Task 2 – Phishing Email Analysis

Objective: Identify phishing characteristics in a suspicious email sample.

Tools Used:

• Email client (for viewing sample email)
• MxToolbox (email header analysis)
• Web browser (to inspect links)

Steps Followed:

- Obtained a sample phishing email from a public phishing archive.
- Checked the sender's email for domain mismatches (e.g., security@paypa1.com instead of paypal.com).
- Analyzed email headers using MxToolbox.
- Identified suspicious links by hovering over them without clicking.
- Looked for urgent or threatening language.
- Checked for spelling and grammar errors.
- Detected mismatched displayed link and actual URL.
- Summarized phishing traits.

Phishing Indicators Found:

Indicator	Example	Risk
Spoofed Sender	security@paypa1.com	Domain impersonation
Mismatched Links	Text: https://paypal.com → Actual: http://malicious.com	Credential theft
Urgent Language	Verify now or lose access	Social engineering pressure
Grammar Errors	Your account are suspended	Phishing clue
Suspicious Attachments	invoice.zip	Possible malware

Security Recommendations:

- Never click suspicious links.
- Verify sender's email domain.
- Use email header analysis tools.
- Enable spam filters.
- Report phishing to your email provider.

Interview Questions & Answers:

Q: What is phishing?
A: A cyber attack where attackers trick users into revealing sensitive information via fraudulent emails or websites.

Q: How to identify a phishing email?
A: Check for spoofed senders, mismatched URLs, grammar errors, and suspicious attachments.

Q: What is email spoofing?
A: Forging the sender's address to appear legitimate.

Q: Why are phishing emails dangerous?
A: They can steal credentials, infect systems, or commit fraud.

Q: How can you verify the sender’s authenticity?
A: Use header analysis tools and verify domains.

Q: What tools can analyze email headers?
A: MxToolbox, Google Admin Toolbox, Microsoft Message Header Analyzer.

Q: What actions should be taken on suspected phishing emails?
A: Do not click links, report to security team, block sender.

Q: How do attackers use social engineering in phishing?
A: They create urgency, fear, or curiosity to trick victims.