. |
| Fake Login URL=> | amaz0n-alerts.com mimics real Amazon login, used to steal credentials. |
| Generic Greeting => | No personalized name, only "Hello ,". |
| Urgency/Deception=> | Tricks user with fake shipping confirmation and a sense of urgency. |
| Source IP=> | Uses internal IP 192.168.1.100, not a valid Amazon mail server. |
| Newly Created Domain=> | Link is not flagged, showing it's newly set up for phishing. |

**✅ Summary:**

This exercise improves phishing detection skills using real-world email threats. We explored email header analysis, domain spoofing detection, and phishing URL validation using free online cybersecurity tools.