Phishing Email Detection & Awareness Report

Cyber Security Task 2 (2026) – By Future Interns

1. Executive Summary

Phishing attacks continue to be one of the most widespread and damaging cyber threats faced by modern organizations. Unlike technical attacks that exploit system vulnerabilities, phishing attacks exploit human behavior, trust, and lack of awareness. This report provides a detailed analysis of a phishing email using email header examination and content-based indicators. The objective is to demonstrate how phishing emails can be detected at an early stage and how awareness can significantly reduce organizational risk.

2. Purpose of the Report

The purpose of this report is to simulate the role of a security analyst tasked with identifying phishing emails within an organization. It aims to explain phishing detection techniques in a simple and understandable manner so that even non-technical users can benefit. The report also serves as an awareness document that organizations can use as part of internal security training programs.

3. Scope and Ethical Considerations

This analysis is strictly limited to read-only inspection of a phishing email sample. No malicious links were clicked, no payloads were executed, and no systems were accessed without authorization. All data used in this report is either publicly available or created for educational purposes. This task fully complies with ethical cybersecurity practices.

4. Tools and Methodology

The analysis was performed using standard email security investigation tools commonly used by security teams. Google Message Header Analyzer and MXToolbox were used to examine the email headers and authentication results. A structured methodology was followed, starting with header analysis, followed by sender verification, content inspection, and risk classification.

5. Phishing Email Header Overview

The analyzed phishing email header revealed multiple anomalies that are commonly associated with phishing attacks. These include mismatched sender information, failed authentication checks, and suspicious routing paths. Header analysis is a critical step because it provides technical evidence that cannot be easily manipulated by attackers.

6. Detailed Header Analysis Findings

The sender domain observed in the email does not belong to any trusted organization and uses misleading security-related keywords. The sending IP address was not authorized to send emails on behalf of the claimed domain, resulting in an SPF softfail. Additionally, the absence of DKIM signatures and the failure of DMARC alignment strongly indicate that the email was spoofed.

7. Social Engineering Indicators

Beyond technical indicators, the email content itself displayed classic social engineering techniques. The subject line created a sense of urgency and fear by threatening account suspension. The greeting was generic and lacked personalization, and the message pressured the user to take immediate action, which is

a common phishing tactic.

8. Risk Classification

Based on both technical header analysis and content-based indicators, the email was classified as a phishing email. The risk level was assessed as high due to the potential for credential theft and account compromise. If acted upon, this email could lead to serious security incidents within an organization.

9. Phishing Attack Flow Explanation

The phishing attack begins with the delivery of a deceptive email designed to appear legitimate. The user is then directed to a fraudulent website that mimics a real service. Once credentials are entered, attackers gain unauthorized access, which may be used for data theft, financial fraud, or lateral movement.

10. Potential Impact on Organizations

Successful phishing attacks can have severe consequences for organizations. These include unauthorized access to internal systems, leakage of sensitive data, financial losses, and reputational damage. In many cases, a single compromised account can be enough to initiate a larger security breach.

11. Prevention and Awareness Guidelines

Employees play a crucial role in preventing phishing attacks. They should be trained to verify sender details, avoid clicking unknown links, and report suspicious emails immediately. Organizations should complement user awareness with technical controls such as email authentication and regular phishing simulations.

12. Conclusion

This report highlights that phishing attacks can be effectively identified using a combination of technical analysis and user awareness. While attackers continue to evolve their techniques, educated users and proactive security practices remain the strongest defense against phishing threats.

13. Disclaimer

This document has been created solely for educational purposes as part of Cyber Security Task 2 (2026) by Future Interns. No real organizations or individuals were targeted during this analysis.