FUTURE INTERNS

CYBER SECURITY

TASK - 2 (2026)

Phishing Email Detection & Awareness System

PREPARED BY :

MUCHARLA SRI HARSHITHA

INTRODUCTION

Phishing is a type of online scam where criminals pretend to be a trusted company, bank, or even your workplace to trick you into sharing sensitive information like passwords, credit card numbers, or one-time passcodes. They usually send emails or messages that create fear or urgency, such as saying your account will be locked unless you act immediately. These messages often include fake links that look real but lead to fraudulent websites designed to steal your information. Phishing is dangerous because once attackers get access to your details, they can steal money, access company systems, or misuse your personal identity.

This report analyzes multiple phishing email samples using header analysis and domain investigation tools. Several high-risk indicators were identified including spoofed domains, urgency-based language, and credential harvesting attempts. The analyzed emails were classified as high-risk phishing attempts.

OBJECTIVE OF THE ANALYSIS

- To understand what phishing emails look like in real-world scenarios
- To identify common phishing indicators (suspicious links, urgency, fake domains, etc.)
- To analyze email headers for sender authenticity and technical anomalies
- To inspect domains and URLs for legitimacy and registration details
- To classify emails based on risk level (Safe / Suspicious / Phishing)
- To explain the attack methods in simple, non-technical language
- To create awareness guidelines that help users recognize and avoid phishing attacks
- To recommend preventive measures for organizations to reduce phishing risks

TOOLS USED

Google Message Header Analyzer (https://toolbox.googleapps.com/apps/messageheader/) – Used to analyze email headers to verify the actual sender and check authentication results such as SPF, DKIM, and DMARC.

MXToolbox Email Header Analyzer (https://mxtoolbox.com/EmailHeaders.aspx) – Used to examine email routing details, identify sender IP address, and detect possible spoofing or header anomalies.

E-MAIL ANALYSIS

SAMPLE #1: New fax message

Header Field	**Observation**	**Risk**
From	Fake/meaningless sender name + malicious domain	High
Return-Path	attack@attacker.example.com	High
To	"Undisclosed recipients" (mass phishing)	Medium
Message-ID	Microsoft Outlook server used but domain isn't Microsoft	High
SPF/DKIM/DMARC	Expected to fail due to domain mismatch	High
Content-Type	Multipart HTML (can hide malicious links)	Medium

1. **Spoofed Sender**

The "From" field contains repeated nonsense text followed by a malicious domain → clear spoofing attempt.

2. **Mismatch Between Domain and Mail Server**

The attacker used an Outlook mail server but claimed to be from attacker.example.com → violates SPF, DKIM, and DMARC.

3. **Mass Emailing Pattern**

Use of “Undisclosed recipients” indicates bulk targeting.

4. **Suspicious Formatting**

Random repeated words like *WirelessReceivedWirelessReceived* suggest automated/bot generation.

5. **Malicious Domain in Return-Path**

Return-path domain is not legitimate, confirming origin is untrusted.

SAMPLE #2: Voice message

Indicator	Evidence	Risk
SPF Fail	Domain does not authorize sending IP	High
DKIM None	No signature → spoofed sender	High
DMARC Fail	Domain has reject policy	High
Subdomain spoofing	target.example.com	High
Suspicious Subject	“Voice Message – Pass-Key-Exception”	Medium
MIME Multipart	Likely malicious attachment	Medium
Mismatch in infrastructure	Outlook protection showing fail	High

- Attacker spoofs the sender using **subdomain impersonation**.

- Sends email from unauthorized IP (192.0.2.1).

- SPF, DKIM, DMARC all fail → confirms spoofing.

- Subject line attempts to create urgency using **“pass-key exception”**.

- Attachment likely contains malware or phishing link.

- Target user thinks voicemail is real and clicks → compromise.

Common Phishing Patterns Identified

1. **Sender Spoofing** – Fake or impersonated email addresses to look legitimate.
2. **Authentication Failures** – SPF, DKIM, and DMARC often fail, indicating spoofing.
3. **Urgency & Fear Tactics** – "Account locked", "Immediate action required", etc.
4. **Suspicious Links** – Unknown domains, HTTP links, or misleading "Verify Now" buttons.
5. **Unexpected Attachments** – HTML, ZIP, PDF attachments carrying malware.
6. **Generic Greetings** – "Dear User", "Dear Customer" instead of real names.
7. **Mass Targeting** – "Undisclosed recipients" or bulk-sent emails.
8. **Poor Formatting** – Grammar mistakes, repeated words, unusual layout.