📄 Phishing Email Analysis Report

📩 Basic Email Details

Field	Value
Subject	Microsoft account unusual signing activity
From	Microsoft account team ,_no-reply@access-accsecurity.com
To	phishing@pot
Date	Fri, 8 Sep 2023 05:47:04 +0000
Reply-To	sotrecognizd@gmail.com
Sender IP	89.144.44.2 (from thcultarfdes.co.uk)

⚠️ Phishing Detection Points

1. Spoofed Sender Address

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

- Domain is **not owned by Microsoft**
- Format is invalid and suspicious

2. Authentication Failures

- SPF: none
- DKIM: none
- DMARC: none
  → All anti-spoofing protections failed

3. Unusual Location Alert (Fear Tactic)

- IP: 103.225.77.255 (Russia/Moscow)
- Tries to scare user into action

4. Suspicious Links

- mailto:sotrecognizd@gmail.com
- "Unsubscribe" also sends to attacker Gmail
- Tracking pixel from thebandalisty.com

5. HTML-Based Email with Branding

- Layout mimics Microsoft (fonts, colors, structure)
- But no genuine Microsoft URLs

6. Urgent or Threatening Language

- "A user from Russia/Moscow just logged into your account..."
- Threatens future action

7. Grammar Red Flags

- Comma splice: "..., If this wasn't you..."
- Suspicious punctuation in header

8. Reply-To is Gmail

- sotrecognizd@gmail.com – attacker's address
- Microsoft does not use Gmail

🔚 **Summary of Phishing Traits**

Indicator	Description
Fake sender domain	access-accsecurity.com
Reply-to mismatch	Gmail address used
Suspicious links	mailto trap, tracking pixel
IP scare tactic	Russia location mentioned
SPF/DKIM/DMARC	All missing or failed
Social engineering	Uses fear to provoke quick response
Fake branding	Mimics Microsoft interface & formatting