Phishing Email Analysis Report – Cyber Security Internship Task 2

# Task Objective

Analyze a phishing email and identify common phishing characteristics using free tools and techniques. This task helps build practical awareness of email-based threats such as phishing, spoofing, and social engineering.

# Sample Email Details

Subject: Urgent: Your PayPal Account Has Been Limited!

From (Name): PayPal Support

From (Email): security-update@secure-paypal.net

Attachment: Update\_Account\_Info.zip

Link in Email: http://paypal-login-authenticate.com

# Phishing Indicators Found

## Spoofed Email Address

The email claims to be from PayPal, but the actual sender domain is secure-paypal.net, which is not an official PayPal domain. This is a common tactic in phishing.

## Suspicious Email Header

Email headers can reveal forged “From” fields. Likely SPF/DKIM failures. IP origin could mismatch known PayPal IPs.

Analyzed via Google Header Analyzer: https://toolbox.googleapps.com/apps/messageheader/

## Malicious Link

Displayed Link Text: “Click here to restore access”. Actual URL: http://paypal-login-authenticate.com. This is a phishing site designed to steal credentials.

## Suspicious Attachment

.zip file attached: Update\_Account\_Info.zip. Likely contains malware. Scan with VirusTotal: https://www.virustotal.com/

## Urgent and Threatening Language

Example line: “Failure to verify your identity within 24 hours will result in permanent suspension.” This is a classic social engineering tactic.

## Mismatched URL Text

The text says “restore access,” giving the impression of a secure link. Hovering reveals a non-official domain.

## Spelling & Grammar Errors

Example: “Your account has been temporary limited” – incorrect grammar. Such errors are common in scam emails.

# Tools Used

• Google Message Header Analyzer – https://toolbox.googleapps.com/apps/messageheader/

• VirusTotal – https://www.virustotal.com/

• URLVoid – https://www.urlvoid.com/

# Conclusion

This email is a classic example of a phishing attack. It combines spoofed sender details, malicious links, fake urgency, and malware-laced attachments to deceive users. Always verify suspicious emails using trusted tools before taking action.