TASK – 2

1.Understading the task :

This report analyzes a sample phishing email to identify key indicators of phishing and provide recommendations for recognizing and avoiding such threats. The findings aim to enhance email security awareness from an ethical hacker's perspective.

2. **Phishing Email :**

From: PayPal Support <paypalsupport@gmail.com>

Subject: Urgent: Account Suspension Notice

Dear Customer,

We have detected suspicious activity on your PayPal account. Your account will be suspended within 24 hours unless you confirm your identity. Please click the link below and login to restore access:

Restore Account

If you do not respond, your account will be permanently deactivated.

Thankyou,
PayPal Security Team

Feature	**Sample Evidence/Example**	**Why This is Suspicious**
Sender's Email	paypalsupport@gmail.com	Not from the official PayPal domain; legitimate emails use @paypal.com.
Greeting	"Dear Customer"	Generic greeting; real companies usually use your real name.
Link	"RestoreAccount"→http://malicious-link.com	Link does not direct to a PayPal website; could steal credentials.
Urgent Language	Account will be suspended within 24 hours	Creates panic to trick recipients into acting quickly
Spelling/Grammar Error	Check for mistakes (none obvious here)	Often present; can signal a scam.
Signature	"PayPal Security Team", no real contact info	Missing company contact details and legal disclaimers

4. Email Header Findings :

- The sender's domain (Gmail) is not consistent with PayPal.
- Lack of SPF/DKIM authentication records (if checked in header analyzer).
- The "Reply-To" or "Return-Path" may differ from the "From" address.

6. Conclusion & Recommendations

This email displays multiple phishing characteristics: fake sender, urgent language, suspicious link, and lack of personalization.

Recommendations:

- Never click suspicious links.
- Always verify unexpected messages with the company directly.
- Use two-factor authentication and keep security software up to date.
- Report phishing attempts to your IT or security team.