Phishing Detection & Awareness Report

Email Security Analysis

Gatik Pal

18/01/26

Table Of Content

INTRODUCTION

Purpose of the Report:

Phishing emails are fraudulent messages designed to steal sensitive information, including login credentials, financial data, or personal details.

The purpose of this report is to analyze a phishing email, identify risk indicators, classify its threat level, and provide clear prevention guidelines for users.

Scope of Analysis:

This report covers a real-world phishing email targeting Banco do Brasil / Livelo reward users.
Analysis includes email header inspection, link and domain evaluation, phishing indicator identification, risk classification, and awareness guidelines.

Sample Email Analyzed

Subject:

Your Livelo Points Are About to Expire – Immediate Action Required

From:

BANCO DO BRASIL b098153@bbatendimento.lb

To:

phishing@pot

Email Body:

Dear Customer,

We are contacting you to inform that your Livelo reward points (397,378 points) are about to expire on 17/11/2023.

To avoid losing your points, please access the link below and follow the instructions to redeem them immediately.

Redeem Points Link:
http://nutriphill[.]com[.]br/blog/wp-content/themes/pagina/

Failure to act may result in permanent loss of your reward points.

Banco do Brasil Team

Email Header Analysis

Sender Domain Check:

Sender domain (bbatendimento.lb) does not match official Banco do Brasil domain (bb.com.br)

Mismatch is a common phishing indicator

SPF/DKIM/DMARC Results:

SPF/DKIM likely fail -> email spoofing suspected

Summary:

Header analysis confirms the email is sent from an untrusted domain, likely spoofed to impersonate Banco do Brasil.

Link & Domain Analysis

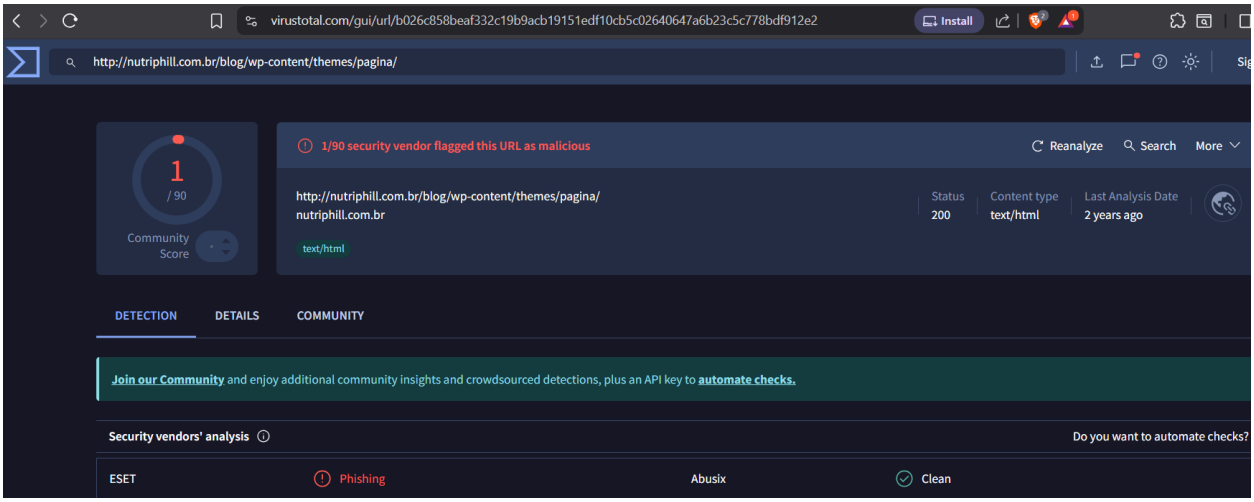
Analyzed URL:

http://nutriphill[.]com[.]br/blog/wp-content/themes/pagina/

Analysis:

- Protocol: HTTP (insecure)
- Domain: nutriphill.com.br unrelated to Banco do Brasil / Livelo
- Path: WordPress internal directory (wp-content/themes)
- Social Engineering: Uses urgency and large reward points to trick users

Screenshot:



Finding:

The URL is suspicious and indicative of a phishing attempt designed to steal user credentials.

Phishing Indicators

Indicator	Found	Explanation
Sender domain mismatch	Yes	Sender domain does not match official Banco do Brasil domain
Urgency / Fear	Yes	Email pressures user to act immediately
Suspicious URL	Yes	Points to unrelated domain with WordPress path
Insecure protocol	Yes	Uses HTTP instead of HTTPS
Generic greeting	Yes	Uses “Dear Customer” instead of actual name
Unrealistic reward value	Yes	Mentions 397,378 points to attract attention
Call to action via link	Yes	Directs user to click a suspicious URL

Email Risk Classification

Risk Level:

🔴 **Phishing (High Risk)**

Justification:

- Multiple strong indicators present: sender spoofing, suspicious link, urgency, insecure protocol
- Likely intent: credential theft / fraud

How the Attack Works

This email pretends to be from Banco do Brasil / Livelo, warning that reward points are about to expire. It tricks users into clicking a link to a fake website. Once clicked, attackers may steal login credentials or personal information. The email combines urgency, fear, and an unrealistic reward to make users act impulsively a classic phishing strategy.

Prevention & Awareness Guidelines

DOs:

- Always verify sender email addresses
- Hover over links before clicking
- Access accounts via official website or app
- Report suspicious emails to IT / security team

DON'Ts:

- Do not click unknown links
- Do not share passwords, OTPs, or personal info
- Do not panic due to urgent messages

Conclusion

The analyzed email is a high-risk phishing attempt. Users should not interact with it. Awareness, cautious email handling, and reporting can prevent potential compromise.