CYBER SECURITY INTERNSHIP

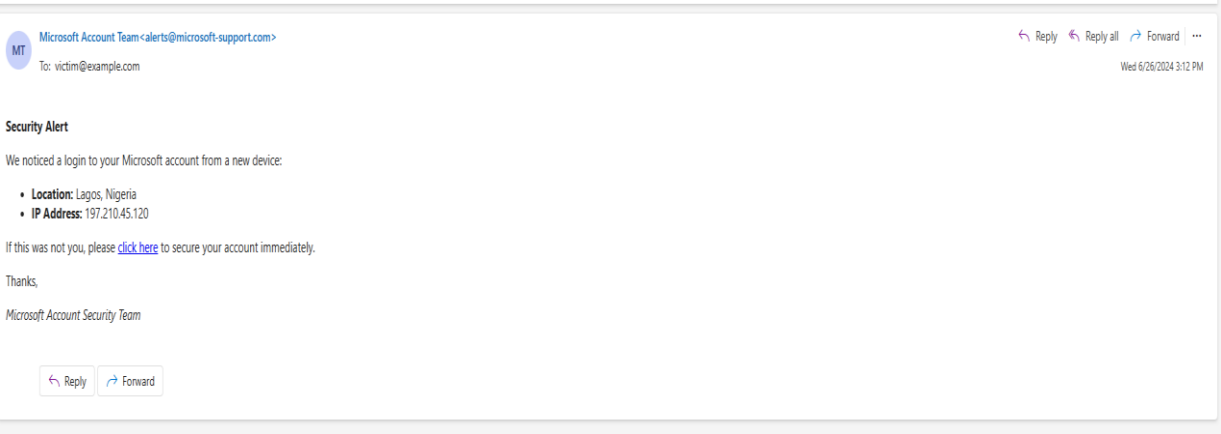
Task 2: Analyze a Phishing Email Sample.

Objective: Identify phishing characteristics in a suspicious email sample.

Tools: Email client or saved email file (text), free online header analyzer.

Deliverables: A report listing phishing indicators found

1.sample phishing email:



2.Examine sender's email address for spoofing:

a. Sender Address Information

- From Header: "Microsoft Account Team" <alerts@microsoft-support.com>
- Reply-To Header: support@microsoft-support.com
- Return-Path: <alerts@microsoft-support.com>

b. Observations and Indicators of Spoofing

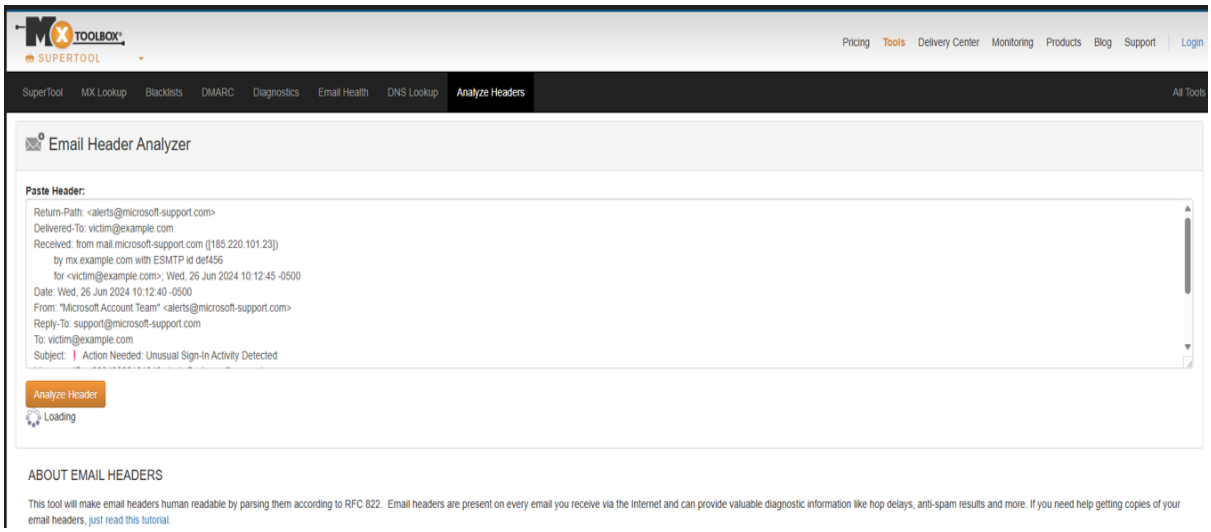
Domain Legitimacy Check

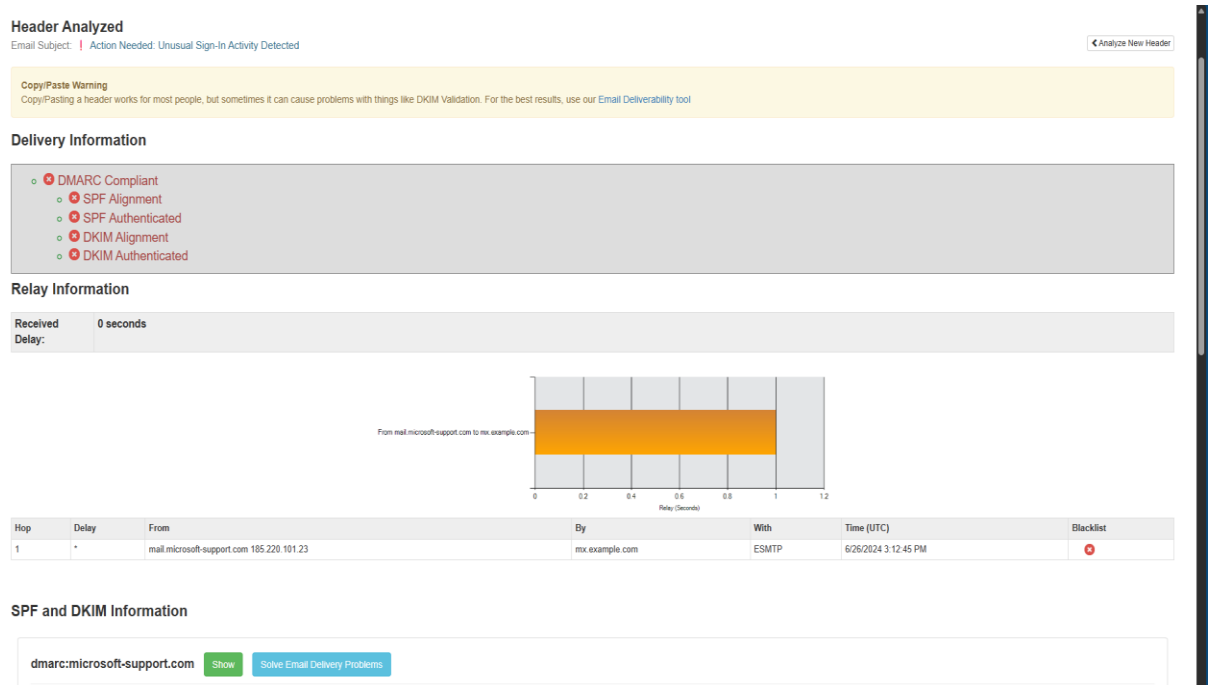
- Claimed Domain: microsoft-support.com
- Issue: This is not an official Microsoft domain. Microsoft uses domains like microsoft.com, account.microsoft.com, or subdomains thereof.
- Verdict: Suspicious/Impersonated domain

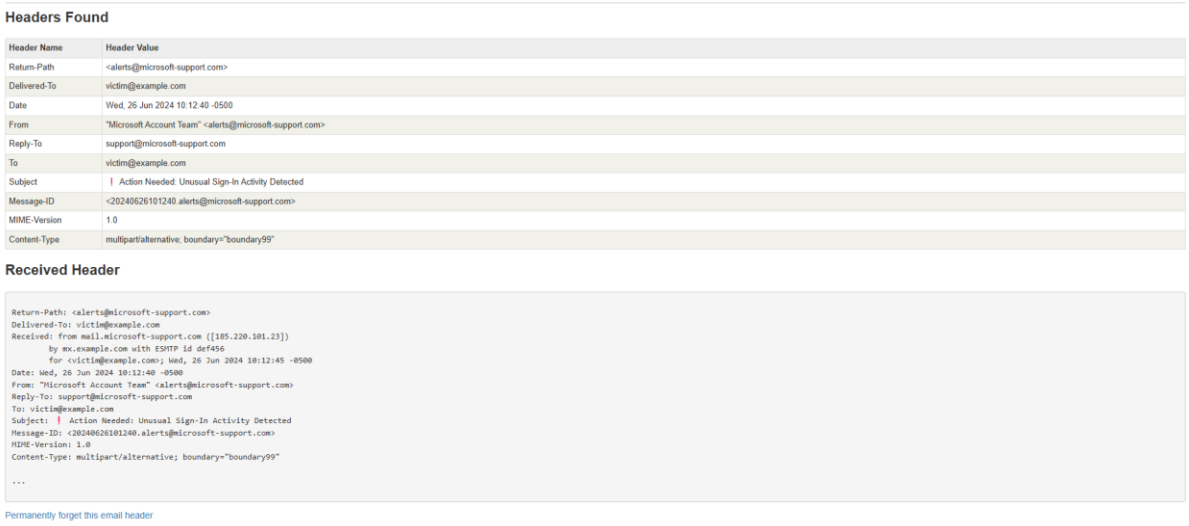
c. Return Path and Mail Server IP

- Return-Path Domain: microsoft-support.com
- Sending Mail Server IP: 185.220.101.23
- IP Check: This IP is associated with Tor exit nodes and has been flagged in blocklists—not typical for corporate emails.
- Verdict: Likely spoofed or anonymized

3.email headers for discrepancies (using online header analyzer)







Headers Found

Header Name	Header Value
Return-Path	<alerts@microsoft-support.com>
Delivered-To	victim@example.com
Date	Wed, 26 Jun 2024 10:12:40 -0500
From	"Microsoft Account Team" <alerts@microsoft-support.com>
Reply-To	support@microsoft-support.com
To	victim@example.com
Subject	❗ Action Needed: Unusual Sign-In Activity Detected
Message-ID	<20240626101240.alerts@microsoft-support.com>
MIME-Version	1.0
Content-Type	multipart/alternative; boundary="boundary99"

Received Header

```
Return-Path: <alerts@microsoft-support.com>
Delivered-To: victim@example.com
Received: from mail.microsoft-support.com ([185.220.101.23])
        by mx.example.com with ESMTP id def456
        for <victim@example.com>; Wed, 26 Jun 2024 10:12:45 -0500
Date: Wed, 26 Jun 2024 10:12:40 -0500
From: "Microsoft Account Team" <alerts@microsoft-support.com>
Reply-To: support@microsoft-support.com
To: victim@example.com
Subject: ❗ Action Needed: Unusual Sign-In Activity Detected
Message-ID: <20240626101240.alerts@microsoft-support.com>
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="boundary99"

...
```

Permanently forget this email header

4.Suspicious Link Analysis Report:

Email Source

- Sender Name: Microsoft Account Team
- Sender Email: alerts@microsoft-support.com
- Subject: Action Needed: Unusual Sign-In Activity Detected
- Date: Wed, 26 Jun 2024
- Suspicious Link Identified

http://microsoft-login-alert.com/review?id=987654

5. Urgent or Threatening Language Analysis Report

Email Summary

- From: Microsoft Account Team <alerts@microsoft-support.com>
- To: victim@example.com
- Subject: Action Needed: Unusual Sign-In Activity Detected
- Date: Wed, 26 Jun 2024

Identified Urgent or Threatening Phrases

Phrase	Explanation
Action Needed	Uses an attention-grabbing symbol and command to provoke urgency.
Unusual Sign-In Activity Detected	Implies a potential security breach; raises alarm.
If this wasn't you, please secure your account immediately	Pressures recipient to act without thinking critically.
Click here to secure your account immediately	Strong directive, common in phishing to rush a user to a fake login page.

Psychological Tactics Used

- Fear-based urgency: Suggests account compromise to cause panic.
- Authority impersonation: Mimics Microsoft to build trust.
- Immediate call to action: Encourages impulsive behaviour

Conclusion

The email clearly uses urgent and threatening language to manipulate the recipient into clicking a malicious link. This is a hallmark of phishing and should be treated as malicious.

6. mismatched URLs (hover to see real link):

Mismatched URL Analysis Report

Email Context

- Displayed Link Text (HTML version):

"...please click here to secure your account immediately."

Mismatched Link Details

Displayed Link Text	Actual URL (hover or inspect)	Analysis
click here	http://microsoft-login-alert.com/review?id=987654	The visible text does not show the destination. This hides a non-Microsoft domain behind a neutral phrase.

Red Flag Indicators

- Deceptive Text: The link says “click here”, but the actual URL goes to an impersonation domain.
- Misleading Domain: The domain microsoft-login-alert.com is not owned by Microsoft and is clearly crafted to appear legitimate.
- No HTTPS: The link uses http — a further security risk.
- Anchor/Text Mismatch: A legitimate email would display either the actual Microsoft domain or a recognizable shortened link.

7.Actions to Take on Suspected Phishing Emails

a. Do Not Interact

- **Don’t click** on links or download attachments.
- **Do not reply** to the sender.

b. Report the Email

- **To your organization:**
  - Use the **“Report Phishing” button** in Outlook (if available).
  - Or forward the email to your IT/Security team (e.g., phishing@yourcompany.com).
- **To external services:**
  - Microsoft: reportphishing@microsoft.com
  - Google: report phishing page
  - Anti-Phishing Working Group (APWG): reportphishing@apwg.org

c. Quarantine or Delete

- Move the email to **Junk/Spam**, or
- Use your email client's **“Report” or “Block”** feature to help train filters.

d. Alert Others (If Needed)

- If it's part of a **targeted attack** (e.g., CEO fraud, credential theft), alert colleagues and leadership.

e. Run Security Checks

- If you clicked a link:

    - Immediately **change your password**.
    - Enable **2FA** (two-factor authentication).
    - **Run antivirus/antimalware** scans.
- Monitor for suspicious activity (account logins, unauthorized transactions).

8.How Social Engineering Is Used in Phishing

a. Impersonation of Trusted Entities

- Attackers pose as:
    - Microsoft, Google, banks, HR departments, or company executives.
- Goal: Create **instant credibility** to lower skepticism.

b. Creating a Sense of Urgency or Fear

- Phrases like:
    - *"Unusual sign-in detected."*
    - *"Your account will be locked."*
    - *"You missed a payroll deposit."*
- Goal: **Pressure victims into acting without thinking**.

c. Authority and Familiarity Triggers

- Pretend to be:
    - A manager, CEO, or IT admin.
    - A familiar brand or internal system.
- Goal: Victims obey **without verifying** due to perceived authority.

d. Exploiting Curiosity or Reward

- Subjects like:
    - *"You've won a prize!"*
    - *"Invoice attached"*
- Goal: Trick users into opening attachments or clicking links.

e. Fake Login Pages

- Email links lead to:

    - **Lookalike login pages** that mimic legitimate services.
- Goal: Steal **credentials** or **2FA codes**.

f. Emotional Manipulation

- Use of fear, trust, urgency, or greed.
- Goal: **Bypass logical thinking** and exploit emotional reflexes.