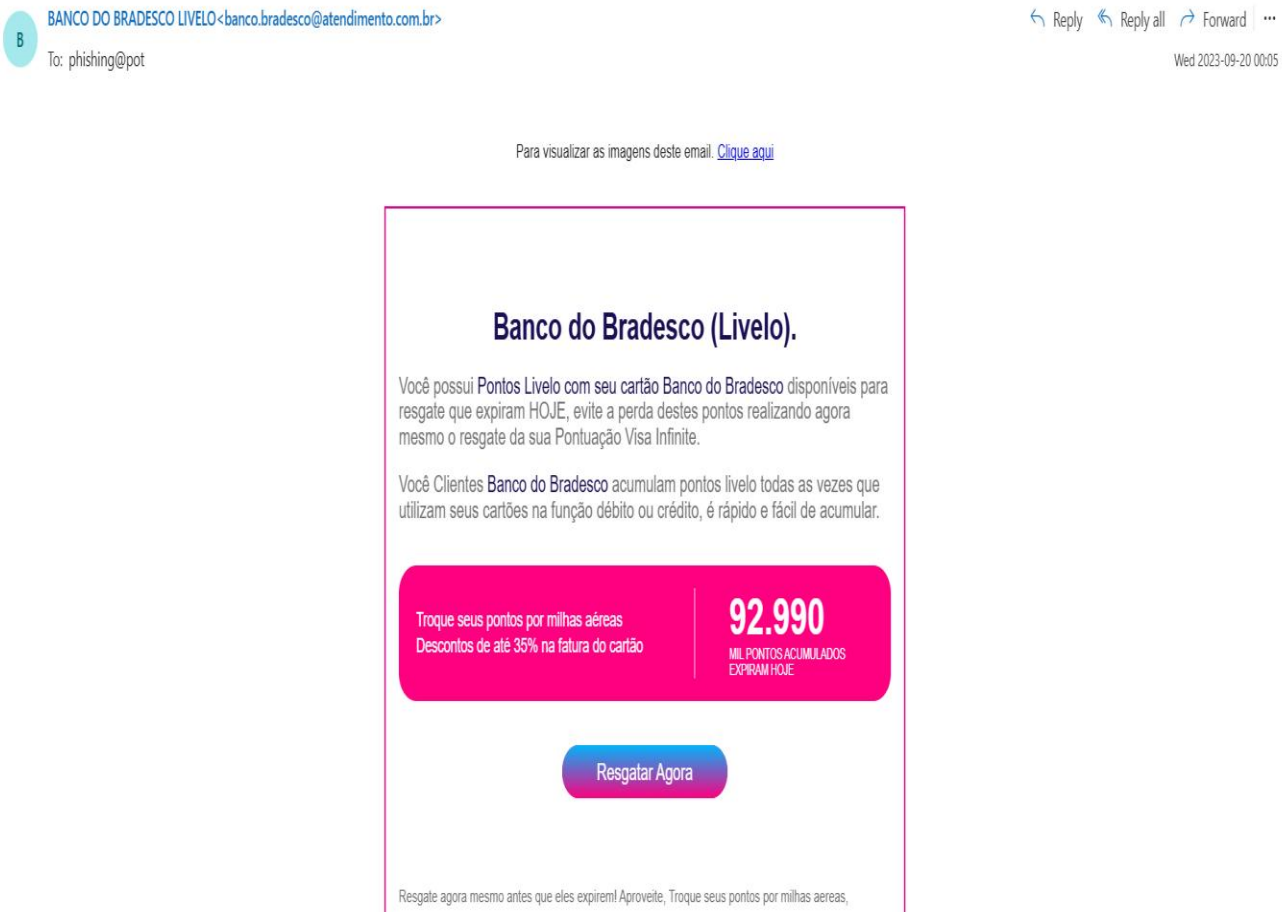
TASK – 2 ELEVATE LABS : ANALYZE A PHISHING EMAIL SAMPLE

OBJECTIVE : IDENTIFY PHISHING CHARACTERISTICS IN A SUSPICIOUS EMAIL SAMPLE.

NAME : PRIYA ROSE

DATE OF SUBMISSION : 06 – 08 -2025



BANCO DO BRADESCO LIVELO<banco.bradesco@atendimento.com.br>

To: phishing@pot

Wed 2023-09-20 00:05

Para visualizar as imagens deste email. Clique aqui

Banco do Bradesco (Livelo).

Você possui Pontos Livelo com seu cartão Banco do Bradesco disponíveis para resgate que expiram HOJE, evite a perda destes pontos realizando agora mesmo o resgate da sua Pontuação Visa Infinite.

Você Clientes Banco do Bradesco acumulam pontos livelo todas as vezes que utilizam seus cartões na função débito ou crédito, é rápido e fácil de acumular.

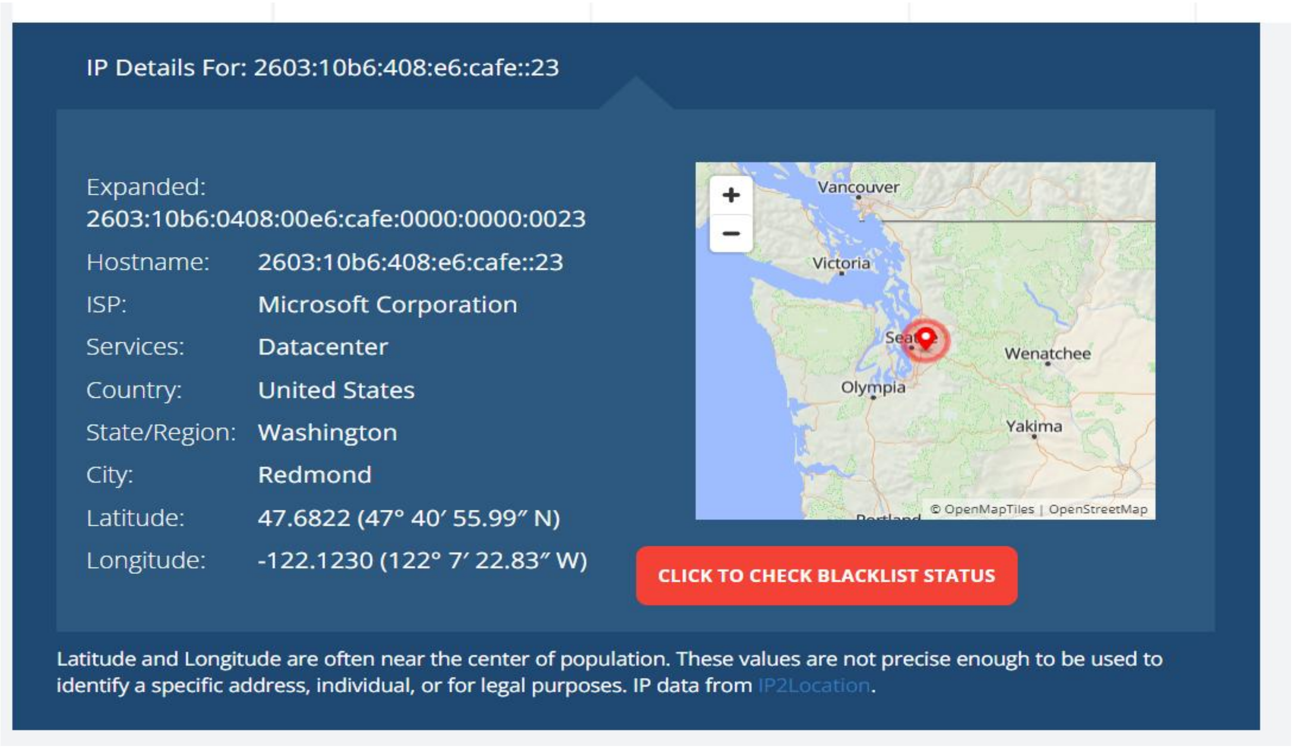
Troque seus pontos por milhas aéreas
Descontos de até 35% na fatura do cartão

92.990
MIL PONTOS ACUMULADOS
EXPIRAM HOJE

Resgate agora mesmo antes que eles expirem! Aproveite, Troque seus pontos por milhas aereas,

- **The mail claims to come from Banco do Bradesco → one of the largest banks in Brazil where they are addressing the feature of Livelo → a Brazilian loyalty points program.**

- **By checking the ip address the location actually turned out to be in United States**



IP Details For: 2603:10b6:408:e6:cafe::23

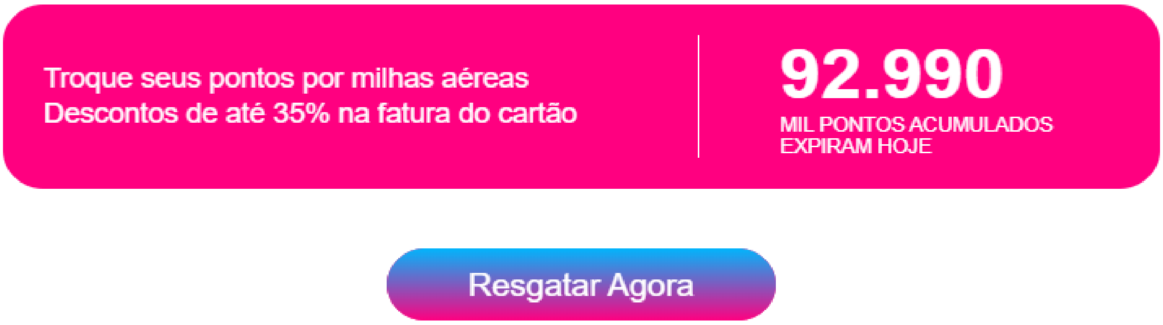
Expanded:
2603:10b6:0408:00e6:cafe:0000:0000:0023

Hostname:	2603:10b6:408:e6:cafe::23
ISP:	Microsoft Corporation
Services:	Datacenter
Country:	United States
State/Region:	Washington
City:	Redmond
Latitude:	47.6822 (47° 40′ 55.99″ N)
Longitude:	-122.1230 (122° 7′ 22.83″ W)

+
−
Vancouver
Victoria
Seattle
Wenatchee
Olympia
Yakima
Portland
© OpenMapTiles | OpenStreetMap
CLICK TO CHECK BLACKLIST STATUS

Latitude and Longitude are often near the center of population. These values are not precise enough to be used to identify a specific address, individual, or for legal purposes. IP data from IP2Location.

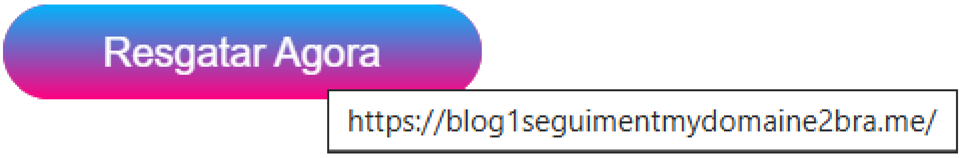
- **The email had malicious links.**



Troque seus pontos por milhas aéreas
Descontos de até 35% na fatura do cartão

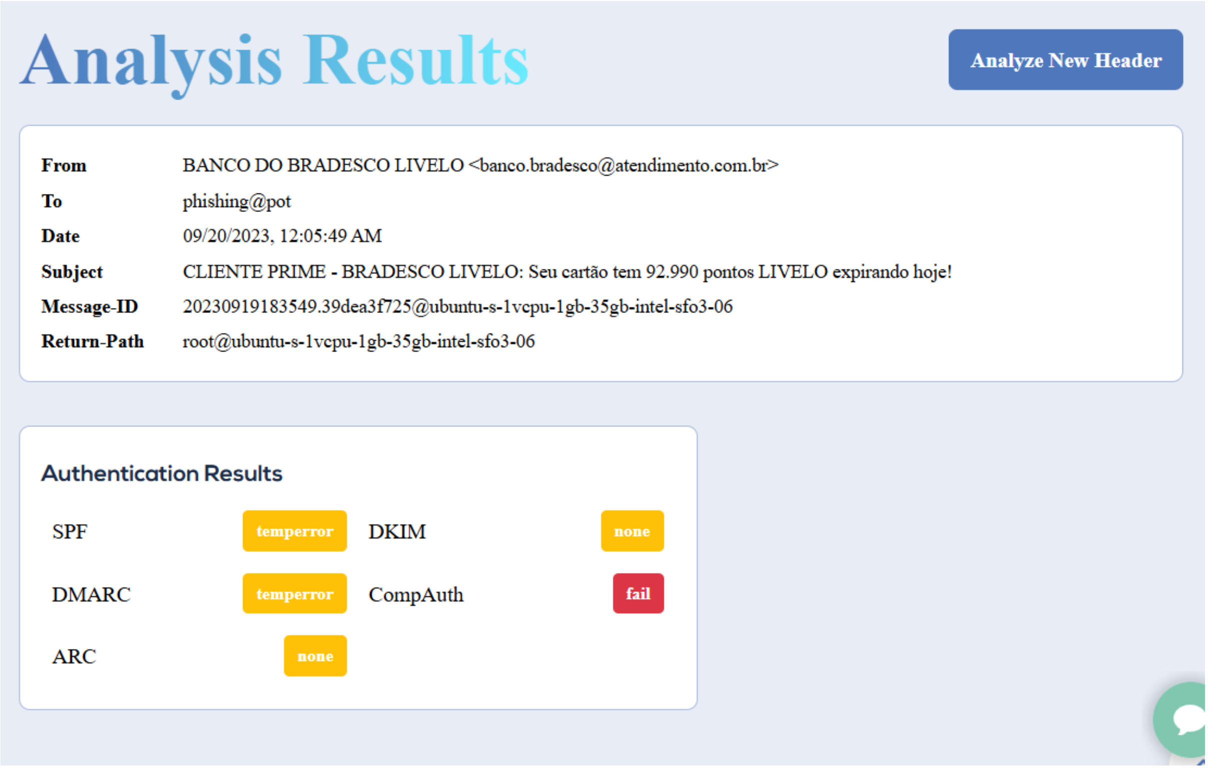
92.990
MIL PONTOS ACUMULADOS
EXPIRAM HOJE

- **The real link :**



https://blog1seguimentmydomaine2bra.me/

- **Email header analysis :**

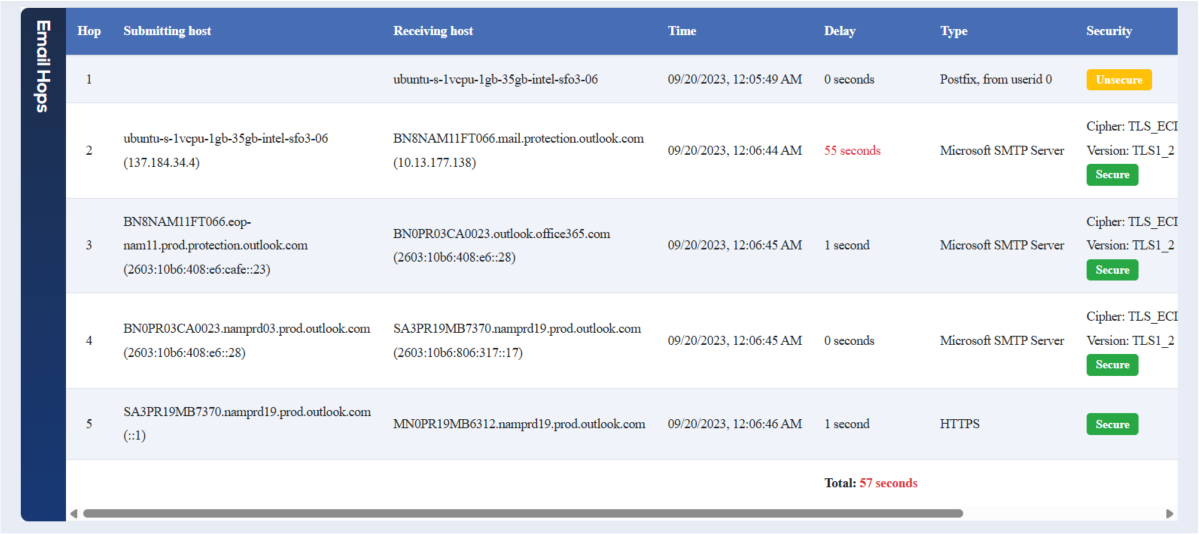


Analysis Results

From	BANCO DO BRADESCO LIVELO <banco.bradesco@atendimento.com.br>
To	phishing@pot
Date	09/20/2023, 12:05:49 AM
Subject	CLIENTE PRIME - BRADESCO LIVELO: Seu cartão tem 92.990 pontos LIVELO expirando hoje!
Message-ID	20230919183549.39dea3f725@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06
Return-Path	root@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06

Authentication Results

SPF	temperror	DKIM	none
DMARC	temperror	CompAuth	fail
ARC	none		



Email Hops

Hop	Submitting host	Receiving host	Time	Delay	Type	Security
1		ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06	09/20/2023, 12:05:49 AM	0 seconds	Postfix, from userid 0	Unsecure
2	ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06 (137.184.34.4)	BN8NAM11FT066.mail.protection.outlook.com (10.13.177.138)	09/20/2023, 12:06:44 AM	55 seconds	Microsoft SMTP Server	Cipher: TLS_ECI Version: TLS1_2 Secure
3	BN8NAM11FT066.eop-nam11.prod.protection.outlook.com (2603:10b6:408:e6:cafe::23)	BN0PR03CA0023.outlook.office365.com (2603:10b6:408:e6::28)	09/20/2023, 12:06:45 AM	1 second	Microsoft SMTP Server	Cipher: TLS_ECI Version: TLS1_2 Secure
4	BN0PR03CA0023.namprd03.prod.outlook.com (2603:10b6:408:e6::28)	SA3PR19MB7370.namprd19.prod.outlook.com (2603:10b6:806:317::17)	09/20/2023, 12:06:45 AM	0 seconds	Microsoft SMTP Server	Cipher: TLS_ECI Version: TLS1_2 Secure
5	SA3PR19MB7370.namprd19.prod.outlook.com (::1)	MN0PR19MB6312.namprd19.prod.outlook.com	09/20/2023, 12:06:46 AM	1 second	HTTPS	Secure
				Total: 57 seconds		

1. SPF (Sender Policy Framework) – temperror

- **Meaning:** The SPF check couldn’t be completed because of a temporary DNS or server issue.
- **Impact:** The receiving mail server couldn’t confirm whether the sending IP is authorized. This doesn’t always mean spam — it could be a DNS timeout or temporary outage.
- **Fix:** Check the SPF DNS record for the sending domain and ensure DNS servers are reachable. Retest later to see if the issue was temporary.

---

2. DKIM (DomainKeys Identified Mail) – none

- **Meaning:** The email had no DKIM signature, so authenticity of the content couldn’t be cryptographically verified.
- **Impact:** Makes the message more likely to fail DMARC if SPF also fails.
- **Fix:** Enable DKIM signing on the sending domain’s email system.

---

3. DMARC (Domain-based Message Authentication, Reporting, and Conformance) – temperror

- **Meaning:** The DMARC policy couldn’t be evaluated because of a temporary DNS or server issue (similar to SPF temperror).
- **Impact:** The receiver couldn’t determine if the email met the sending domain’s authentication policy.
- **Fix:** Ensure the DMARC DNS record is published correctly and DNS resolution is reliable.

---

4. CompAuth (Composite Authentication) – fail

- **Meaning:** Microsoft’s internal composite authentication (which combines SPF, DKIM, DMARC, ARC) determined the email isn’t trustworthy.
- **Impact:** Likely to be treated as suspicious or sent to junk.
- **Fix:** Address SPF, DKIM, and DMARC issues first.

---

5. ARC (Authenticated Received Chain)

- **Meaning:** No result shown, likely meaning either not present or not evaluated. ARC helps preserve authentication results when emails are forwarded

Summarising Phishing traits found in the email :

Phishing Traits Found

1. **Brand impersonation** – Claims to be from *Banco do Bradesco* and references *Livelo*, both legitimate Brazilian services.
2. **Geolocation mismatch** – IP trace showed the sender's location as United States, not Brazil.
3. **Malicious links** – Contained hidden URLs that likely lead to phishing or malware sites.
4. **Authentication failures** –
    - SPF: temperror (check couldn't be completed).
    - DKIM: none (no signature to verify authenticity).
    - DMARC: temperror (policy couldn't be evaluated).
    - CompAuth: fail (overall authentication check failed).
    - ARC: not present/evaluated.
5. **Trustworthiness compromised** – Lack of proper authentication combined with suspicious links makes the email highly untrustworthy.
6. **Potential social engineering** – Uses urgency (points expiring today) to pressure quick action.