Task 2: Phishing Email Analysis Report

Objective:

Identify phishing characteristics in a suspicious email sample.

Phishing Email Characteristics:

Subject: Microsoft Account - Unusual Sign-in Activity
Sender: no-reply@access-accsecurity.com
Reply-to: solutionteamrecognizd02@gmail.com
Email Body Theme: Microsoft sign-in alert claiming suspicious login from Russia.

Technical Analysis

1.EML Analyzer Findings:

- **Attack Verdict:** Malicious
- **Attack Signals:**
  - Brand Impersonation: Pretends to be Microsoft.
  - Credential Theft: Uses language to trick users into providing credentials.
  - Suspicious Sender: Domain access-accsecurity.com is **not registered**, indicating spoofing.
- **Mismatches Detected:**
  - Reply-to email uses a free Gmail address.
  - No domain authentication (SPF/DKIM/DMARC failures).

2. WHOIS Lookup

- Domain access-accsecurity.com was checked.
- Result: Domain does not exist or is not registered, proving spoofed "From" address.

3.VirusTotal URL Scan

- The URL found in the email leads to an AWS-hosted link flagged by multiple security vendors:

    - **CRDF:** Malicious
    - **Phishing Database:** Phishing
- Other vendors may mark it clean initially, but this reflects evolving detection rates.

The email is a confirmed phishing attempt designed to impersonate Microsoft security notifications, create urgency via a fake sign-in alert, steal user credentials through malicious links.