Phishing Email Detection & Awareness Report

Cyber Security Internship – Future Interns (2026)

1. Executive Summary

This report presents the analysis of suspicious email samples to identify phishing attacks and improve employee awareness. Multiple spoofed domains and email authentication failures were detected. All samples were classified as high-risk phishing attempts.

2. Scope & Ethics

Only passive analysis methods were used. No malicious links were clicked and no attachments were opened. The investigation focused on headers, domains, and content inspection.

3. Tools Used

- MXToolbox Header Analyzer
- Google Message Header Analyzer
- Browser domain inspection
- Manual review

4. Email Analysis Findings

Email Sample 1 – Secure Account Verify Domain

Risk Level: High (Phishing). The domain shows multiple configuration and DNS issues indicating an untrusted or malicious source.

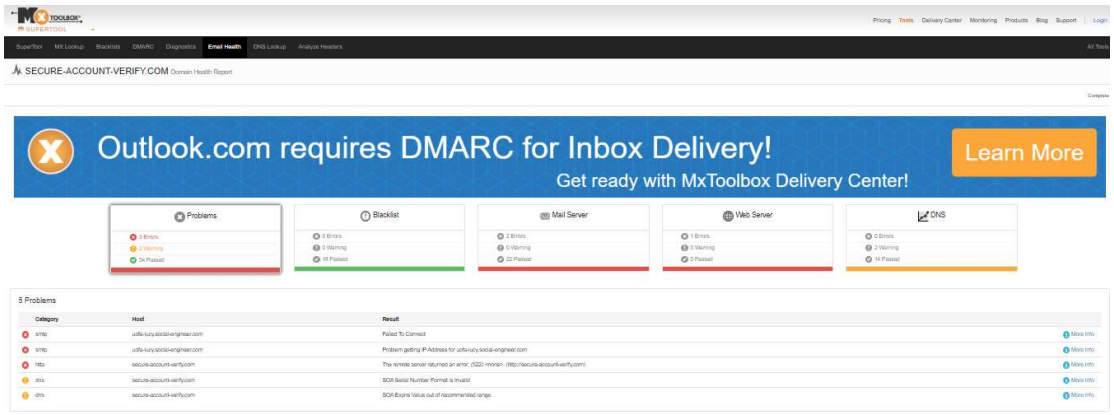

Figure: MXToolbox domain health report showing several problems and warnings.

Email Sample 2 – Microsoft Security Check Domain

Risk Level: High (Phishing). The domain lacks proper SPF, DKIM, and DMARC protection and appears to impersonate Microsoft services.

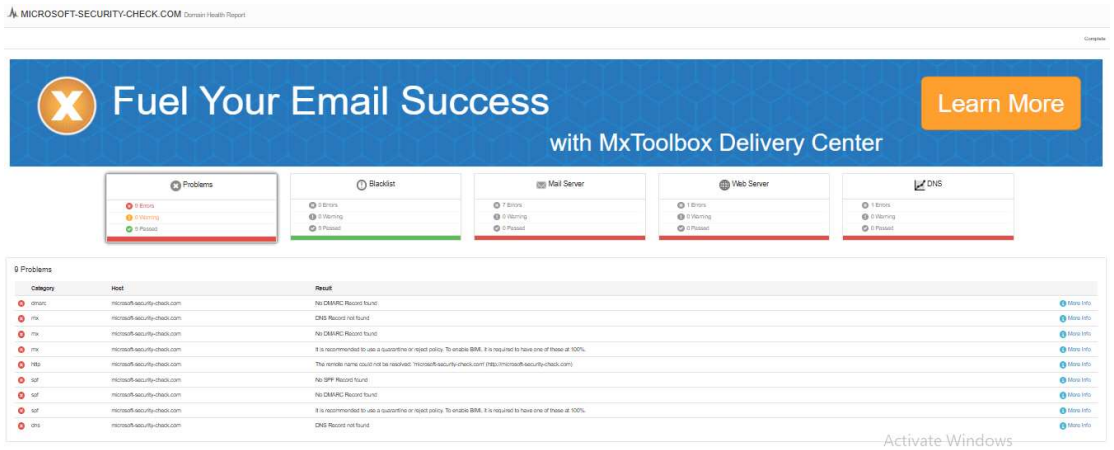

Figure: Domain health results highlighting missing security and authentication records.

Email Sample 3 – Payroll Secure Login Domain

Risk Level: High (Phishing). The domain cannot be resolved correctly and shows DNS failures commonly associated with malicious infrastructure.

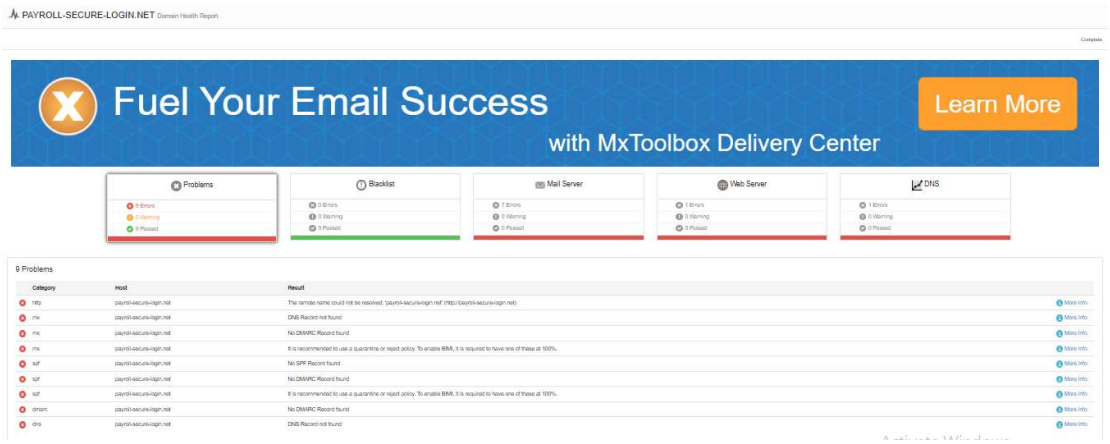

Figure: Domain lookup indicating DNS record failures and configuration problems.

Email Sample 4 – Header Authentication Analysis

Risk Level: High (Phishing). SPF, DKIM, and DMARC checks failed, confirming that the sender cannot be authenticated.

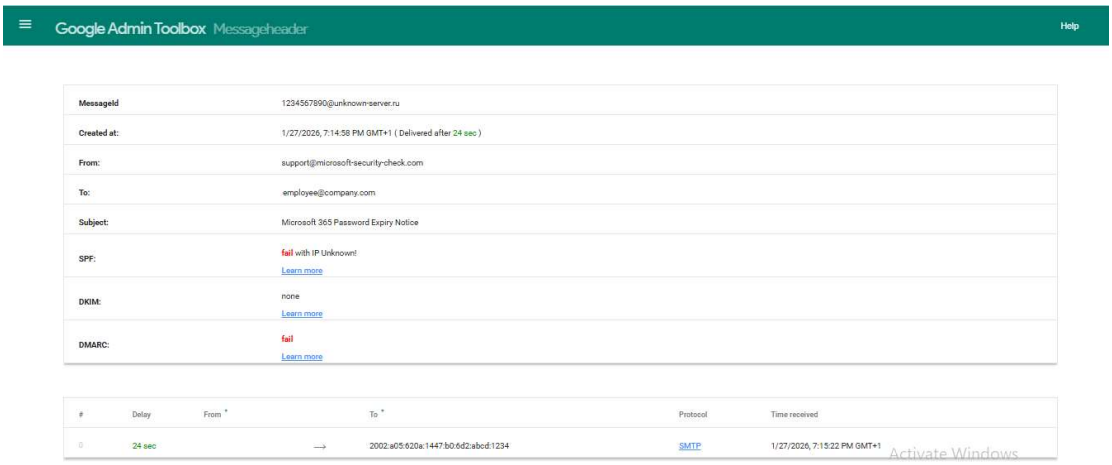

Figure: Google Header Analyzer showing SPF fail, DKIM none, DMARC fail.

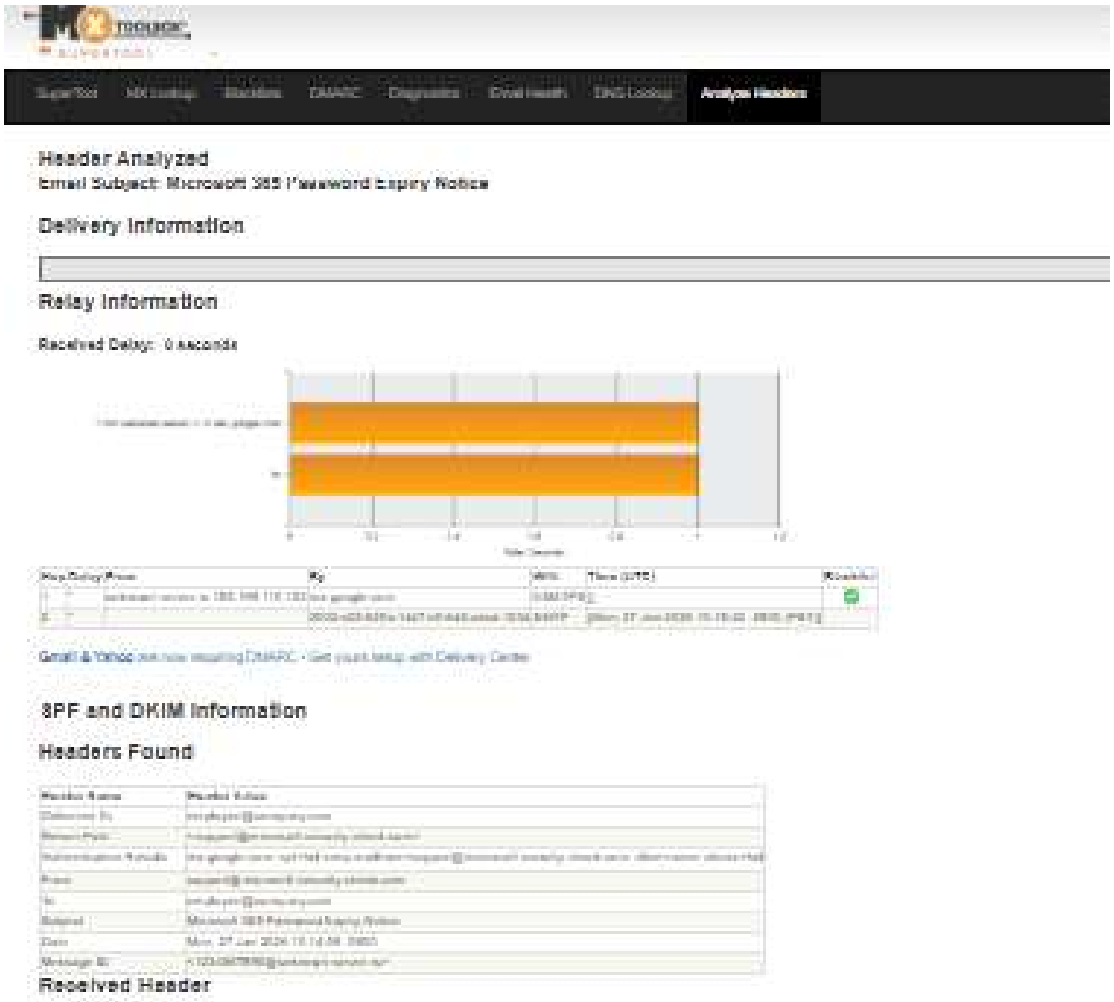

Figure: MXToolbox Header Analyzer confirming authentication and relay information.

5. Common Phishing Indicators Observed

- Generic greetings
- Urgent or threatening language
- Spoofed domains
- Authentication failures (SPF/DKIM/DMARC)
- Requests for sensitive information

6. Prevention & Awareness Guidelines

Do:

- Verify sender addresses
- Hover over links before clicking
- Report suspicious emails
- Enable MFA

Don't:

- Click unknown links
- Share passwords or OTPs
- Download unexpected attachments

7. Evidence

All supporting evidence is embedded directly within this report under each finding.

8. Conclusion

The analyzed emails demonstrate common real-world phishing techniques. Continuous awareness training and verification practices are essential to reduce risk.