**Task 2 - Phishing Email Analysis**

This report presents an analysis of a phishing email using publicly available tools. The objective was to examine email headers, identify spoofing or suspicious behavior, and verify the reputation of sender IP addresses. This practical investigation helps in understanding real-world phishing tactics and learning how to defend against them.

**Phishing Email Subject:** CLIENTE PRIME - BRADESCO LIVELO

**Message Content:** "Seu cartão tem 92.990 pontos LIVELO expirando hoje!"

This message urges the recipient to act quickly, which is a common psychological tactic used in phishing attacks.

**Header Analysis:**

Using MXToolbox, the following issues were identified:

* ■ **DMARC Missing:** No DMARC record found.
* ■ **SPF Alignment Failed:** Email failed SPF check.
* ■ **SPF Authentication Failed:** Likely spoofed sender.
* ■ **Delay Path:** Suspicious delays and multiple relay hops shown in graph.

**IP Reputation Check (VirusTotal):**

Analyzed IP: **137.184.34.0** — associated with the phishing email.

* ■ Flagged as **Malicious** by 1 security vendor (Criminal IP).
* Host AS: **DigitalOcean** — commonly used for bulk spoofing and relay.

**Red Flags Identified:**

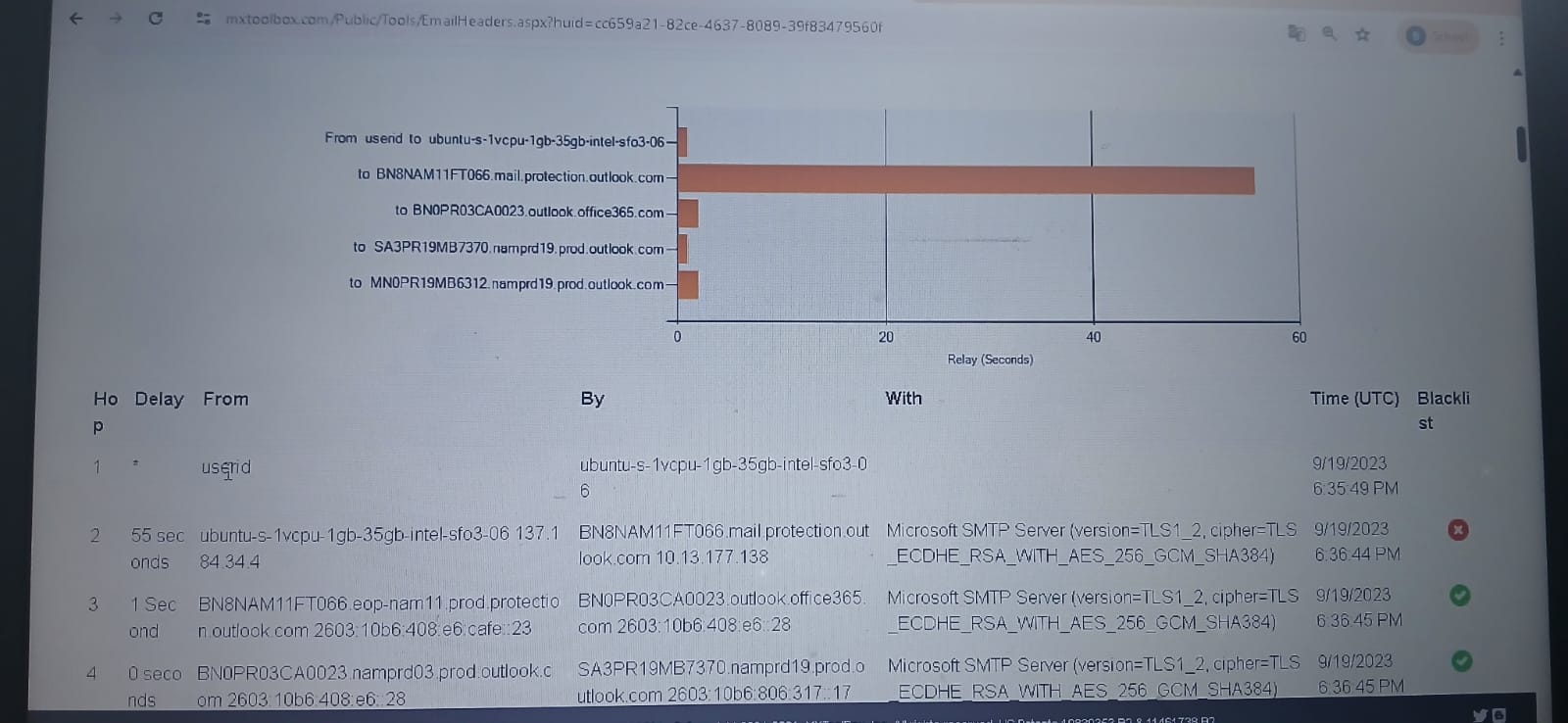
* No DMARC, SPF misalignment: indicates spoofed origin.
* Public VPS relay (DigitalOcean) is common in spam campaigns.
* Email subject has urgency and reward tactic.

These indicators clearly classify the email as a phishing attempt.

**Tools Used:**

* MXToolbox (https://mxtoolbox.com)
* VirusTotal (https://virustotal.com)
* Chrome Browser (for testing links and screenshots)

**Conclusion:**

The email analyzed is likely a phishing attempt due to header manipulation, failed authentication protocols, and malicious IP involvement. This exercise demonstrates the importance of examining technical details before trusting unknown messages.