1. Sender email address :

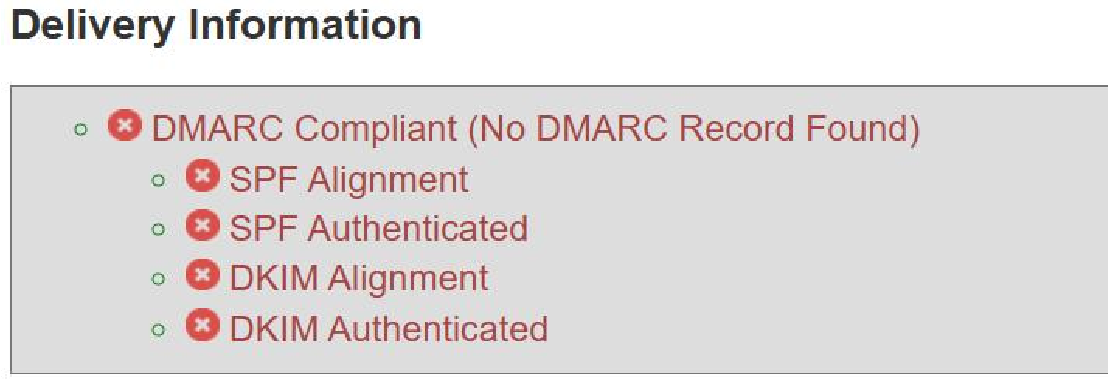
From: Microsoft account team , <no-reply@access-accsecurity.com>

By examining this address, it cannot be considered legitimate because instead of using an official Microsoft domain after the @ symbol (such as @microsoft.com or @account.microsoft.com), it uses access-accsecurity.com, which is not a Microsoft-owned domain.
This indicates it is likely a phishing attempt.

2. Discrepancy :

The email claims to be from Microsoft, but the sending server is not from Microsoft.
Return path: bounce@thcultarfdes.co.uk
When I attempted to look up this domain using WHOIS, it showed that the domain name is not registered, which is a major red flag.

Header Analysis Results (via mxtoolbox.com):



Delivery Information

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

DMARC = Domain-based Message Authentication, Reporting, and Conformance: It's a rule set published by a domain owner telling email providers how to handle messages that fail SPF or DKIM.

SPF = Sender Policy Framework: SPF alignment means the domain in the SPF check matches the From address domain.

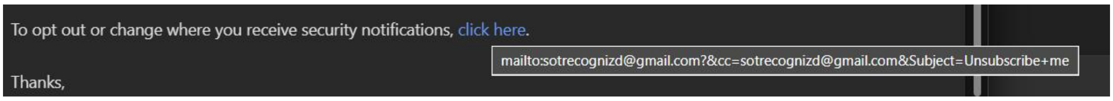
DKIM = Domain Keys Identified Mail: DKIM alignment means the signing domain in the DKIM signature matches the From address domain.

3. Email Type

The email contains urgent language ("A user from Russia/Moscow just logged into your account…") intended to create fear and push the recipient into acting quickly.
This is a common phishing tactic.

4. Mismatched url :

By hovering over the links in the email (without clicking), the visible link text appears to reference Microsoft's website, but the actual hyperlink directs to a different, suspicious domain unrelated to Microsoft.This is a classic phishing indicator.



To opt out or change where you receive security notifications, click here.

mailto:sotrecognizd@gmail.com?&cc=sotrecognizd@gmail.com&Subject=Unsubscribe+me

Thanks,