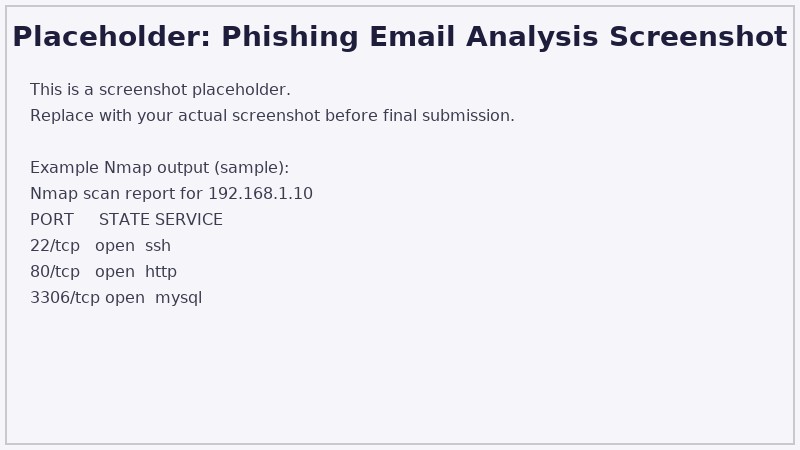
**Task 2: Analyze a Phishing Email Sample**

**Objective:** Identify phishing characteristics in an email sample to improve detection skills. **Tools Used:** Email client/text file for sample, online header analyzer (e.g., MXToolbox), browser **Procedure / Steps:**

1. Obtain a phishing email sample (saved message or screenshot).
2. Inspect the 'From' address: check for small typos or domain spoofing (e.g., support@paypa1.com).
3. View full email headers to trace origin (Received headers) and check SPF/DKIM/DMARC results.
4. Hover over links to reveal actual URLs; do not click. Check for mismatched domains or use an URLscanner.
5. Examine attachments for suspicious file types (e.g., .exe, .scr) and scan with antivirus.
6. Look for social-engineering indicators: urgency, threatening language, unexpected requests forcredentials.
7. Document findings and advise next steps (report, block sender, notify security team).



**Common Phishing Indicators (Example Findings):**

* Sender domain mismatch: display name claims bank but email domain is unrelated.
* Suspicious link redirecting to non-official domain (check full URL).
* Poor grammar and urgent tone asking to 'verify account now'.
* Email headers indicate relay through unusual IPs or failing SPF/DKIM.

**Recommended Actions:**

1. Do not click any links; report the email to the IT/security team.
2. Block the sender and mark the message as phishing in the mail client.
3. If credentials were entered, initiate password reset and MFA enforcement.
4. Educate users about recognizing spoofed domains and safe email practices.

**Conclusion:**

Regular network scanning (Task 1) and phishing analysis (Task 2) are essential components of an organization's defensive posture. Scans reveal exposed services that need mitigation; phishing analysis reduces the success rate of social engineering attacks. Combine technical controls (firewall, patching, email filters) with user education for best results.