

Yespanchi - Email Scan Guardian

Website: <https://www.yespanchi.tech>

Contact: 9360784554

Address: TM Maistry Street Extn Thiruvanmiyur Chennai



Email Security Analysis Report

File: Show-original.eml

Generated: 07/10/2025, 11:36:29

Analysis Summary

Authentication:

SPF: fail or not present

DKIM: fail or not present

DMARC: fail or not present

Security Issues: 5 Issues

Phishing Risk: High (70%)

High

Risk Level

20

Risk Score

70%

Confidence



System Verdict: Suspicious

AI Security Analysis Report

Analysis for: yespanchi.com

Security Report: eka@yespanchi.com

1. Executive Summary

This email analysis report summarizes the findings of an investigation into an email sent from eka@yespanchi.com with the filename Show-original.eml. The analysis reveals a high-risk phishing detection, failed authentication checks for SPF, DKIM, and DMARC, and the presence of suspicious links.

2. Risk Assessment

The risk assessment for this email is MALICIOUS due to multiple authentication failures (SPF, DKIM, and DMARC) and the presence of high-risk keywords ("confidential"). The lack of authentication checks passing also increases the likelihood of the email being malicious.

3. Key Security Findings

Key findings from the analysis include:

- High-risk phishing detection with a score of 20
- Failed SPF, DKIM, and DMARC authentication checks
- Presence of suspicious links (3)
- No attachments found
- Route analysis indicates 0 hops, suggesting no clear origin or transit information

4. Recommendations for Further Investigation

To further investigate this email, we recommend:

- Verifying the authenticity of the sender's identity through additional means, such as contacting the supposed sender directly to confirm their request
- Analyzing the links found in the email using a reputable link scanner to identify potential malicious destinations
- Reviewing any relevant logs or system records for evidence of suspicious activity related to this email

5. Overall Verdict

Based on the analysis, it is clear that this email poses a significant security risk and should be treated with caution.

6. Final Recommendation

In light of these findings, we strongly recommend taking immediate action to mitigate potential risks associated with this email. This includes:

- Not responding or engaging with the email

-
- Not clicking on any links or opening attachments
 - Reporting the email as suspicious to your organization's security team or IT department
 - Implementing additional security measures to prevent similar emails from reaching your inbox in the future

By taking these precautions, you can help protect yourself and your organization from potential cyber threats.