In [ ]:

```
Training Day 19 Report– 11 July 2025
 Introduction
 Day 19 focused on phishing and email-borne threats: how attackers craft messa
 senders, and embed malicious content.
 Key Concepts Discussed
 We discussed email authentication protocols (SPF, DKIM, DMARC) conceptually,
 they reduce spoofing, and their limitations. The session covered indicators c
 and steps to evaluate suspicious messages.
 Lab Preparation in Theory
 Plans for simulated phishing campaigns were described, including ethical cons
sent, and safe remediation. The trainer explained how to measure campaign effe
 and remediate vulnerable behaviors.
 Practical Understanding (Theory)
 We discussed secure mail gateways, attachment sandboxing, URL analysis, and u
 reporting channels as layered defenses against email threats.
 Key Takeaways
 Email remains a primary attack vector; layered defenses and user training wor
 to reduce success rates.
 Conclusion
 Next session will address endpoint threats and monitoring strategies.
```