Phishing Email Analysis Report

Overview:

This report analyzes a suspected phishing email claiming to be from 'Banco do Bradesco Livelo'. The purpose is to identify indicators of phishing based on header inspection, content analysis, and sender verification.

Phishing Indicators Found:

1. Spoofed Sender Email Address

The sender name is 'BANCO DO BRADESCO LIVELO' but the actual address is banco.bradesco@atendimento.com.br with a return-path of root@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06. This indicates spoofing.

2. Failed Email Authentication (SPF, DKIM, DMARC)

The SPF check returned 'temperror', DKIM is missing, and DMARC also failed. These indicate that the email origin is not verified.

3. Suspicious Link

The email contains a hyperlink to 'https://blog1seguimentmydomaine2bra.me/', which is not related to Bradesco or any known legitimate domain.

4. Urgent and Threatening Language

Subject line and body urge the recipient to act immediately: 'Seu cartão tem 92.990 pontos expirando HOJE!'. This urgency is used to pressure the recipient.

5. Mismatched URLs

The link text appears trustworthy, but when hovered over, it points to a suspicious domain that does not match the sender.

6. Spelling and Grammar Issues

The email contains minor grammatical errors and awkward sentence structures, which are common in phishing attempts.

Conclusion:

The email contains multiple phishing indicators including spoofed sender, failed authentication, misleading links, and urgency tactics. Based on the analysis, this email should be classified as a phishing attempt and should not be trusted or interacted with.