Yespanchi - Email Scan Guardian

Website: https://www.yespanchi.tech
Contact: 9360784554
Address: TM Maistry Street Extn Thiruvanmiyur Chennai

Email Security Analysis Report

File: pasted-email.eml
Generated: 07/10/2025, 12:49:33

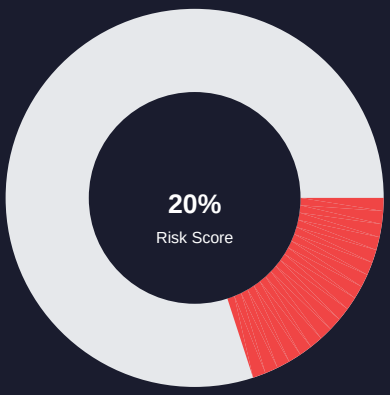
Analysis Summary

Authentication:
- SPF: fail or not present
- DKIM: fail or not present
- DMARC: pass

Security Issues: 4 Issues

Phishing Risk: High (70%)

High	20	70%
Risk Level	Risk Score	Confidence



System Verdict: Suspicious

AI Security Analysis Report

Analysis for: yespanchi.com

Security Report: eka@yespanchi.com

1. Executive Summary

This security report summarizes the analysis of an email sent from eka@yespanchi.com with the subject "pasted-email.eml". The email has failed SPF and DKIM authentication checks, indicating potential spoofing or tampering. Additionally, high-risk phishing indicators were detected, suggesting a possible malicious intent. This report provides a comprehensive assessment of the email's security posture and recommends further investigation to determine the authenticity and legitimacy of the message.

2. Risk Assessment

The risk associated with this email is HIGH due to the failed SPF and DKIM authentication checks, indicating potential spoofing or tampering. The presence of high-risk phishing indicators also increases the likelihood of a malicious attack. Furthermore, the lack of route analysis (0 hops) suggests that the email may have been routed through an unknown or untrusted network.

3. Key Security Findings

- SPF verification failed or missing
- DKIM verification failed or missing
- DMARC result: pass
- High-risk phishing detected (Score: 20)
- High-risk keywords: confidential
- Links found: 3
- Attachments: 1
- Route analysis: 0 hops

4. Recommendations for Further Investigation

To determine the authenticity and legitimacy of this email, further investigation is recommended. This may include:

- Verifying the sender's identity through additional authentication methods or contacting the alleged sender directly
- Analyzing the content and context of the email to identify potential red flags or inconsistencies
- Conducting a thorough scan of attachments for malware or other malicious code
- Reviewing the email's headers and metadata for any suspicious activity or anomalies

5. Overall Verdict

Based on the analysis, this email is classified as SUSPICIOUS due to the failed SPF and DKIM authentication checks, high-risk phishing indicators, and unknown origin IP.

6. Final Recommendation

Given the high risk associated with this email, it is recommended that you exercise extreme caution when interacting with it. Do not open any attachments or click on links until the authenticity of the sender has been verified through additional means. If possible, contact the alleged sender directly to confirm their identity and intentions.