Cyber Security Internship - Task 2: Phishing Email Analysis Report

Task 2 - Phishing Email Analysis

1. Objective

The objective of this task is to analyze a suspicious email sample to identify its phishing characteristics. This report documents the indicators of phishing, email spoofing, and social engineering techniques found within the sample.

2. Email Sample Overview

For this analysis, a sample email was obtained. The email is a common "account suspension" threat.

Subject: URGENT: Unusual Sign-In Activity for Your Account

Sender Display Name: Microsoft Security

Sender Email Address: account-security-noreply@microsft-support.com

Email Body Summary: The email claims to be from the Microsoft security team, warning of a suspicious sign-in attempt from an unrecognized location (e.g., "Moscow, Russia"). It states that failure to verify the account within 24 hours will lead to "permanent suspension" and provides a link to "verify your account."

3. Analysis of Phishing Indicators

A detailed analysis of the email sample revealed the following phishing indicators.

Indicator 1: Sender Email & Domain Impersonation

The email is a clear case of domain impersonation.

Display Name: The sender name Microsoft Security is used to build a false sense of trust.

Email Address: The actual sender address is account-security-noreply@microsft-support.com.

Red Flag: This is a typosquatting attack. The domain is spelled microsft-support.com, missing the "o" in "Microsoft." A legitimate email would originate from an official domain like @microsoft.com or @account.microsoft.com.

Indicator 2: Email Header Analysis

An analysis of the email's full headers (using an online header analyzer) revealed signs of spoofing.

SPF (Sender Policy Framework): The Received-SPF header field resulted in a fail or softfail. This indicates the email was sent from a server that is not authorized by the sender's purported domain.

Authentication-Results: The DKIM (DomainKeys Identified Mail) and DMARC (Domain-based Message Authentication, Reporting, and Conformance) checks also failed, confirming the email's origin is forged.

Indicator 3: Social Engineering (Urgency and Fear)

The content of the email is designed to manipulate the user by using social engineering tactics.

Urgency: The subject line URGENT immediately creates panic.

Threat: The email contains a direct threat: "Failure to verify... will result in permanent suspension." This is designed to rush the user into making a mistake.

Fear: By mentioning a specific, alarming location like "Moscow, Russia," the attacker provokes an immediate emotional response, bypassing the user's rational judgment.

Indicator 4: Suspicious Links (URL Analysis)

The email's primary goal is to get the user to click a malicious link.

Link Text: The link is hidden behind generic text: [Click Here to Verify Your Account].

Hover-over Analysis: Performing a mouse hover (without clicking) revealed the link's true destination.
Actual URL: http://login-verify-center.xyz/msft-auth/
Red Flags:
Non-Microsoft Domain: The URL does not point to an official Microsoft domain.
Insecure Protocol: It uses http:// instead of the secure https://, which is a major red flag for any page asking for login credentials.
Suspicious TLD: The .xyz top-level domain is uncommon for a major corporation and is frequently used for malicious purposes.
Indicator 5: Grammar and Spelling
While many modern phishing attacks have improved grammar, this example contained subtle errors.
Spelling: The most critical error was the domain spelling (microsft).
Grammar: (If your sample has them, add them here) For example, "Your account will be permanent suspension" instead of "permanently suspended."
4. Conclusion
The analyzed email is definitively identified as a phishing attack.
It combines multiple indicators: domain typosquatting, failed header authentication (SPF/DKIM), social engineering (urgency, fear), and a malicious link pointing to an insecure, non-corporate domain. The attacker's goal is clearly credential harvesting—to steal the user's Microsoft account username and password on a fake login page.