Phishing Email Detection & Awareness Report

Cyber Security Internship – Future Interns (2026)

Executive Summary

This report analyzes suspicious email samples to detect phishing attacks and provide employee awareness guidance. Multiple spoofing and authentication failures were observed. All emails were classified as phishing.

Methodology

- Collect phishing samples
- Analyze headers using MXToolbox and Google
- Inspect domains and links safely
- Identify indicators
- Classify risk
- Document findings

Tools Used

- MXToolbox Header Analyzer
- Google Message Header Analyzer
- Browser inspection tools

Findings

- Generic greetings
- Urgent or fear-based language
- Suspicious domains
- SPF fail, DKIM none, DMARC fail
- Unknown sending server

Risk Classification: HIGH – PHISHING

Prevention Guidelines

- Verify sender address
- Hover over links before clicking
- Report suspicious emails
- Enable MFA
- Never share credentials

Conclusion

Phishing attempts rely on social engineering. Continuous awareness reduces risk. Evidence files are stored in the GitHub repository.