**TASK-2**

**ANALYSE A PHISHING EMAIL SAMPLE**

* The sender address here shows to be @**msupdate**.**net** but MS OFFICE usually uses @microsoft.com, @account.microsoft.com or @email.microsoft.com. Hence, the address is not a official one but a fake malicious used for phishing purpose.
* When we look at the header it looks more of like urgency, it states, “YOUR PASSWORD CHANGED’. It makes one panic and makes you urgent. It is one of phishing tactics.
* Other suspicious content includes “if this wasn’t you, your account has been compromised”- this creates a sense of panic and it gives out a tone of concern and urgency.
* They design these to make ourselves panic and click without thinking.
* There is no exact time of when the password was changed or any information regarding device, this is suspicious.
* The instructions given are, “reset your password” but doesn’t provide any official Microsoft office link. The malicious link maybe hidden in the text provided.
* This is a well-written email which makes it difficult to acknowledge it as a malicious one.
* At **conclusion**, the **phishing indicators** found are:

Spoofed sender

Urgency techniques

Social engineering

Suspicious request

Mismatched Branding.