Phishing Email Analysis Report

Step 1: Phishing Email Sample

Sample Email:

From: micorsoft-support@example.com

Subject: Urgent: Account Verification Required

Body: Your account will be suspended if you do not verify your credentials immediately.

Click here to verify: http://malicious-site.com/login

Attachment: invoice.zip

Step 2: Sender Email Analysis

- Misspelled domain: micorsoft-support@example.com
- Display name does not match official Microsoft domain

Step 3: Header Analysis

- SPF failed
- DKIM not verified
- DMARC failed
- Sender IP does not match legitimate Microsoft servers

Step 4: Suspicious Links and Attachments

- Link redirects to http://malicious-site.com/login
- Attachment invoice.zip is potentially malicious

Step 5: Urgent Language

- Phrases like "Your account will be suspended" and "Immediate action required" indicate phishing attempt

Step 6: Spelling and Grammar

- Misspellings and awkward grammar throughout the email

Step 7: Phishing Traits Summary

Indicator	Details

Sender Email	micorsoft-support@example.com (misspelled domain)
Header Analysis	SPF fail, IP mismatch
Links	Redirects to http://malicious-site.com/login
Attachments	invoice.zip (suspicious)
Language	Urgent, threatening tone
Grammar/Spelling	Multiple errors
Phishing Type	Credential theft / malware delivery

Step 8: Interview Questions

1. What is phishing? Attempt to steal sensitive information via deceptive emails.

2. How to identify a phishing email? Suspicious sender, unexpected links/attachments, urgency, spelling errors, header inconsistencies.

3. What is email spoofing? Faking the sender's address to appear legitimate.

4. Why are phishing emails dangerous? They can steal credentials, install malware, or commit fraud.

5. How to verify sender authenticity? Check headers, SPF/DKIM/DMARC, contact sender via official channels.

6. Tools to analyze headers? MXToolbox, Google Admin Toolbox, MailTester.

7. Actions on suspected phishing emails? Do not click links, report, delete/quarantine.

8. Social engineering in phishing? Exploits fear, urgency, curiosity, or trust.