Email Security Analysis Report

File: pasted-email.eml
Generated: 08/09/2025, 10:46:40

Analysis Summary

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

Security Issues: 2 Issues

Phishing Risk: Medium (40%)

System Verdict: Suspicious

IP: unknown

Security Report: tarch4.com

1. Executive Summary

This security report summarizes the analysis of an email received from the sender domain tarch4.com. The email was found to have failed DMARC authentication, indicating a potential security risk. Additionally, medium-risk phishing was detected, suggesting that the email may be attempting to trick the recipient into divulging sensitive information.

2. Risk Assessment

The risk assessment for this email is categorized as SUSPICIOUS due to the failure of DMARC authentication and the detection of medium-risk phishing. This suggests that the email may not be legitimate or trustworthy, and further investigation is warranted.

3. Key Security Findings

The sender domain tarch4.com has failed DMARC authentication, indicating a potential security risk.

Medium-risk phishing was detected in the email, suggesting that it may be attempting to trick the recipient into divulging sensitive information.

No links or attachments were found in the email.

The route analysis indicates 0 hops, which is normal for an email.

4. Recommendations for Further Investigation

To further investigate this suspicious email, we recommend the following:

Verify the authenticity of the sender domain tarch4.com by checking its DMARC policy and ensuring that it aligns with industry best practices.

Conduct a thorough analysis of the email's content to identify any potential phishing indicators or malicious code.

Check the recipient's email account for any suspicious activity or unauthorized access.

5. Overall Verdict

Based on the security assessment, we conclude that the email from tarch4.com is SUSPICIOUS and may not be legitimate or trustworthy. Further investigation is necessary to determine the true nature of the email and ensure the security of the recipient's email account.

6. Final Recommendation

In light of these findings, we strongly recommend that the recipient exercise extreme caution when interacting with this email. Specifically:

Do not respond to the email or provide any sensitive information.

Do not click on any links or open any attachments.

Report the email as suspicious and consider marking it as spam.

By taking these precautions, you can help protect your email account from potential security risks and maintain a high level of cybersecurity.

> **Final Recommendation**
>
> This email shows suspicious indicators. Exercise caution and verify the sender before taking any action.