🛡 Phishing Email Analysis Report

1. Case Summary

- **Date of Analysis**: July 22, 2025
- **Analyst**: Michele Covi
- **Type of Threat**: Phishing with sender spoofing
- **Objective**: Identify the true origin of the email and assess the legitimacy of its headers
- **Tools Used**:
  - Sublime Text (for raw header inspection)
  - VirusTotal (for IP reputation)
  - AbuseIPDB (for abuse reports and ISP info)
  - MXToolbox (for email authentication checks)

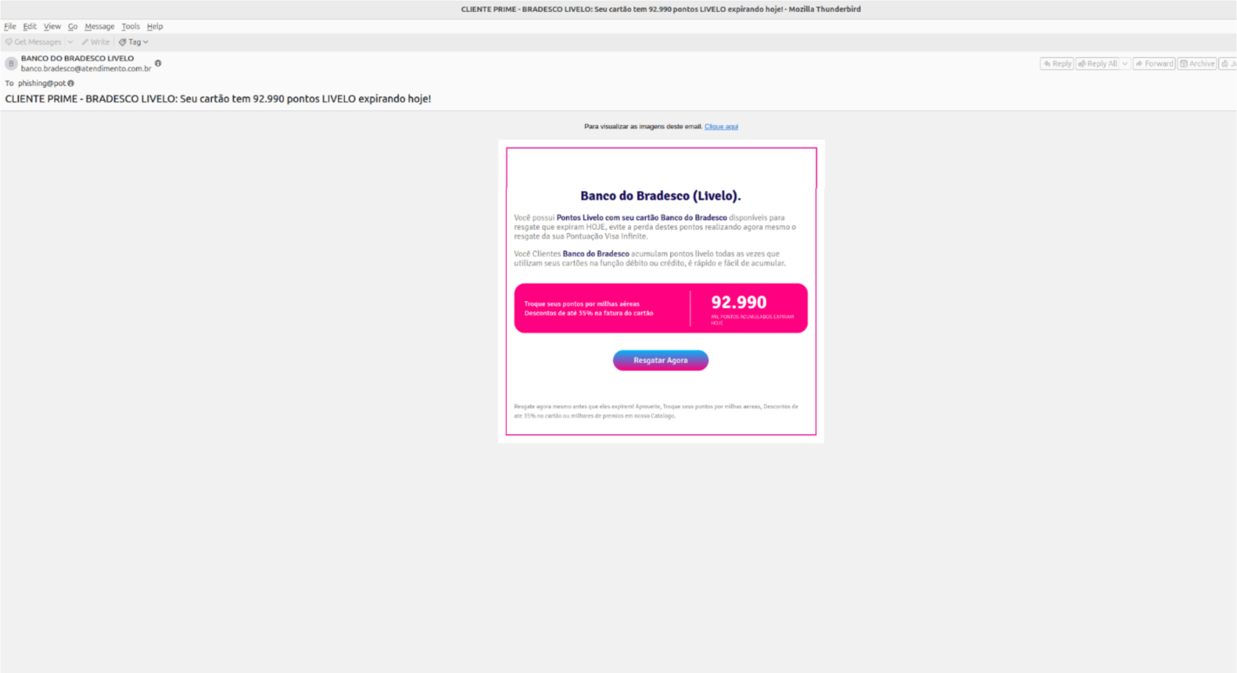
2. Visual Appearance of the Email

When the phishing email is opened in a standard email client (such as Mozilla Thunderbird), it presents itself as a legitimate message from Banco do Bradesco (Livelo). The design mimics official bank communication, using:

- The Bradesco branding and colors
- A strong call-to-action button ("Resgatar Agora" – "Redeem Now")
- A sense of urgency, stating that "92,990 points are expiring today"
- Brazilian Portuguese language targeting local users
- A spoofed sender name and email: BANCO DO BRADESCO LIVELO <banco.bradesco@atendimento.com.br>

This approach is designed to build user trust and provoke immediate action, increasing the risk of credential theft or malware infection.

Figure 1 – Visual appearance of the phishing email in Thunderbird.
The email pretends to come from Bradesco and includes a fake reward with a CTA button to lure users.



CLIENTE PRIME - BRADESCO LIVELO: Seu cartão tem 92.990 pontos LIVELO expirando hoje! - Mozilla Thunderbird

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

To phishing@pot

CLIENTE PRIME - BRADESCO LIVELO: Seu cartão tem 92.990 pontos LIVELO expirando hoje!

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

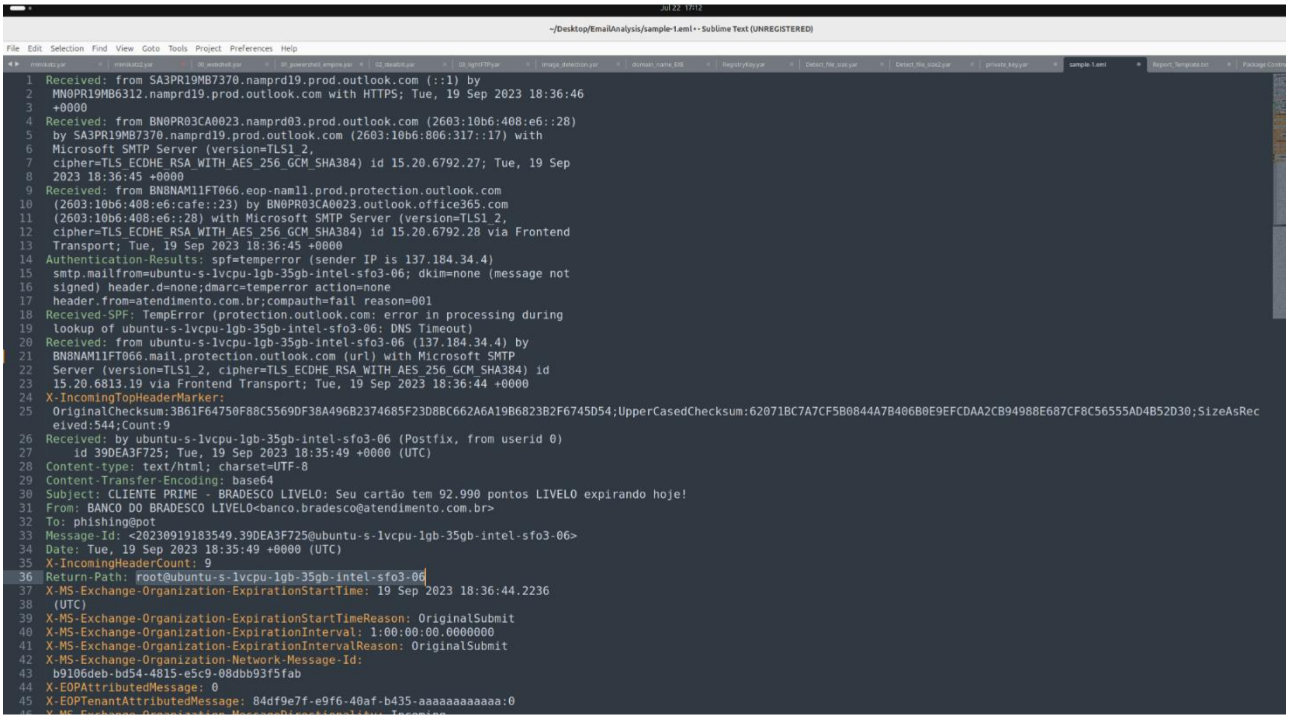
Resgate agora mesmo antes que eles expirem! Aproveite, Troque seus pontos por milhas aereas, Descontos de ate 35% no cartão ou milhares de premios em nosso Catalogo.

3. Email Overview

Field	Value
Subject	CLIENTE PRIME - BRADESCO LIVELLO: Seu cartão tem 92.990 pontos LIVELO expirando hoje!
From	Same as displayed in client view (spoofed Bradesco sender)
To	phishing@pot
Return-Path	root@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06
Content-Type	text/html; charset=UTF-8

Figure 2 – Full email headers opened in Sublime Text

This view exposes raw SMTP headers including the Received, Return-Path, and authentication fields. It reveals the sender IP and spoofed domain, forming the basis of the analysis.



```
Received: from SA3PR19MB7370.namprd19.prod.outlook.com (::1) by
 MN0PR19MB6312.namprd19.prod.outlook.com with HTTPS; Tue, 19 Sep 2023 18:36:46
 +0000
Received: from BN0PR03CA0023.namprd03.prod.outlook.com (2603:10b6:408:e6::28)
 by SA3PR19MB7370.namprd19.prod.outlook.com (2603:10b6:806:317::17) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6792.27; Tue, 19 Sep
 2023 18:36:45 +0000
Received: from BN8NAM11FT066.eop-nam11.prod.protection.outlook.com
 (2603:10b6:408:e6:cafe::23) by BN0PR03CA0023.outlook.office365.com
 (2603:10b6:408:e6::28) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6792.28 via Frontend
 Transport; Tue, 19 Sep 2023 18:36:45 +0000
Authentication-Results: spf=temperror (sender IP is 137.184.34.4)
 smtp.mailfrom=ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06; dkim=none (message not
 signed) header.d=none;dmarc=temperror action=none
 header.from=atendimento.com.br;compauth=fail reason=001
Received-SPF: TempError (protection.outlook.com: error in processing during
 lookup of ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06: DNS Timeout)
Received: from ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06 (137.184.34.4) by
 BN8NAM11FT066.mail.protection.outlook.com (url) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
 15.20.6813.19 via Frontend Transport; Tue, 19 Sep 2023 18:36:44 +0000
X-IncomingTopHeaderMarker:
 OriginalChecksum:3B61F64750F88C5569DF38A496B2374685F23D8BC662A6A19B6823B2F6745D54;UpperCasedChecksum:62071BC7A7CF5B0844A7B406B0E9EFCDAA2CB94988E687CF8C56555AD4B52D30;SizeAsRec
 eived:544;Count:9
Received: by ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06 (Postfix, from userid 0)
    id 39DEA3F725; Tue, 19 Sep 2023 18:35:49 +0000 (UTC)
Content-type: text/html; charset=UTF-8
Content-Transfer-Encoding: base64
Subject: CLIENTE PRIME - BRADESCO LIVELO: Seu cartão tem 92.990 pontos LIVELO expirando hoje!
From: BANCO DO BRADESCO LIVELO<banco.bradesco@atendimento.com.br>
To: phishing@pot
Message-Id: <20230919183549.39DEA3F725@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06>
Date: Tue, 19 Sep 2023 18:35:49 +0000 (UTC)
X-IncomingHeaderCount: 9
Return-Path: root@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06
X-MS-Exchange-Organization-ExpirationStartTime: 19 Sep 2023 18:36:44.2236
 (UTC)
X-MS-Exchange-Organization-ExpirationStartTimeReason: OriginalSubmit
X-MS-Exchange-Organization-ExpirationInterval: 1:00:00:00.0000000
X-MS-Exchange-Organization-ExpirationIntervalReason: OriginalSubmit
X-MS-Exchange-Organization-Network-Message-Id:
 b9106deb-bd54-4815-e5c9-08dbb93f5fab
X-EOPAttributedMessage: 0
X-EOPTenantAttributedMessage: 84df9e7f-e9f6-40af-b435-aaaaaaaaaaaa:0
X-MS-Exchange-Organization-MessageDirectionality: Incoming
```

4. Header Analysis

Key Headers:

Extracted from headers (see Figure 2): the Return-Path and originating IP indicate spoofing via a DigitalOcean VPS, and SPF/DKIM/DMARC validations fail.

- **Origin IP**: 137.184.34.4
- **SMTP Server:** Postfix running on a DigitalOcean VPS (hostname: ubuntu-s-1vcpu...)
- **Authentication**: SPF, DKIM, and DMARC all failed or not aligned → classic sign of spoofing.

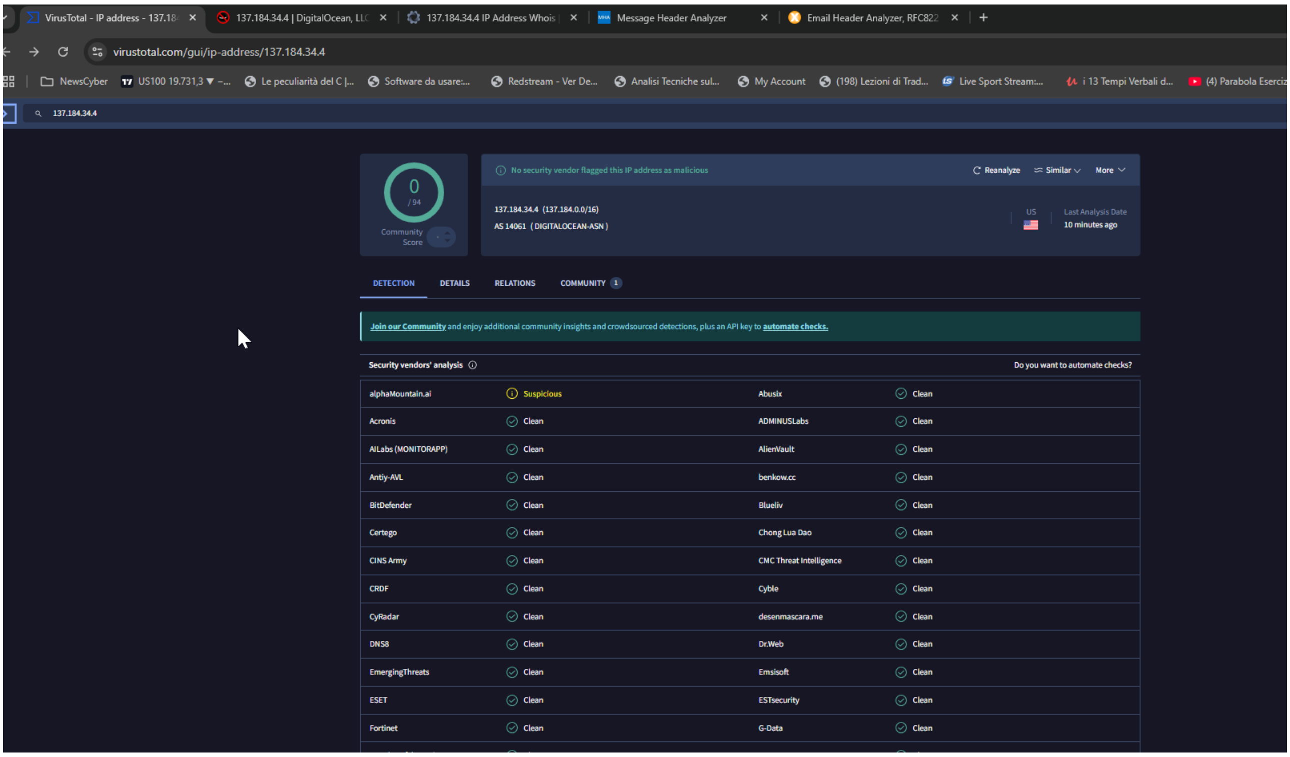
5. IP Reputation and Ownership

VirusTotal

- **Reputation**: No detections by AV vendors
- **Community Score**: 0 / 94
- **Note**: Marked as "Suspicious" by one engine

Figure 3 – VirusTotal IP reputation result for 137.184.34.4

The IP address is not flagged by antivirus engines but is considered suspicious by at least one scanner.



0 / 94
Community Score

No security vendor flagged this IP address as malicious

137.184.34.4 (137.184.0.0/16)
AS 14061 (DIGITALOCEAN-ASN)

US

Last Analysis Date
10 minutes ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

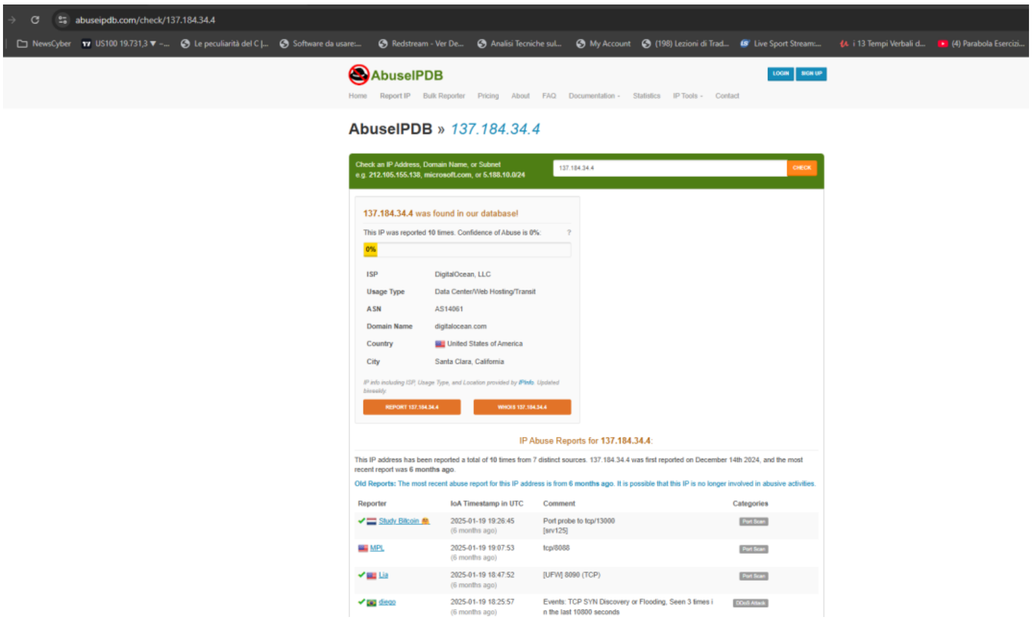
alphaMountain.ai	Suspicious	Abusix	✓ Clean
Acronis	✓ Clean	ADMINUSLabs	✓ Clean
AILabs (MONITORAPP)	✓ Clean	AlienVault	✓ Clean
Antiy-AVL	✓ Clean	benkow.cc	✓ Clean
BitDefender	✓ Clean	Blueliv	✓ Clean
Certego	✓ Clean	Chong Lua Dao	✓ Clean
CINS Army	✓ Clean	CMC Threat Intelligence	✓ Clean
CRDF	✓ Clean	Cyble	✓ Clean
CyRadar	✓ Clean	desenmascara.me	✓ Clean
DNS8	✓ Clean	Dr.Web	✓ Clean
EmergingThreats	✓ Clean	Emsisoft	✓ Clean
ESET	✓ Clean	ESTsecurity	✓ Clean
Fortinet	✓ Clean	G-Data	✓ Clean

6. AbuseIPDB

- **Owner**: DigitalOcean, LLC
- **Location**: United States – Santa Clara, California
- **Reported abuse**: 10 reports, including port scanning and DDoS activity

Figure 4 – AbuseIPDB report for the sender IP

The IP is hosted by DigitalOcean and has 10 abuse reports, including activity like port scanning and potential DDoS.



AbuseIPDB » 137.184.34.4

Check an IP Address, Domain Name, or Subnet
e.g. **212.105.155.138**, **microsoft.com**, or **5.188.10.0/24**

137.184.34.4

137.184.34.4 was found in our database!

This IP was reported **10** times. Confidence of Abuse is **0%**: ?

ISP	DigitalOcean, LLC
Usage Type	Data Center/Web Hosting/Transit
ASN	AS14061
Domain Name	digitalocean.com
Country	United States of America
City	Santa Clara, California

IP info including ISP, Usage Type, and Location provided by IPInfo. Updated biweekly.

IP Abuse Reports for **137.184.34.4**:

This IP address has been reported a total of **10** times from 7 distinct sources. 137.184.34.4 was first reported on December 14th 2024, and the most recent report was **6 months ago**.

Old Reports: The most recent abuse report for this IP address is from **6 months ago**. It is possible that this IP is no longer involved in abusive activities.

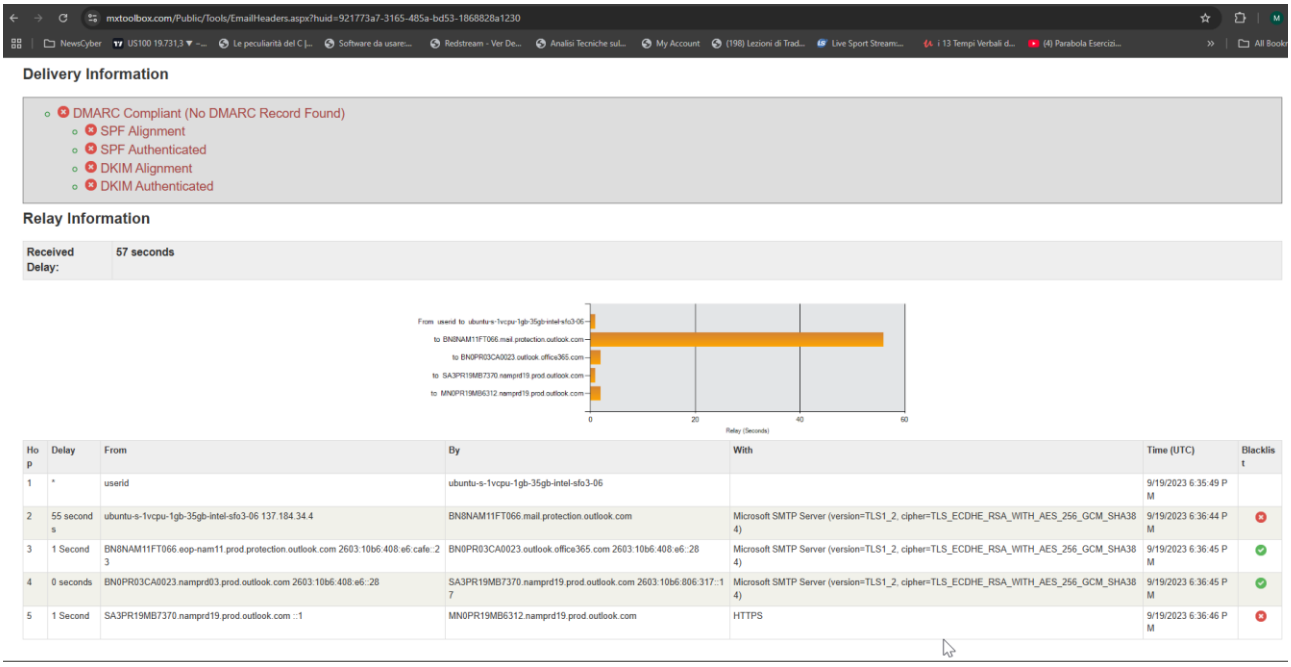
Reporter	IoA Timestamp in UTC	Comment	Categories
✓ Study Bitcoin	2025-01-19 19:26:45 (6 months ago)	Port probe to tcp/13000 [srv125]	Port Scan
MPL	2025-01-19 19:07:53 (6 months ago)	tcp/8088	Port Scan
✓ Lia	2025-01-19 18:47:52 (6 months ago)	[UFW] 8090 (TCP)	Port Scan
✓ diego	2025-01-19 18:25:57 (6 months ago)	Events: TCP SYN Discovery or Flooding, Seen 3 times i n the last 10800 seconds	DDoS Attack

7. Email Authentication Check (via MXToolbox)

- ✗ **SPF**: Fail
- ✗ **DKIM**: Not authenticated
- ✗ **DMARC**: No record found
- ✗ **SPF/DKIM Alignment**: Fails
- ☑ **Sender Origin Delay**: 57 seconds from local Postfix to Microsoft servers

Figure 5 – MXToolbox header analysis report

Authentication mechanisms SPF, DKIM, and DMARC all fail. This strongly confirms that the email was spoofed and unauthenticated.


mxtoolbox.com/Public/Tools/EmailHeaders.aspx?huid=921773a7-3165-485a-bd53-1868828a1230
NewsCyber
US100 19.731,3 ▼ -...
Le peculiarità del C |...
Software da usare:...
Redstream - Ver De...
Analisi Tecniche sul...
My Account
(198) Lezioni di Trad...
Live Sport Stream:...
i 13 Tempi Verbali d...
(4) Parabola Esercizi...
All Book
From userid to ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06
to BN8NAM11FT066.mail.protection.outlook.com
to BN0PR03CA0023.outlook.office365.com
to SA3PR19MB7370.namprd19.prod.outlook.com
to MN0PR19MB6312.namprd19.prod.outlook.com
0
20
40
60
Relay (Seconds)

Delivery Information

- ✗ DMARC Compliant (No DMARC Record Found)
  - ✗ SPF Alignment
  - ✗ SPF Authenticated
  - ✗ DKIM Alignment
  - ✗ DKIM Authenticated

Relay Information

Received Delay:	57 seconds

Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	userid	ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06		9/19/2023 6:35:49 PM	
2	55 seconds	ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06 137.184.34.4	BN8NAM11FT066.mail.protection.outlook.com	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	9/19/2023 6:36:44 PM	✗
3	1 Second	BN8NAM11FT066.eop-nam11.prod.protection.outlook.com 2603:10b6:408:e6:cafe::23	BN0PR03CA0023.outlook.office365.com 2603:10b6:408:e6::28	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	9/19/2023 6:36:45 PM	✓
4	0 seconds	BN0PR03CA0023.namprd03.prod.outlook.com 2603:10b6:408:e6::28	SA3PR19MB7370.namprd19.prod.outlook.com 2603:10b6:806:317::17	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	9/19/2023 6:36:45 PM	✓
5	1 Second	SA3PR19MB7370.namprd19.prod.outlook.com ::1	MN0PR19MB6312.namprd19.prod.outlook.com	HTTPS	9/19/2023 6:36:46 PM	✗

8. Analysis Conclusion

- The email is **not legitimately sent from Bradesco**.
- It is a **spoofed message** delivered through a **DigitalOcean-hosted VPS**.
- The Return-Path and Received headers clearly identify a **Linux Postfix setup**, likely scripted or automated for bulk phishing.
- The combination of a spoofed sender, failed authentication, and an origin from a known VPS (DigitalOcean) confirms the malicious intent of this phishing attempt.

9. Suggested Mitigations

- Report the IP address and server to DigitalOcean Abuse Contact
- Block IP 137.184.34.4 at the mail server or firewall level
- Add the spoofed domain bradescoseg.br to your **SPF/DMARC monitoring rules**
- Use this example to train users on how phishing can appear deceptively legitimate