Task 2 – Phishing Email Analysis (Anonymized)

Task 2 – Phishing Email Analysis (Anonymized)

Objective
Analyze a sample phishing email and identify indicators that suggest it is malicious. All sensitive details (addresses, links, names) have been anonymized.

Steps Followed
1. Obtained a sample phishing email (saved as text). The content was anonymized prior to analysis.
2. Examined the 'From' field and display name for spoofing: the display name matched a known organization, but the actual sending address was inconsistent with the organization's domain (anonymized here).
3. Analyzed email headers using an online header analyzer to check origin IPs, SPF/DKIM/DMARC authentication results, and 'Received' chains.
4. Hovered over links in the email body to reveal mismatched URLs (anonymized). No attachments contained executable files in this sample.
5. Checked the message body for social engineering cues: urgency, threats, and requests for credentials.
6. Compiled findings and recommendations for remediation and user awareness.

Findings (Anonymized)
- Sender spoofing: Display name impersonates a trusted organization; sending address uses a suspicious third-party domain.
- Authentication failures: SPF and DKIM checks failed or were neutral (anonymized result shown as 'failed/none').
- Malicious links: Visible links point to familiar domains, but hovering reveals redirectors or unrelated domains (anonymized).
- Urgent language: The email demanded immediate action ("verify now" / "account will be closed"), which is a classic phishing cue.
- Grammar and formatting: Several awkward phrases and minor spelling errors present.
- No malicious attachments detected in this sample; links were the primary vector.
- Header anomalies: 'Received' headers indicate the message traversed unexpected intermediary servers (anonymized).

Risk Assessment
- High: If clicked, links could lead to credential harvesting pages.
- Medium: Email could be used in targeted spear-phishing if combined with other contextual info.
- Low: No active malware attachment found in this sample.

Recommendations
- Do not click links or download attachments from suspicious emails.
- Verify senders by contacting the organization via official channels (not via email reply).
- Implement and enforce SPF, DKIM, and DMARC for organizational domains.
- Educate users about phishing red flags (urgency, mismatched URLs, odd sender addresses).
- Use email gateway filtering and URL reputation services to block malicious links.
- Report the phishing email to the security team and to anti-phishing services if applicable.

Sample Anonymized Evidence (excerpt)
- From: "Trusted Org"
- Subject: "Important: Verify Your Account Now"
- Link shown: https://trusted-org.example.com/verify
- Link target (hover reveals): https://redirector.example.net/track?u=malicious-page

Deliverables
- `phishing_analysis_anonymized.pdf` → This report (anonymized)
- `phishing_evidence_anonymized.txt` → Extracted anonymized headers and link evidence
- `README.md` → Short README describing repo contents