

## Task 11: Phishing Attack Simulation & Detection

### Tools:

- GoPhish
- Alternatives: Manual phishing templates

### Hints / Mini Guide:

1. Understand phishing attacks.
2. Create fake email template.
3. Setup landing page.
4. Send test phishing email.
5. Track responses.
6. Identify red flags.
7. Learn prevention.
8. Document simulation.

### Deliverables:

- Phishing simulation report

### Final Outcome:

- Social engineering awareness

### Interview Questions Related To Above Task:

- What is phishing?
- Types of phishing?
- How to detect phishing?
- Why phishing is dangerous?
- Prevention methods?

## Task Submission Guidelines

-  **Time Window:**

You can complete the task anytime between 10:00 AM to 10:00 PM on the given day. Submission link closes at 10:00 PM.

-  **Self-Research Allowed:**

You are free to explore, Google, or refer to tutorials to understand concepts and complete the task effectively.

-  **Debug Yourself:**

Try to resolve all errors by yourself. This helps you learn problem-solving and ensures you don't face the same issues in future tasks.

-  **No Paid Tools:**

If the task involves any paid software/tools, do not purchase anything. Just learn the process or find free alternatives.

-  **GitHub Submission:**

Create a new GitHub repository for each task.

Add everything you used for the task — code, datasets, screenshots (if any), and a short README.md explaining what you did.

### Submit Here:

After completing the task, paste your GitHub repo link and submit it using the link below:

-  [\[Submission Link\]](#)

