

Homework

Three tasks to turn the lab into a reusable phishing-defense playbook.

All homework is **defensive**: awareness content, detection, and policy. Never send unauthorized phishing to real people.

Task 1 — Awareness Training Module

Objective

Turn campaign analysis into user-facing content.

Instructions

1. Pick three phishing emails from the lab.
2. For each, write a 100-word "red flag walkthrough" in plain language for non-technical employees.
3. Include a "what to do instead" step for each.

Deliverable

A one-page employee handout in markdown.

Task 2 — DMARC Deployment Plan

Objective

Propose a phased DMARC rollout that would block the lab campaign.

Instructions

1. Draft an SPF, DKIM, and DMARC record for a fictional acmecorp.com.
2. Describe a 90-day rollout: monitor → quarantine → reject.
3. For each phase, list monitoring metrics and rollback triggers.

Deliverable

Rollout plan as markdown.

Task 3 — Lookalike Domain Monitor

Objective

Automate domain monitoring.

Instructions

1. Write a Python script that, given a brand domain, generates common typo-squat and homograph variants.
2. Bonus: check each variant against a DNS resolver to see if it is live.
3. Output: CSV with variant, technique, live Y/N.

Deliverable

`domain_monitor.py`.