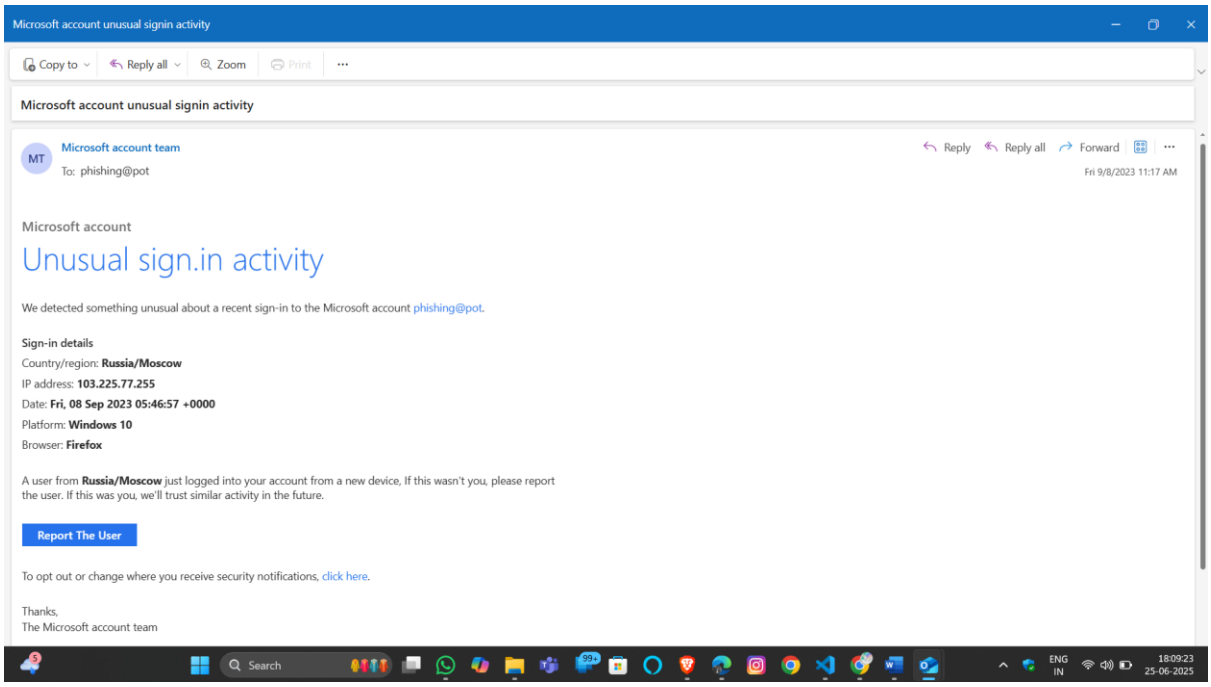
CYBER SECURITY INTERNSHIP

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.

1.sample phishing email.



2.Examing sender's email address for spoofing

analysis of the email, especially focusing on possible spoofing and phishing indicators:

Red Flags Suggesting This May Be a Phishing or Spoofed Email:

Suspicious Sender Email:

- The sender is shown as Microsoft account team, but the email address is phishing@pot.
- This is not a legitimate Microsoft domain. Microsoft uses domains like @microsoft.com or @accountprotection.microsoft.com.

Urgency and Prompting Action:

- The message asks you to “Report The User”, which is a common tactic in phishing emails to make the user click a malicious link.

- Legitimate security emails will usually ask you to log in securely at their official site, not press a vague button.

Link Anomalies:

- The text contains links such as “click here” or “Report The User”, which could be hiding malicious URLs.
- The actual destination of these links isn't shown in the image, but phishing emails often mask links with legitimate-sounding text.

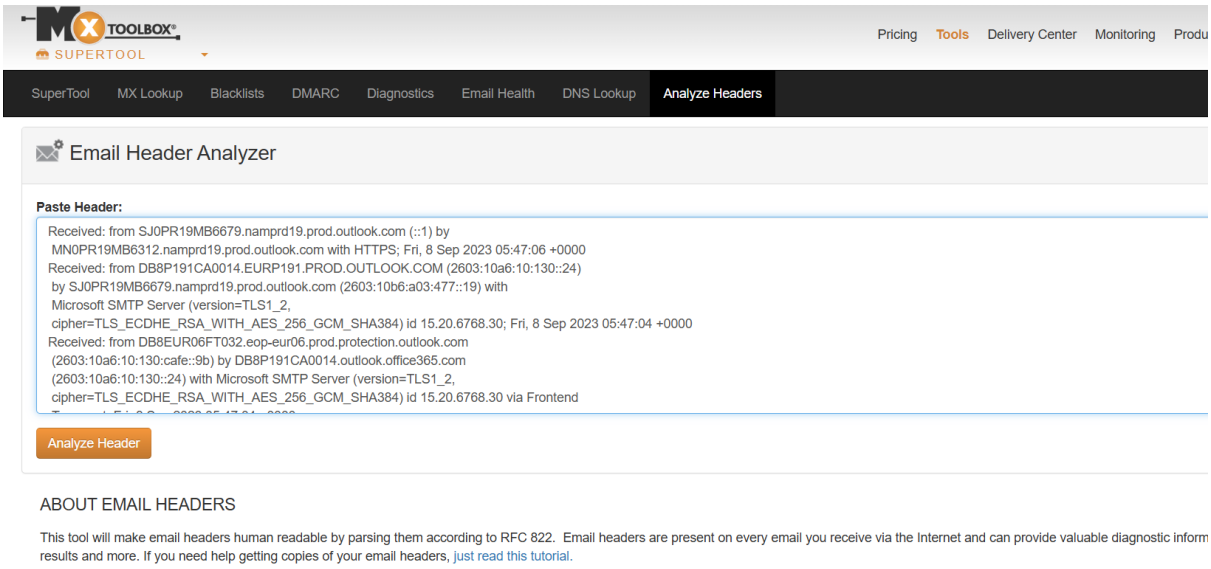
Grammatical and Format Errors:

- Use of odd punctuation in "Unusual sign.in activity".
- This is not typical of Microsoft’s polished communications.

Generic Language:

- Phrases like "A user from Russia/Moscow..." without using the actual name or email tied to the account is a common phishing tactic**.**

3.Checks the email headers for discrepancies by using online header analyzer.



Header Analyzed

Email Subject: Microsoft account unusual signin activity

Analyze New Header

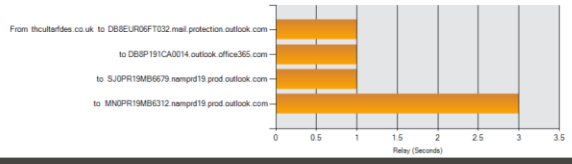
Copy/Paste Warning
Copy/Pasting a header works for most people, but sometimes it can cause problems with things like DKIM Validation. For the best results, use our Email Deliverability tool

Delivery Information

- DMARC Compliant (No DMARC Record Found)
  - SPF Alignment
  - SPF Authenticated
  - DKIM Alignment
  - DKIM Authenticated

Relay Information

Received Delay:	**2 seconds**



Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	thcultarfdes.co.uk 89.144.44.2	DB8EUR06FT032.mail.protection.outlook.com 10.233.253.34	Microsoft SMTP Server	9/8/2023 5:47:04 AM	✓
2	0 seconds	DB8EUR06FT032.eop-eur06.prod.protection.outlook.com 2603:10a6:10:130.cafe::9b	DB8P191CA0014.outlook.office365.com 2603:10a6:10:130::24	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	9/8/2023 5:47:04 AM	✓
3	0 seconds	DB8P191CA0014.EURP191.PROD.OUTLOOK.COM 2603:10a6:10:130::24	SJ0PR19MB6679.namprd19.prod.outlook.com 2603:10b6:a03:477::19	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	9/8/2023 5:47:04 AM	✓
4	2 seconds	SJ0PR19MB6679.namprd19.prod.outlook.com ::1	MN0PR19MB6312.namprd19.prod.outlook.com	HTTPS	9/8/2023 5:47:06 AM	✗

SPF and DKIM Information

dmarc:access-accsecurity.com Show Solve Email Delivery Problems

spf:thcultarfdes.co.uk:::1 Show Solve Email Delivery Problems

Dkim Signature Error:
No DKIM-Signature header found - more info

Dkim Signature Error:
There must be at least one aligned DKIM-Signature for the message to be considered aligned. - more info

Headers Found

Header Name	Header Value
Authentication-Results	spf=none (sender IP is 89.144.44.2) smtp.mailfrom=thcultarfdes.co.uk; dkim=none (message not signed) header.d=none; dmarc=permerror action=none header.from=access-accsecurity.com;
Received-SPF	None (protection.outlook.com: thcultarfdes.co.uk does not designate permitted sender hosts)
From	Microsoft account team _<no-reply@access-accsecurity.com>
Subject	Microsoft account unusual signin activity
To	phishing@pot
Reply-To	sotrecognizd@gmail.com
Date	Fri, 8 Sep 2023 05:47:04 +0000
Return-Path	bounce@thcultarfdes.co.uk
Message-ID	<032672b4-77ca-42f8-a036-9711e91bd1f3@DB8EUR06FT032.eop-eur06.prod.protection.outlook.com>
X-Sender-IP	89.144.44.2
X-Priority	1
Importance	high
MIME-Version	1.0
Content-Type	text/html; charset="UTF-8"
Content-Transfer-Encoding	8bit

Received Header

```
Received: from SJ0PR19MB6679.namprd19.prod.outlook.com (::1) by
 MN0PR19MB6312.namprd19.prod.outlook.com with HTTPS; Fri, 8 Sep 2023 05:47:06 +0000
Received: from DB8P191CA0014.EURP191.PROD.OUTLOOK.COM (2603:10a6:10:130::24)
 by SJ0PR19MB6679.namprd19.prod.outlook.com (2603:10b6:a03:477::19) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6768.30; Fri, 8 Sep 2023 05:47:04 +0000
Received: from DB8EUR06FT032.eop-eur06.prod.protection.outlook.com
 (2603:10a6:10:130:cafe::9b) by DB8P191CA0014.outlook.office365.com
 (2603:10a6:10:130::24) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6768.30 via Frontend
 Transport; Fri, 8 Sep 2023 05:47:04 +0000
Authentication-Results: spf=none (sender IP is 89.144.44.2)
 smtp.mailfrom=thcultarfdes.co.uk; dkim=none (message not signed)
 header.d=none; dmarc=permerror action=none header.from=access-accsecurity.com;
Received-SPF: None (protection.outlook.com: thcultarfdes.co.uk does not
 designate permitted sender hosts)
Received: from thcultarfdes.co.uk (89.144.44.2) by
 DB8EUR06FT032.mail.protection.outlook.com (10.233.253.34) with Microsoft SMTP
 Server id 15.20.6768.30 via Frontend Transport; Fri, 8 Sep 2023 05:47:04 +0000
From: Microsoft account team ,_<no-reply@access-accsecurity.com>
Subject: Microsoft account unusual signin activity
To: phishing@pot
Reply-To: sotrecognizd@gmail.com
Date: Fri, 8 Sep 2023 05:47:04 +0000
Return-Path: bounce@thcultarfdes.co.uk
Message-ID:
 <032672b4-77ca-42f8-a036-9711e91bd1f3@DB8EUR06FT032.eop-eur06.prod.protection.outlook.com>
X-Sender-IP: 89.144.44.2
X-Priority: 1
Importance: high
MIME-Version: 1.0
Content-Type: text/html; charset="UTF-8"
Content-Transfer-Encoding: 8bit
```

Permanently forget this email header

4.Identifying suspicious links or attachments.

- No file attachments present**.**

- All interaction links lead to personal Gmail addresses instead of verified Microsoft domains.

- A hidden tracker is embedded, indicating possible email harvesting or engagement monitoring.

"Report The User" button

- **Visible text:** “Report The User”
- **Actual action:** Opens a mail client to send an email to mailto:sotrecognizd@gmail.com?subject=unusual signin activity&body=Report The User
- **Why it's suspicious:** Pretends to be a Microsoft action link, but contacts a personal Gmail address not associated with Microsoft.

"Unsubscribe me" link

- **Visible text:** “click here”
- **Actual action:** Also opens a new email to mailto:sotrecognizd@gmail.com?subject=Unsubscribe me
- **Why it's suspicious:** Microsoft uses secure unsubscribe pages, not email replies to unknown Gmail addresses.

Tracking pixel (invisible image)

- **URL:** http://thebandalisty.com/track/o43062rdzGz...

- **Purpose:** Hidden 1×1 pixel to detect if the email was opened.
- **Why it's suspicious:** Domain thebandalisty.com is unrelated to Microsoft and used for tracking purposes by attackers.

5. Urgent or threatening language in the email body.

Subject line:

"Microsoft account unusual signin activity"

- Immediately suggests a **security breach** and compels the recipient to check their account.

Opening line:

"We detected something unusual about a recent sign-in to the Microsoft account..."

- Implies the user's account may have been compromised.

Sign-in Details:

"A user from Russia/Moscow just logged into your account from a new device..."

- Specifically naming **Russia** and a **foreign IP address** (103.225.77.255) is designed to scare the user into action.

Call to Action:

"If this wasn't you, please report the user."

- Pushes immediate action, appealing to fear of unauthorized access

6. Mismatched URLs

Links and Their Real Targets:

1. **"Report The User" Button**
    - Display: Appears like a security action link.
    - Actual link: mailto:sotrecognizd@gmail.com?subject=unusual signin activity&body=Report The User
    - Mismatch: Instead of taking you to Microsoft or a secure login, it opens your email client to send a message to a Gmail address.

2. **"Unsubscribe me" / “Click here” Link**
    - Display: Poses as a standard unsubscribe option.
    - Actual link: mailto:sotrecognizd@gmail.com?subject=Unsubscribe me
    - Mismatch: Real unsubscribe links go to Microsoft-managed unsubscribe URLs, not personal Gmail.
3. **Hidden tracking image**
    - Source: http://thebandalisty.com/track/...
    - Mismatch: Microsoft would never use third-party domains like thebandalisty.com for tracking pixels.

7.Verify presence of spelling or grammar errors.

Identified Issues:

1. **Typographical/Punctuation Errors:**
    - “Unusual sign.in activity”
        - Should be: sign-in (hyphen instead of period)
2. **Grammatical Awkwardness:**
    - “A user from Russia/Moscow just logged into your account from a new device, If this wasn't you, please report the user.”
        - Incorrect: comma used where a period should be; capital “If” after comma.
        - Correct: "...from a new device. If this wasn't you..."
3. **Unnatural phrasing:**
    - “If this was you, we'll trust similar activity in the future.”
        - Sounds vague and not reflective of Microsoft’s tone. A real email would likely say, “You can safely ignore this message if the activity was yours.”

8. Phishing traits found in the email

The email displays multiple classic phishing characteristics, including:

1.Fake sender address

The email claims to be from the "Microsoft account team" but uses the sender

address no-reply@access-accsecurity.com, which is not a legitimate Microsoft domain.

2.Suspicious reply-to address
Any replies are directed to sotrecognizd@gmail.com, a personal Gmail address. Microsoft does not use Gmail for support communication.

3.Urgent and threatening language
The message warns that a user from Russia has logged into the recipient's account, urging the recipient to "report the user" immediately. This type of urgency is a known social engineering tactic to provoke a quick reaction.

4.Misleading and mismatched links
The buttons labeled "Report The User" and "Unsubscribe" look legitimate but actually open an email client to contact the attacker via the same Gmail address. These links do not lead to Microsoft's official domain.

5.Presence of tracking pixel
A hidden image from thebandalisty.com is embedded in the email. This is commonly used by attackers to track whether the recipient opened the email.

6.Spelling and grammar issues
Minor errors such as "sign.in" instead of "sign-in" and awkward sentence structure undermine the legitimacy and professionalism expected from Microsoft.

7.Authentication failures
The email failed standard email authentication checks: SPF is not set, DKIM is missing, and DMARC validation results in a permanent error. These are strong indicators of spoofing or email forgery.

8.Unfamiliar and unrelated sending infrastructure
The message passed through multiple suspicious domains, including thcultarfdes.co.uk, which is not associated with Microsoft and may be used to mask the true origin.

9.Lack of legitimate Microsoft links
Nowhere in the email is there a secure Microsoft link (such as login.microsoftonline.com or support.microsoft.com), which would be expected in genuine communications.