**Task 2: Analyze a Phishing Email Sample.**

* **Subject:** “CLIENTE PRIME - BRADESCO LIVELO: Seu cartão tem 92.990 pontos LIVELO expirando hoje!”
* **Pretends to be:** Banco Bradesco (Brazilian bank)
* **Purpose:** To make the victim click on a fake link to “claim” or “save” their Livelo points.

This is a **phishing lure** — it uses urgency (“expiring today”) and brand impersonation to trick users.

|  |  |  |
| --- | --- | --- |
| **Field** | **What It Shows** | **Why It’s Suspicious** |
| From: | BANCO DO BRADESCO LIVELO <banco.bradesco@atendimento.com.br> | Domain looks generic, **not** from bradesco.com.br |
| Return-Path: | root@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06 | Sent from a **DigitalOcean Ubuntu server**, not a bank |
| X-Sender-IP: | 137.184.34.4 | Belongs to DigitalOcean (common for phishing VPS servers) |
| Received-SPF: | TempError | SPF (Sender Policy Framework) check failed |
| DKIM: | none | No DKIM signature — not authenticated |
| DMARC: | temperror | DMARC validation failed |
| Authentication-Results: | compauth=fail reason=001 | Microsoft confirms: **authentication failed** |
| X-MS-Exchange-Organization-SCL: | 5 | Spam Confidence Level = 5 (high) |

**All indicators point to spoofing** — it tries to look legitimate but fails authentication.

* Suspicious link: https://blog1seguimentmydomaine2bra.me/

|  |  |
| --- | --- |
| **Technique** | **Description** |
| **Brand impersonation** | Uses Bradesco’s name and style |
| **Sense of urgency** | Points “expiring today” |
| **Malicious redirect** | Fake domain, not official Livelo or Bradesco |
| **Spoofed sender** | Random Ubuntu VPS pretending to be official |
| **No authentication** | SPF, DKIM, and DMARC all failed |
| **HTML obfuscation** | Base64 encoding hides the malicious link |