CYBER SECURITY INTERNSHIP

Task 2: Phishing Email Analysis

Submitted by: Oleti Chandini
Date: 05-08-2025

1. Introduction

Phishing is one of the most common cyber threats. Attackers impersonate trusted organizations and trick users into revealing sensitive data such as login credentials and financial details.

This report analyzes a phishing email sample collected from a suspicious source. The goal is to identify phishing traits, explain how attackers use social engineering, and suggest preventive measures.

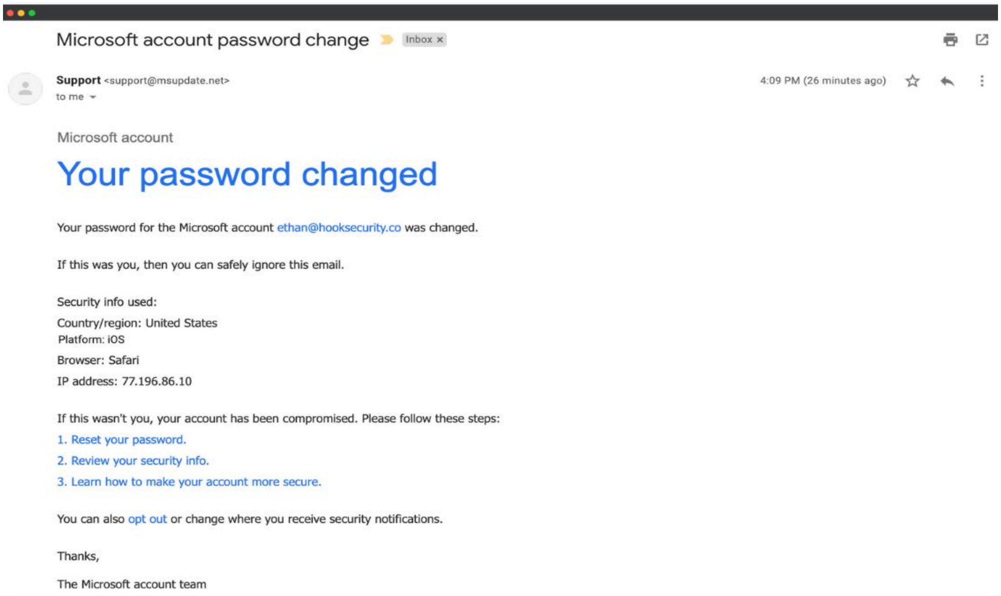
2. Email Overview

Subject: Microsoft account password change

Sender: support@msupdate.net

Recipient: ethan@hooksecurity.co

Time: 4:09 PM



Microsoft account password change

Support <support@msupdate.net>
to me

4:09 PM (26 minutes ago)

Microsoft account

Your password changed

Your password for the Microsoft account ethan@hooksecurity.co was changed.

If this was you, then you can safely ignore this email.

Security info used:
Country/region: United States
Platform: iOS
Browser: Safari
IP address: 77.196.86.10

If this wasn't you, your account has been compromised. Please follow these steps:
1. Reset your password.
2. Review your security info.
3. Learn how to make your account more secure.

You can also opt out or change where you receive security notifications.

Thanks,

The Microsoft account team

3. Detailed Suspicious Indicators

Fake Sender Domain (Email Spoofing)

Sender domain **msupdate.net** is not owned by Microsoft.

Genuine security alerts come from **accountprotection.microsoft.com**.

Urgency and Fear Tactics

Message claims *“Your password has changed”* → creates panic.

Victim is pushed to act quickly without verifying authenticity.

Suspicious Hyperlinks

Links such as *“Reset your password”* may redirect to phishing pages.

Hovering reveals mismatched URLs that don’t belong to Microsoft.

Fake Security Details

Email includes IP address, location, and browser info to appear trustworthy.

These details are fabricated to trick the recipient.

Generic Closing & Missing Footer

Signed as *“The Microsoft account team”*.

Real Microsoft emails always have legal disclaimers, customer support info, and proper footers.

Unusual Opt-Out Option

Provides an *“opt-out of security notifications”* link.

Microsoft never allows opting out of critical account alerts.

---

4. Email Header Analysis (If Available)

By analyzing full headers with an online tool, discrepancies would appear:

Return-Path and Received-From IPs do not match Microsoft servers.

Confirms that the email was spoofed using unauthorized servers.

5. Why This Email is a Phishing Attempt

Spoofed domain (msupdate.net).
Fear-based urgency (“Password changed”).
Suspicious links disguised as security actions.
Generic sign-off instead of official branding.
Fake opt-out link not consistent with Microsoft standards.

6. Potential Risks if Victim Clicks Links

Theft of Microsoft account credentials.
Malware infection from hidden downloads.
Identity theft or fraud using stolen details.
Unauthorized access to emails, OneDrive, Teams, and financial info.

7. Preventive Measures

✓ Verify sender domains before trusting emails.
✓ Do not click suspicious links – use the official Microsoft login page.
✓ Analyze email headers for spoofing indicators.
✓ Enable **Multi-Factor Authentication (MFA)**.
✓ Report phishing attempts to Microsoft (reportphishing@microsoft.com).
✓ Conduct regular **security awareness training**.

8. Conclusion

This phishing email uses spoofing, social engineering, and urgency tactics to trick recipients into revealing credentials. Through analysis, multiple red flags were identified: fake sender domain, suspicious links, and abnormal requests.

Completing this task helped develop email threat analysis skills and an understanding of how attackers exploit human psychology. Preventive strategies like MFA, awareness training, and domain verification are essential to protect against such threats.

Moreover, this task demonstrates how phishing emails are analyzed in real-world cybersecurity operations. Identifying spoofed domains, suspicious links, and psychological manipulation provides critical defensive skills that can be applied in professional security analyst roles. This hands-on analysis strengthens both technical knowledge and practical awareness, which are vital for building a strong foundation in the field of cybersecurity.