**Task 2 – Phishing Email Analysis Report**

**Objective:**

To identify phishing characteristics in a suspicious email and list the indicators found.

**Phishing Email:**

From: Apple Support <support@apple.verifylogin.com>

Subject: Urgent: Suspicious activity detected on your Apple ID

Dear Customer,

We detected unusual login activity on your Apple ID. For your security, your account has been temporarily locked.

Please verify your identity to unlock it:

[Click here to verify your account]

Failure to verify within 24 hours will result in permanent suspension.

Thank you,

Apple Support

**Phishing Indicators Found:**

| **No.** | **Indicator** | **Description** |
| --- | --- | --- |
| 1 | **Fake Email Address** | The email is from @verifylogin.com, which is not Apple’s official domain (@apple.com). |
| 2 | **Urgent/Scary Language** | Subject line says "Suspicious activity detected", which creates fear and urgency. |
| 3 | **Generic Greeting** | Uses “Dear Customer” instead of recipient's actual name, shows it's bulk email. |
| 4 | **Scare Tactics in Body** | Email says the account is "locked" to scare the user into clicking the link. |
| 5 | **Fake Link** | The link looks like Apple but actually redirects to a suspicious domain (verifylogin.com). |

**Conclusion:**

This email contains multiple phishing indicators including a fake sender domain, threatening language, and a suspicious link. It is not from a genuine Apple source. Users should not click on any links or share personal information.

**THANK YOU**