Phishing Prevention

# ****Phishing Prevention – Notes****

### **Task 1 – Introduction**

* Phishing is a cyberattack where attackers impersonate trusted entities via email to steal sensitive data.
* Prevention techniques rely on authentication mechanisms, secure protocols, and traffic analysis.

### **Task 2 – SPF (Sender Policy Framework)**

* Email authentication method that prevents spoofing.
* Works via DNS TXT records.
* Defines which mail servers are allowed to send email for a domain.
* Example:
* v=spf1 include:\_spf.google.com ~all
* Outcomes: **Pass, Fail, SoftFail, Neutral**.

### **Task 3 – DKIM (DomainKeys Identified Mail)**

* Ensures integrity & authenticity of email.
* Uses **public-key cryptography** (RSA).
* Email headers/body signed with a private key, receiver verifies with public key in DNS.
* Prevents tampering during transit.

### **Task 4 – DMARC (Domain-Based Message Authentication, Reporting & Conformance)**

* Builds on SPF & DKIM.
* Defines a domain’s email handling policy if SPF/DKIM checks fail.
* Published via DNS TXT records.
* Example policy:
* v=DMARC1; p=reject; rua=mailto:dmarc-reports@domain.com
* Helps block spoofed/fake emails.

### **Task 5 – S/MIME (Secure/Multipurpose Internet Mail Extensions)**

* Provides **encryption + digital signatures** for emails.
* Uses **X.509 certificates**.
* Ensures:
  + **Confidentiality** (via encryption).
  + **Integrity & Authentication** (via digital signature).
* Supported by most enterprise email systems.

### **Task 6 – SMTP Status Codes**

* SMTP (Simple Mail Transfer Protocol) handles email transmission.
* Codes:
  + **2xx** → Success (e.g., 250 OK).
  + **4xx** → Temporary failure (retry later).
  + **5xx** → Permanent failure (e.g., 550 User not found).

### **Task 7 – SMTP Traffic Analysis**

* SMTP traffic can be analyzed to detect anomalies.
* Suspicious signs:
  + Large outbound email volume.
  + Connections to unusual IPs.
  + Use of non-standard ports (e.g., TCP 2525 instead of 25/587).
* Tools: Wireshark, tcpdump, IDS/IPS.

### **Task 8 – SMTP and C&C Communication**

* Attackers abuse SMTP for **Command & Control (C2)**.
* Malware can use emails to:
  + Receive commands.
  + Exfiltrate stolen data.
* Detection:
  + Look for suspicious email attachments.
  + Monitor outbound traffic to unknown mail servers.

### **Task 9 – Conclusion**

* Phishing prevention requires **layered defense**:
  + SPF, DKIM, DMARC for authentication.
  + S/MIME for confidentiality & integrity.
  + Monitoring SMTP status codes and traffic.
  + Detecting C2 misuse of SMTP.

