

## Objective: Identify phishing characteristics in a suspicious email sample.

### Step 1: Examine the "From" Address for Spoofing

#### Goal:

Determine if the sender's email address is **fake or impersonating** a legitimate source.

From: Microsoft account team ,\_<no-reply@access-accsecurity.com>

#### What We Notice:

Field	Observation
Display Name	Microsoft account team – This is <b>easily spoofed</b> . Anyone can set this.
Email Address	no-reply@access-accsecurity.com – Suspicious domain. Definitely <b>not</b> Microsoft.

- **Microsoft legitimate domains** include:

- microsoft.com
- account.microsoft.com
- outlook.com
- live.com

So this fails that test. Therefore, it is not a real Microsoft domain.

## Whois Lookup

```
(ayush@kali)-[~]  
$ whois access-accsecurity.com  
No match for domain "ACCESS-ACCSECURITY.COM".  
>>> Last update of whois database: 2025-05-27T14:29:27Z <<<
```

### Verdict:

- This is a spoofed sender pretending to be Microsoft.
- The domain is fake, trying to appear legit.
- Most likely part of a phishing campaign targeting Microsoft users.

## Step 2: Analyze the Email Headers for Technical Clues

### Goal:

Detect signs of **spoofing**, **relay abuse**, or **mismatched sender info** by checking the technical "Received" path of the email.

### Return-Path:

Return-Path: bounce@thcultarfdes.co.uk

- Different domain from what the "From" line showed (access-accsecurity.com)
- This is a spoof indicator — legitimate domains don't use unrelated return-paths.
- Also, thcultarfdes.co.uk looks like a nonsensical, suspicious domain

### Received Chain:

```
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=pererror 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
```

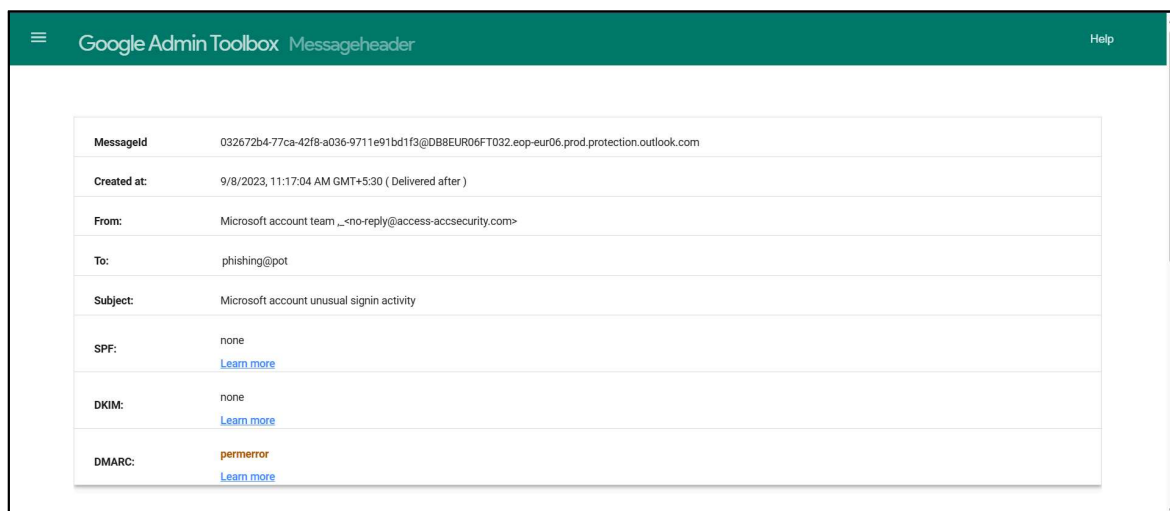
Fig : screenshot of the source code of the email

- This tells us the original server that sent the message was:
  - IP: 89.144.44.2
  - Domain: thcultarfdes.co.uk
- When traced, this IP belongs to a residential ISP in Europe — not Microsoft or a mail provider.

**Conclusion:** This email originated from a private server, not an official corporate email system.

## SPF, DKIM, and DMARC:

I analyzed the email header using the **Google Admin Toolbox – Messageheader** . The results for these are as follows:



Google Admin Toolbox Messageheader	
MessageId	032672b4-77ca-42f8-a036-9711e91bd1f3@DB8EUR06FT032.eop-eur06.prod.protection.outlook.com
Created at:	9/8/2023, 11:17:04 AM GMT+5:30 ( Delivered after )
From:	Microsoft account team _<no-reply@access-accsecurity.com>
To:	phishing@pot
Subject:	Microsoft account unusual sign-in activity
SPF:	none <a href="#">Learn more</a>
DKIM:	none <a href="#">Learn more</a>
DMARC:	permerror <a href="#">Learn more</a>

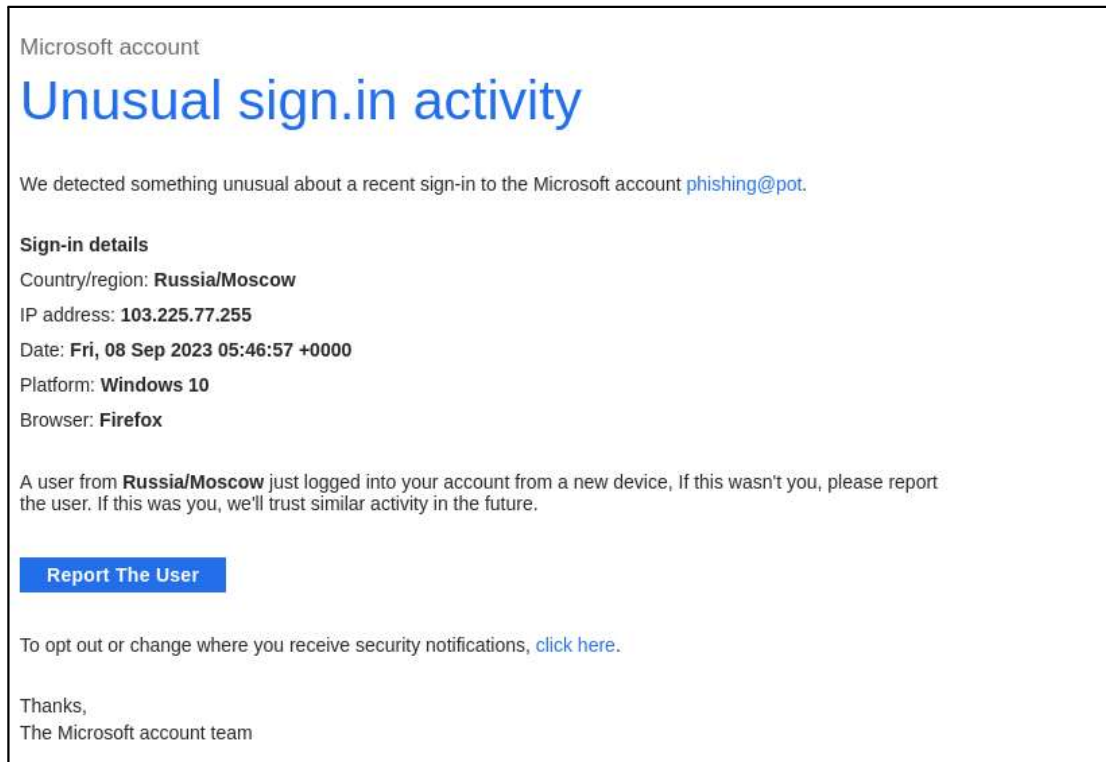
Protocol	Purpose	Status	Meaning
SPF	Verifies sender server is allowed to send for the domain	none	No SPF set → easy spoof
DKIM	Ensures message hasn't been altered	none	No cryptographic signature
DMARC	Enforces SPF/DKIM policy	permerror	Misconfigured → another red flag

These should all pass in legitimate corporate emails. Their absence is a major phishing indicator.

## Verdict:

- Fake origin server
- No authentication
- Return-path mismatch
- Header confirms sender was not authenticated properly

## Step 3: Analyze the Email Body



- **Spelling/grammar mistakes:** There are noticeable grammar and formatting issues:
  - a. The subject line and header say "**Unusual sign.in activity**" instead of "**Unusual sign-in activity.**"
  - b. The phrase "**If this wasn't you, please report the user**" is awkwardly phrased; typically, it would say "**If this wasn't you, please let us know**" or "**please report this activity.**"
  - c. The email ends with "**Thanks,**" and "**The Microsoft account team**" without proper punctuation or signature formatting.
- **Odd tone or broken formatting:** The tone is somewhat inconsistent and informal for a Microsoft security alert. The formatting is basic and lacks professional polish typical of official Microsoft emails. The email address mentioned is "phishing@pot," which is suspicious and not a legitimate Microsoft domain.

### Conclusion:

Overall, these clues strongly suggest the email is a phishing attempt designed to trick the recipient into clicking the "**Report The User**" button, potentially compromising their account. The combination of minor grammar errors, odd phrasing, suspicious sender address, and lack of direct Microsoft branding or professional formatting are key red flags.

## Step 4: Inspect URLs in the Email

While hovering over the button “**Report The User**”, the link appeared as:

“ **mailto:sotrecognizd@gmail.com?&cc=sotrecognizd@gmail.com&subject=unusual signin activity&body=Report the user** ” .

- **Use of a mailto link:** Instead of directing the user to a secure Microsoft webpage or official support portal, this link opens the user's email client to send an email to a generic Gmail address ([sotrecognizd@gmail.com](mailto:sotrecognizd@gmail.com)). Legitimate Microsoft security alerts do not ask users to report suspicious activity by emailing a public Gmail account.
- **Suspicious recipient address:** The email address is a free, personal Gmail account, not a Microsoft-owned domain. This is a classic phishing tactic to collect user responses or lure victims into further interaction.
- **Pre-filled subject and body:** The subject "unusual signin activity" and body "Report the user" try to simulate a legitimate report action but actually encourage direct communication with the attacker.
- **No secure verification:** Official Microsoft alerts instruct users to visit their account security page via a verified Microsoft domain to review recent activity or secure their account. They never ask users to send emails manually to unknown addresses.
- **Supporting context from search results:**
  - Microsoft's official guidance confirms that unusual sign-in alerts come with instructions to check recent activity on their secure site, not to send emails to third parties.
  - Phishing campaigns often mimic such alerts but use tactics like mailto links to bypass security filters and engage victims directly.

### Conclusion:

This hover link is a clear social engineering attempt designed to trick users into contacting an attacker-controlled email address under the guise of reporting suspicious activity. It bypasses legitimate security procedures and exposes users to phishing risks.

### Precautionary action:

Do not click or interact with such links. Instead, independently log in to your Microsoft account via the official website to check for any unusual activity. Mark the email as phishing and delete it.