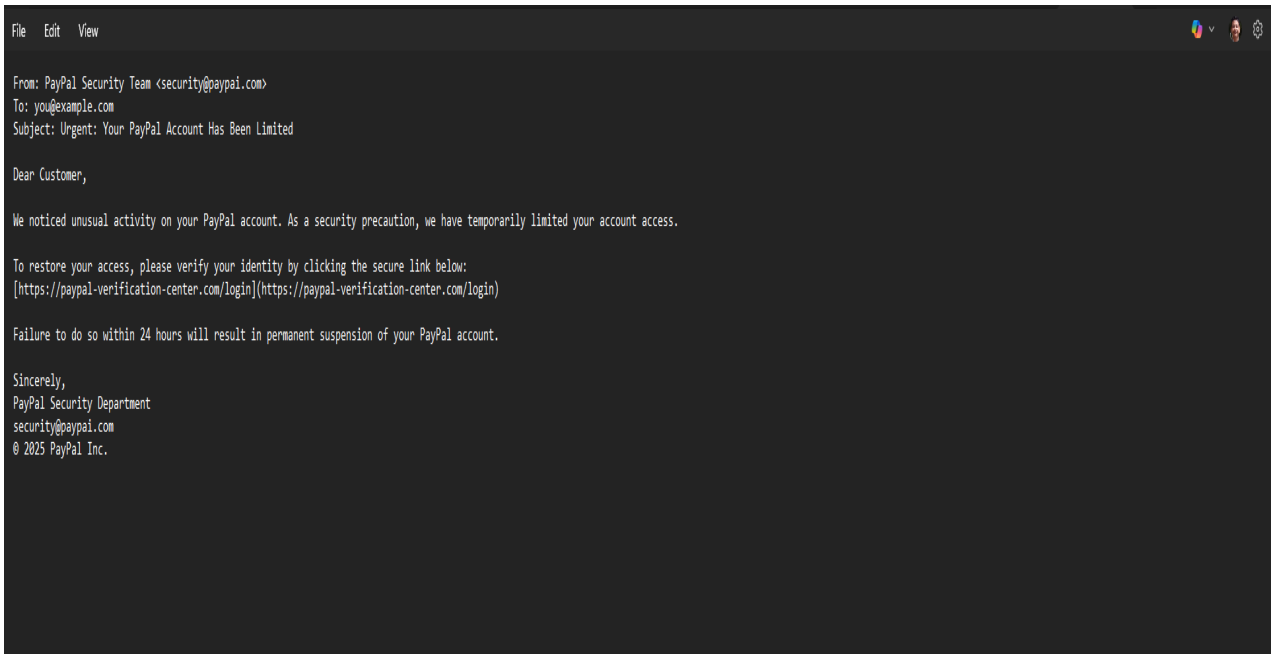
Spondon Nath

Task 2 :

Email:



Report :

The above email contains a number of phishing indicators, which I picked up using publicly available cybersecurity tools. The sender's email address (security@paypai.com) is a spoofed version of PayPal's domain name and is obviously intended to deceive the target recipient. The subject, "Urgent: Your PayPal Account Has Been Limited," is meant to be intimidating and elicit user response straight away. The email content sustains the sense of urgency by stating that the account will be suspended if the user doesn't respond within 24 hours. The email content contains a dodgy link — https://paypal-verification-center.com/login — that is a close imitation of PayPal branding but leads to a possibly malicious third-party website.

To check this, I used VirusTotal, a web-based free threat intelligence tool. It informed me that the link had been detected as phishing by one among 97 security vendors, which reflects the likely threat of credential theft. I also scanned the email header using the Google Admin Toolbox MessageHeader analyzer. It informed me that the email did not pass all three major authentication tests, which include SPF, DKIM, and DMARC. This

indicates that the sender's domain has not been verified and the message could not be authenticated as legitimate.

Also, the email lacks any personalisation, basically the ‘Human Touch’ and includes a generic greeting ("Dear Customer"), which is not typical for professional services such as PayPal. Although the message is grammatically correct, this is actually a higher threat level since it is most likely to trick more users into believing it is real. The whole combination of spoofed identity, domain authentication failure, a phishing URL, and psychological pressure tactics ensure the fact that this is a phishing email.

Phishing Traits Summary:

Trait	Area
Spoofed sender domain	The sender’s email address - ‘security@paypai.com’ is a spoofed version of the original PayPal domain.
Urgency / Threatening tone	Subject - ... aims to trigger panic" and "warning of account suspension if the user does not act
Suspicious link	https://paypal-verification-center.com/login... redirects to a potentially malicious site
VirusTotal result	Flagged as phishing by one of the 97 security vendors
Header failures (SPF, DKIM, DMARC)	Failed all three major authentication checks..." with each term explained
Generic greeting	The email lacks personalization and uses a generic greeting
Grammatically correct but deceptive	Language appears grammatically correct... increases the threat level
Urgency	“Failure to do so…”