1) INFORMATION ON SENT EMAIL

|  |  |
| --- | --- |
| 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!  Which translates to “PRIME CUSTOMER - BRADESCO LIVELO: Your card has 92,990 LIVELO points expiring today!” |
| DATE/time | 19 Sep 2023 18:36:44.1298 (UTC) |
| FROM(displayed sender) | banco.bradesco@atendimento.com.br |
| RETURN PATH(from- actual address) | root@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06 |
| EXTRACTED URL’s | <https://blog1seguimentmydomaine2bra.me/> |
| EXTRACTED DOMAINS | 1) blog1seguimentmydomaine2bra.me  2) fonts.gstatic.com  3) fonts.googleapis.com |

2) EMAIL HEADER ANALYSIS

Security header- “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”

|  |  |  |
| --- | --- | --- |
| *HEADER* | *VALUE OBSERVED* | *PHISHING INDICATOR* |
| SPF | temperror | SPFcheck couldn’t validate. Real domain not verified. |
| DKIM | None(message not signed) | Email not signed. Cannot verify authenticity. |
| DMARC | Temperror, action=none | Check failed. No alignment with sender domain. |
| RETURN PATH | root@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06 | Mismatched with display sender. Indicates spoofing. |

**Observation:** Header analysis should multiple authentication failures and mismatched sender information. Indicates phishing.

3)SENDER AUTHENTICITY

-Display name of sender is : [banco.bradesco@atendimento.com.br,](mailto:banco.bradesco@atendimento.com.br) but the actual sending server is a personal VPS: root@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06

- No SPF/DKIM/DMARC VALIDATION Available: Cannot Confirm Legitimacy

-Domain name atendimento.com.br does not match sending IP/server.

4)SUSPICIOUS LINKS

-All the attached links do not belong to/are not related to BRADESCO.

\*\*RED FLAGS- Mismatched URL’s.

5) MESSAGE CONTENT ANALYSIS

-Urgency / Threats: Mentions points expiring *“HOJE”* : pressures recipient to act quickly.

-Request for Action: Prompts user to click a link to redeem points.

-Doesn’t address recipient by name. It’s a generic addressing.

6)OVERALL RISK ASSESSMENT

-Risk Rating: High

-Rationale: Multiple phishing indicators detected:

* + Sender spoofing
  + Authentication failures (SPF/DKIM/DMARC)
  + Mismatched and suspicious URLs
  + Urgent call-to-action and social engineering language

7)ACTIONS TAKEN

- EML analyzed in a safe environment using header and link inspection.

- URLs extracted but not clicked.(only hovered)

- No attachments executed.

- Findings documented in this report.

8) SUMMARY

-Sender domain does not match the actual sending server.

-SPF/DKIM/DMARC checks failed.

- Suspicious domain used for all links.

- Urgency and reward used to pressure recipient.