Task 11: Phishing Attack Simulation & Detection

(Educational & Defensive Simulation) **By : NROUPSINH GOHIL**

Objective

To understand how phishing attacks work, identify common phishing indicators, simulate a **controlled phishing scenario** in a lab environment, and learn effective detection and prevention techniques.

What is Phishing?

Phishing is a **social engineering attack** where attackers trick users into revealing sensitive information such as usernames, passwords, OTPs, or bank details by pretending to be a trusted entity (bank, company, admin, etc.).

Phishing Simulation (Lab-Only & Ethical)

Note:
This simulation was performed in a **controlled test environment** for learning purposes only.
No real users or real credentials were targeted.

1 Phishing Email Template (Example – Analysis Only)

A test email was **designed for awareness**, containing:

- Urgent tone (“Action required”, “Account will be suspended”)
- Spoofed sender name (appears trusted)
- Suspicious link text
- Generic greeting (“Dear User”)

Observation:
Such elements are commonly used by attackers to create panic and force quick action.

---

2 Landing Page Simulation (Conceptual)

A fake login-style page was **theoretically designed** to study:

- How users may be tricked into entering credentials
- How attackers collect data

Observation:
Users often fail to verify URLs and HTTPS certificates.

---

3 Tracking & Response Analysis (Conceptual)

In phishing simulations:

- Email open rate
- Link click rate
- Data submission attempts
  are tracked to understand user behavior.

Observation:
Urgency + trust branding significantly increases success rate.

Phishing Red Flags Identified

Indicator	Explanation
Urgent language	“Act now”, “Account blocked”
Unknown sender	Domain mismatch
Suspicious links	Shortened or misspelled URLs
Generic greeting	No personal name
Grammar mistakes	Poor language quality
Attachment warnings	Unexpected files

Phishing Prevention Techniques

- Enable **Email Filtering & Spam Protection**
- Always **verify sender email address**
- Hover over links before clicking
- Never share OTPs or passwords
- Enable **Multi-Factor Authentication (MFA)**
- Conduct **user awareness training**
- Use browser & email security extensions

Deliverables Summary

✓ Phishing awareness report
✓ Red flags identification
✓ Prevention techniques
✓ Ethical simulation explanation

Final Outcome

This task helped build **strong awareness of phishing attacks**, improved ability to **identify malicious emails**, and reinforced **defensive security practices** against social engineering.