1. Sample Phishing Email

From: `security-update@microsift-support.com`
To: [Recipient's Email Address]
Subject: Immediate Action Required: Unusual Login Activity Detected in Your Account

Dear User,

We have detetced **unusual login attempts** on your Microsoft account from an **unknow device** in a different location.

Location: Kolkata,India
Device: Windows 10 PC
Time: 3:24 AM IST

To **protect your account**, we have temporarily **locked your access**. You must **verify your identity** within 12 hours, or your account will be permanently suspended.

Click here to verify now: http://www.micro-sift-security-verification.com/verify

If you don't take action, you could lose access to your emails, contacts, and files.

Thank you for your immediate attention.
– Microsoft Security Team

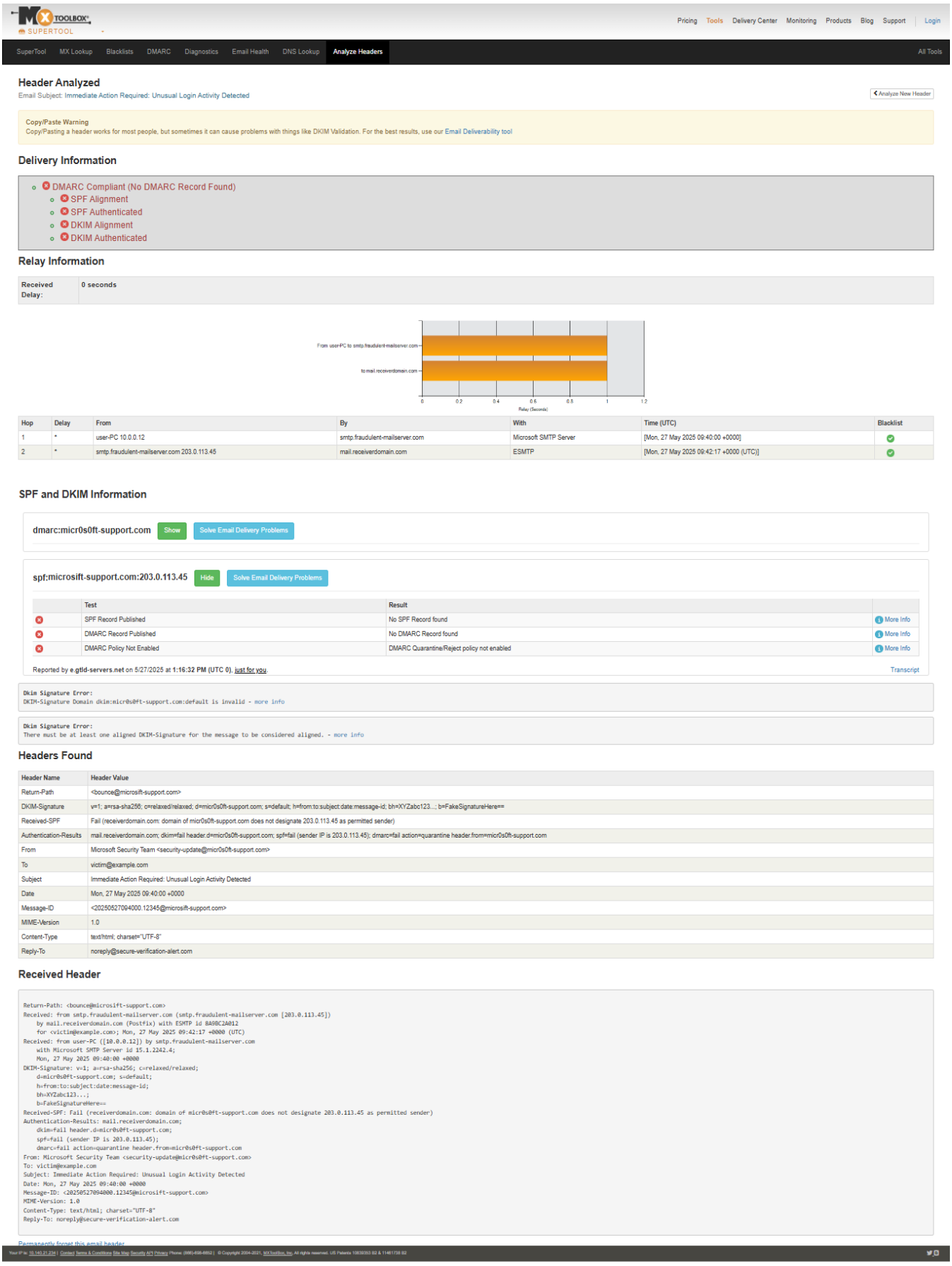
Attachment: `Account_Verification_Form.htm`

2. Examine sender's email address for spoofing.

`security-update@microsift-support.com`

- By examining the email address it is observed that there is a grammatical error is seen suggesting that it is not a recognized Microsoft and from some shady organization.
- Microsoft never provides security updates or blocks account for account verification purposes, here, pressure is being created over the receiver to act upon the email by the mention of 12 hour time limit.

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



- In this snapshot, it clearly observed that it failed all basic tests such as SPF record, DMARC record & DMARC Policy. It also fails Dkim signatures as no signatures are attached

- SPF record (Sender Record Policy) – It is a type of DNS record that tells recieveing email servers which servers are authorized to send emails on behalf of a specific domain.

- DMARC Record (Domain-based Message Authentication, Reporting, and Conformance) – It is a TXT record within a domain's DNS that defines a policy for how receiving email servers should handle emails that claim to originate from that domain but fail SPF or DKIM authentication

- DMARC Policy (Domain-based Message Authentication, Reporting, and Conformance) - It is a part of the record that defines the actions to be taken with unauthenticated emails, such as rejecting, quarantining, or delivering them.

4. Identify suspicious links or attachments.

http://www.micro-sift-security-verification.com/verify

While observing the link carefully, few points are observed mentioned as follows

1. At the start of the link, the link works on ‘http’ rather than ‘https’, implying that the site does not use any encryption making the link unsafe for use & leaving the user data exposed and user data to be hacked

2. The organization the link is trying to impersonate tries to be Microsoft but there appears to be a spelling error, which in first look might seem like Microsoft, but the user would be redirected to fake Microsoft leading credential theft, user information leak, etc.

3. A simple search to WHOIS would also refer to the observation that the link is a counterfeit one and not registered to Microsoft

5. Look for urgent or threatening language in the email body.

“You must **verify your identity** within 12 hours, or your account will be permanently suspended.

If you don’t take action, you could lose access to your emails, contacts, and files.”

- Observing the language of the, it is observed that the language is threatening and create a subtle pressure on the receiver of taking an action and click on the link as early as possible and making the receiver vulnerable.

6. Note any mismatched URLs (hover to see real link).

- The email contains a mismatched link, which is a common phishing tactic. While the visible text may appear legitimate, such as "Click here to verify now," hovering over the link reveals the actual URL: http://www.micro-sift-security-verification.com/verify, which does not belong to Microsoft's official domain. Legitimate companies use secure, branded URLs (e.g., https://account.microsoft.com). This mismatch is a clear red flag indicating the link may lead to a fraudulent site designed to steal personal information.

7. Verify presence of spelling or grammar errors.

“We have detetced **unusual login attempts** on your Microsoft account from an **unknow device** in a different location.

To **protect your account**, we have temporarily **locked your access**. You must **verify your identity** within 12 hours, or your account will be permanently suspended.

Click here to verify now: http://www.micro-sift-security-verification.com/verify
If you don’t take action, you could lose access to your emails, contacts, and files.”

- The email contains clear indicators of phishing, including spelling errors such as “detetced” instead of “detected” and “unknow device” instead of “unknown device.” The language is unprofessional and overly urgent, with phrases like “your account will be permanently suspended” and “you could lose access to your emails,” which are designed to create panic. Legitimate companies like Microsoft use calm, clear, and respectful language, avoid threats, and personalize their communication. The lack of a personalized greeting and the presence of a suspicious link further support that this is not a formal or trustworthy email.

8. Summarize phishing traits found in the email.

Summary of Phishing Traits Observed

1. Spelling and Grammar Errors
    - Misspellings like “detetced” and “unknow” reduce credibility and signal lack of authenticity
2. Urgent and Threatening Language
    - Phrases such as “verify within 12 hours” and “permanently suspended” are used to create fear and prompt rash action.
3. Suspicious and Mismatched URL
    - The visible link text suggests legitimacy, but the actual URL (`micro-sift-security-verification.com`) is a deceptive lookalike.
4. Unsecured Link (HTTP instead of HTTPS)
    - The use of `http://` instead of secure `https://` shows the site is not protected, which is uncommon for real services.
5. Lack of Personalization
    - No use of the recipient’s name or account details, indicating a generic mass message.
6. Spoofed Sender Address
    - The email appears to come from Microsoft but uses a fake domain (`micr0s0ft-support.com`), often revealed through header analysis.
7. Failed Email Authentication Checks
    - Header analysis would likely show SPF, DKIM, and DMARC failures, confirming the sender is not authorized.