# Task2 : Phishing Email Analysis Report

1. What's This Email About?

I grabbed a phishing email sample from GitHub, saved as phishing email.eml, to see how scammers try to trick people. It pretends to be from the "Microsoft account team" and claims there's "unusual sign-in activity" for an account tied to phishing@pot. The email landed on August 2, 2023, at 03:34:35 +0000. Let's tear it apart to spot the shady stuff!

2. Is the Sender Legit?

- What I Found: The email claims it's from Microsoft account team <no-reply@access-accsecurity.com>, with replies going to solutionteamrecognizd03@gmail.com and a return address of bounce@iustozncau.co.uk. None of these look like Microsoft's real email addresses, which are usually @microsoft.com or @accountprotection.microsoft.com. A Gmail address? A random .co.uk domain? Big red flag. Oh, and "recognizd" in the reply address is totally misspelled.
- Why It's a Problem: Microsoft doesn't send official emails from free Gmail accounts or sketchy domains. This is a classic scam move to fake a legit sender.

3. Checking the Email's Techy Bits (Headers)

- What I Found: The email's behind-the-scenes details (called headers) scream "not Microsoft":
    - It flunks security checks (SPF, DKIM, DMARC—think of these as ID verification for emails).
    - It came from an IP address (89.144.9.91) linked to a German internet provider, not Russia (like the email claims) or Microsoft's servers.
    - The sender's domain (iustozncau.co.uk) doesn't match the "From" address (access-accsecurity.com) or anything Microsoft-related.
- Why It's a Problem: These mismatches are like a fake driver's license that doesn't scan. Real Microsoft emails pass these checks and come from their own servers.

4. Any Dodgy Links or Files?

- What I Found: The email has three links, but they're super fishy:
    - The "phishing@pot" link pops open an email to solutionteamrecognizd03@gmail.com with the subject "Report The User."
    - The "Report The User" button does the same, with a subject about "unusual signin activity."
    - The "click here" opt-out link also sends an email to that same Gmail address to "Unsubscribe."
    - There's a sneaky "tracking pixel" (a tiny hidden image) from thebandalisty.com that tells the sender if you opened the email.
    - No files were attached, so no worries there.

5. Is It Trying to Scare Me?

- What I Found: The email says things like:
    - “We detected something unusual about a recent sign-in.”
    - “A user from Russia/Moscow just logged into your account from a new device. If this wasn’t you, please report the user.”
      These lines are meant to spook you into clicking the “Report The User” link without thinking twice.
- Why It’s a Problem: Scammers love making you panic so you act fast. Real Microsoft emails are chill and straightforward, not dramatic like this.

6. Do the Links Match Up?

- What I Found: The “Report The User” and “click here” links look like they’ll take you to a legit Microsoft page, but they just open your email app to message a Gmail address. The tracking pixel points to thebandalisty.com, which has zero to do with Microsoft.
- Why It’s a Problem: Microsoft’s real emails link to their actual website, not random email addresses or weird tracking sites. These mismatches are a huge warning sign.

7. Any Typos or Weird Wording?

- What I Found: The email’s got some sloppy mistakes:
    - “Unusual sign.in activity” (whoops, a dot instead of a space in “sign.in”).
    - The subject line says “Microsoft account unusual signin activity” (missing a hyphen in “sign-in”).
    - The line “we’ll trust similar activity in the future” sounds way too casual for Microsoft’s usual polished style.
    - The reply address has “recognizd” instead of “recognized.”
- Why It’s a Problem: Microsoft’s emails are squeaky clean with no typos. These slip-ups show someone threw this together in a hurry, and it wasn’t Microsoft.

8. Why This Email’s a Total Phishing Scam

This GitHub sample is a textbook phishing email. Here’s the rundown:

- Fake Sender: The email addresses (access-accsecurity.com, gmail.com, iustozncau.co.uk) aren’t Microsoft’s.
- No Security Cred: It fails SPF, DKIM, and DMARC checks, so it’s not legit.
- Shady Links: Those mailto: links to Gmail and the tracking pixel from thebandalisty.com are not Microsoft’s style.
- Panic Tactics: It tries to scare you with “unusual sign-in” warnings.
- Sloppy Writing: Typos like “sign.in” and “recognizd” are dead giveaways.
- No Personal Touch: It doesn’t use your name, unlike Microsoft’s real alerts.

- Made-Up Details: The “Russia/Moscow” sign-in and IP 103.225.77.255 seem fake, and the real sender IP (89.144.9.91) doesn’t match.
- Sneaky Tracking: That hidden image from thebandalisty.com tracks if you open the email, which is pure scammer vibes.

What to Do with Phishing Emails Like This

Since this is a GitHub sample, it’s great for learning, but here’s what to do if you get a real one:

1. Don’t Touch the Links: Those Gmail mailto: links are trouble. Stay away.
2. Report It: Forward it to reportphishing@microsoft.com or hit “Report Phishing” in your email app.
3. Check Your Account: Type https://account.microsoft.com into your browser (don’t click email links) to make sure everything’s okay.
4. Beef Up Security: Turn on two-factor authentication in your Microsoft account for extra safety.
5. Warn Others: Share this with friends—watch out for emails with weird links or scary messages!