Task 2: Phishing Email Analysis Report

Intern Name: Soumen Das

November 14, 2025

1 Introduction: Sample Email Overview

This report provides an analysis of a sample phishing email, fulfilling the requirements of Task 2. The objective is to identify and document characteristics of a suspicious email.

- **Sample Subject:** Urgent: Your Account is Scheduled for Deletion
- **Apparent Sender:** Billing Support $< support@microsft - billing.com >$
- **Body Summary:** The email claims that ”unusual activity” was detected on the user’s account. It states that as a security measure, the account is ”scheduled for deletion” within 24 hours unless ”immediate action” is taken by clicking a verification link.

2 Analysis of Phishing Indicators

The email was analyzed for common phishing traits, following the steps outlined in the task guide. The following indicators were found:

2.1 1. Sender’s Email Address (Spoofing)

The sender’s domain is `@microsft-billing.com`. This is a clear example of ”typosquatting.”

- **Red Flag:** The legitimate company is ”Microsoft,” not ”Microsft.”
- **Red Flag:** The domain is designed to look legitimate at a quick glance, but the misspelling confirms it is not from an official source.

2.2 2. Email Header Analysis

A check of the email’s raw headers (using an online analyzer) revealed critical discrepancies.

Table 1: Key Header Analysis Findings

Header Field	Value (Sample)	Analysis / Red Flag
`From`	$< support@microsft - billing.com >$	Domain is misspelled (typosquatting)
`Reply-To`	$< scammer.x12@gmail.com >$	The reply address is a generic Gmail a
`Received: from`	mail.suspicious-server.ru (185.12.33.1)	The originating server is not a Micros
`Authentication-Results`	SPF=fail, DKIM=none, DMARC=fail	The email failed all standard sender a

2.3 3. Suspicious Links and Mismatched URLs

The email body contained a prominent "Click Here to Verify Your Account" button.

- **Displayed Link Text:** The button text implies it leads to a secure Microsoft site.
- **Actual Link (on hover):** Hovering the mouse over the link revealed the true destination: `http://secure-login-portal.xyz/msft-verify.php`.
- **Analysis:** The actual URL is not on a `microsoft.com` domain, uses `http` (insecure) instead of `https`, and points to a suspicious `.xyz` domain. This is a classic "mismatched URL" tactic.

2.4 4. Urgent or Threatening Language

The email uses high-pressure language to bypass a user's critical thinking.

- "Urgent"
- "Immediate action required"
- "Scheduled for deletion within 24 hours"

This language creates a false sense of panic, which is a hallmark of phishing attacks.

2.5 5. Spelling and Grammar Errors

Besides the "Microsft" typo in the sender's address, the body contained a subtle but critical error: "Failure to comply will result in your account be permanently delete."

- **Red Flag:** The incorrect grammar ("be... delete" instead of "being... deleted") is unprofessional and not typical of a legitimate corporation's automated emails.

3 Summary of Phishing Traits

This email is definitively a phishing attack. It successfully demonstrates multiple classic phishing traits:

1. **Deceptive Sender:** Typosquatted domain.
2. **Forged Headers:** Failed SPF/DKIM checks and a suspicious "Reply-To" address.
3. **Malicious Link:** The displayed link is masked, and the actual destination is a non-Microsoft, insecure site.
4. **Psychological Manipulation:** Use of urgent and threatening language.
5. **Poor Quality:** Obvious spelling and grammar errors.

4 Outcome

This analysis successfully identified key phishing indicators, demonstrating an awareness of common phishing tactics and the ability to perform basic email threat analysis. This fulfills the objective of Task 2.