Task-2

Analyzing a Phishing Email Sample:

Objective: Identifying phishing characteristics in a suspicious email sample.

Phishing: Phishing is a type of cyberattack that uses fraudulent emails, text messages, phone calls or websites to trick people into sharing sensitive data, downloading malware or otherwise exposing themselves to cybercrime.

Sample email : https://github.com/raghava00/Analyzing-a-Phishing-Email-Sample-Task2-/blob/main/BRADESCO%20LIVELO%20(1).eml

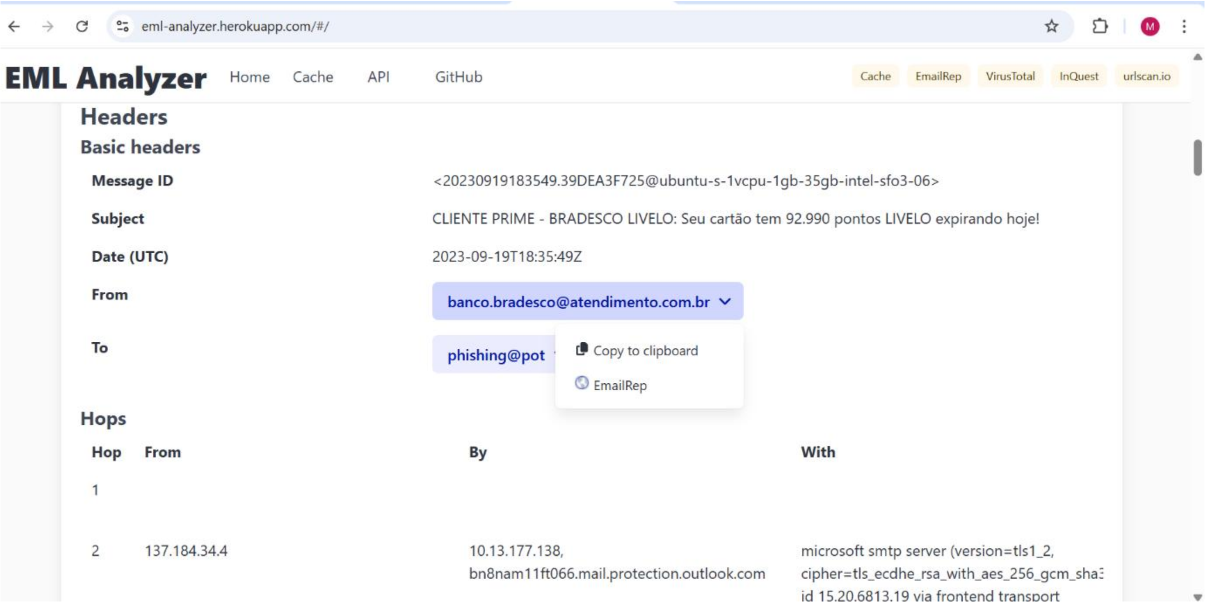
The email is pretending to be from **Bradesco or Livelo** (a Brazilian bank and its points/rewards program). It claims:

- You have **92,990 Livelo points**.
- These points are **about to expire today**.
- If you don't act quickly, you will **lose them**.
- It likely contains a **button or link** urging you to click to "redeem" or "rescue" the points.

To make you panic about losing valuable points so you **click a malicious link** — probably to:

- Steal login credentials
- Download malware
- Collect personal or banking information

The sample phishing email is submitted to an **EML Analyzer**. The purpose is to determine whether the email poses a security threat and to document its malicious indicators.



Headers

Basic headers

Message ID	<20230919183549.39DEA3F725@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06>
Subject	CLIENTE PRIME - BRADESCO LIVELO: Seu cartão tem 92.990 pontos LIVELO expirando hoje!
Date (UTC)	2023-09-19T18:35:49Z
From	banco.bradesco@atendimento.com.br
To	phishing@pot

Hops

Hop	From	By	With
1			
2	137.184.34.4	10.13.177.138, bn8nam11ft066.mail.protection.outlook.com	microsoft smtp server (version=tls1_2, cipher=tls_ecdhe_rsa_with_aes_256_gcm_sha3 id 15.20.6813.19 via frontend transport

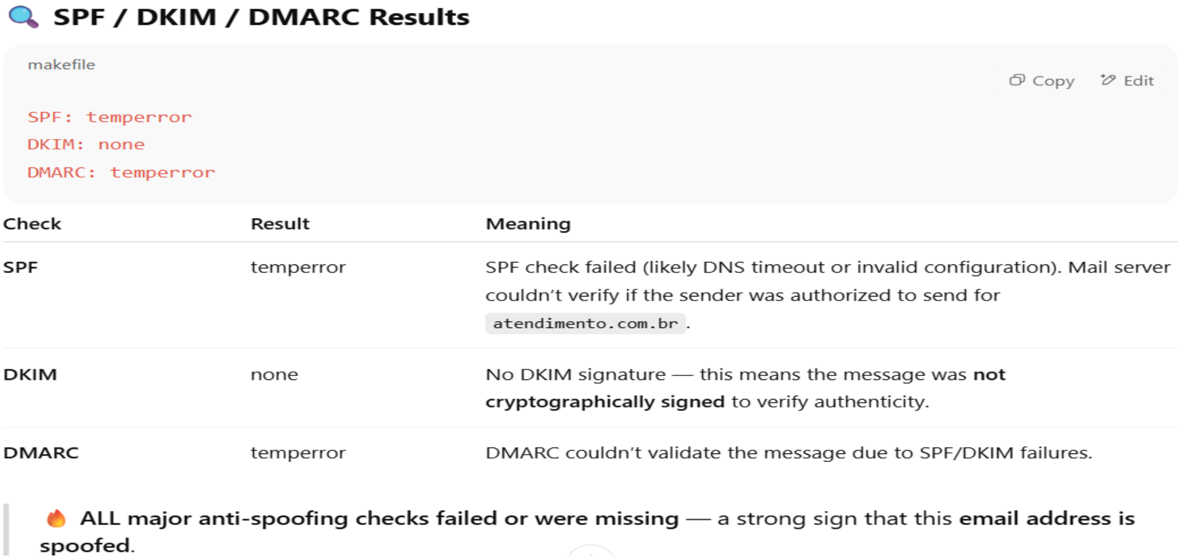
From Header (Sender Info)

From: BANCO.BRADESCO@ATENDIMENTO.COM.BR

Return-Path: root@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06

Appears as: BANCO.BRADESCO@ATENDIMENTO.COM.BR

This looks like an official Bradesco email address — **but appearances are easily faked** in email headers.



🔍 SPF / DKIM / DMARC Results

```makefile
SPF: temperror
DKIM: none
DMARC: temperror
```

Check	Result	Meaning
SPF	temperror	SPF check failed (likely DNS timeout or invalid configuration). Mail server couldn't verify if the sender was authorized to send for `atendimento.com.br`.
DKIM	none	No DKIM signature — this means the message was **not cryptographically signed** to verify authenticity.
DMARC	temperror	DMARC couldn't validate the message due to SPF/DKIM failures.

> 🔥 **ALL major anti-spoofing checks failed or were missing** — a strong sign that this **email address is spoofed**.

Key Email Header Analysis & Discrepancies

1. Timestamp Discrepancy

Header	Value
Date:	2023-09-19T18:35:49Z
Received:	2023-09-19T18:36:44Z (Outlook.com)
Delay	~55 seconds delay

2. Return-Path vs. From Address Mismatch

Header	Value
Return-Path:	root@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06
From:	BANCO.BRADESCO@ATENDIMENTO.COM.BR

3. IP Address / Source Host Discrepancy

Header	Value
Sender IP	137.184.34.4
IP origin	DigitalOcean (USA-based cloud)

This IP belongs to a DigitalOcean VPS, commonly used for spam/phishing campaigns — not used by legitimate corporations like Bradesco.

4. Message-ID vs Hostname

Header	Value
Message-ID:	<20230919183549.39DEA3F725@ubuntu-s-1vcpu...>

The Message-ID confirms the message originated from a self-hosted Linux server, not an official Bradesco or Livelo email system.

•**This email header analysis reveals multiple critical discrepancies — it is not from Bradesco, is spoofed, and is highly likely to be part of a phishing or scam operation.**

Suspicious Elements:

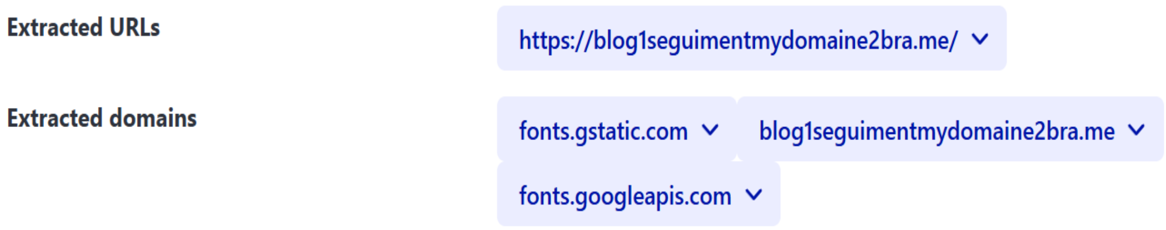
Element	Details
https://blog1seguimentmydomaine2bra.me/	Malicious-looking fake domain pretending to be Bradesco
Image links	May be used to track user behavior when opened
Base64 encoded HTML body	Potential obfuscation to avoid detection
No attachments	None found, but body content could contain interactive phishing

Urgency:

- “Your card has 92,990 Livelo points expiring today!”
- **Urgency tactic**: Creates pressure by suggesting immediate loss.
- Purpose: Force users to **act quickly**, often without verifying legitimacy.

Mismatched URL Indicators:

What was shown	What was linked	Verdict
“Resgatar Agora” button	https://blog1seguimentmydomaine2bra.me/	Phishing
Brand (Bradesco / Livelo)	None of the links point to real brand domains	Spoofed



Extracted URLs	https://blog1seguimentmydomaine2bra.me/
Extracted domains	fonts.gstatic.com blog1seguimentmydomaine2bra.me fonts.googleapis.com

Phishing Indicators Summary:

Issue	What It Means
Fake Link	The link goes to a strange website, not Bradesco or Livelo.
Spoofed Sender	The email pretends to be from Bradesco, but isn't verified.
Security Checks Failed	SPF, DKIM, and DMARC checks failed – common in phishing.
Bad Formatting	Email headers are messy or broken.
Spelling Mistakes	Several grammar and spelling errors – unusual for real bank emails.
Scare Tactics	Urgent phrases like “points expire today” try to make you act quickly.

This email shows multiple clear signs of phishing. It attempts to create urgency, spoofs a trusted brand, and lures the user to a suspicious link likely used for credential harvesting or malware.
