Practical Session: Social Engineering - Phishing and Baiting

---

1. STUDENT WORKSHEET

Activity 1: Video Reflection\ Watch the two video clips provided and fill in the table below:

Attack Type	Technique Used	How Victim Reacted	Red Flags Noticed

Activity 2: Mock Phishing Email Creation\ Create a basic phishing email targeting a student or staff member. Use persuasive language.

Scenario Given: You want the recipient to believe they need to reset their university portal password.

Write your mock phishing email below:

```
Subject:

Body:

Link (optional):
```

Lab Exercise – Part A: Phishing Email Analysis\ Analyze the provided phishing email samples and answer:

1. What is the **goal** of the email?
2. What **psychological trick** is being used? 3. ## List 2 signs that indicate this is a phishing attempt: -
3. What type of phishing attack is this (e.g., spear phishing, whaling, etc.)?

---

2. FLOWCHART TEMPLATE: "Planning a Phishing Attack"

Students should sketch a flowchart showing the stages of a phishing attack:

Start:

- Research target (LinkedIn, company website)
- Create phishing email/webpage
- Send to target
- Target opens email/clicks link
- Credentials/data entered
- Data harvested
- Attacker access/use/exfiltrate data

End

(Students can draw this or use sticky notes to represent each step.)

---

3. QUIZ: End-of-Class Assessment

Name: _____ Date: _____

Instructions: Answer the following questions. Circle the correct answer where applicable.

1. What is phishing?\ a) Sending gifts via email\ b) Tricking someone into giving sensitive info via fake messages\ c) Fishing for bugs in code

2. Which of the following is a red flag in an email?\ a) Personalized greeting\ b) Grammar errors and urgent tone\ c) Domain-matched email address

3. What is baiting?\ a) Offering fake rewards or media (e.g. USBs) to trick victims\ b) Waiting patiently for a victim to click\ c) Sending a mass email to many people

4. List two techniques hackers use in phishing attacks:

---

5. What tool can simulate a phishing attack in a controlled lab?

[BONUS] What is the best way to avoid phishing?

---

4. INSTRUCTOR CHEAT SHEET (SET DEMO)

Social-Engineer Toolkit (SET) Basic Phishing Demo on Kali Linux

Step-by-Step:

1. Open terminal, type:

```
sudo setoolkit
```

1. Select:

From the main menu:

- 1. Social-Engineering Attacks - 1. Spear-Phishing Attack Vectors - 2. FileFormat Attack - 13. Adobe PDF Embedded EXE Social Engineering

1. When prompted:

2. Choose a safe payload (or cancel before completion)

3. SET will generate a malicious-looking PDF

4. Save location: `/root/.set/reports/`

5. Do not send or open the PDF — only demonstrate that such a file can be crafted.

Alternate Safe Demo: Use:

- 5. Mass Mailer Attack
- Send a mock email (no attachment or malicious link) to demonstrate phishing email content only

---

Understanding LHOST and LPORT

- **LHOST**: Local Host – the attacker's IP address (your Kali machine)
- To find it, run: `ip a`
- Look for the IP under your active interface (e.g., `192.168.56.x`)
- **LPORT**: Local Port – the port your listener will use (e.g., `4444`)
- Default is usually `4444`, but you can use any free port above 1024
- To check availability: `netstat -tuln | grep 4444`

Example: If Kali IP is `192.168.56.101`, and you use port `4444`:

```
LHOST = 192.168.56.101
LPORT = 4444
```

The payload will connect back to that IP and port, opening a shell.

Ensure your **Kali VM and target VM are on the same network** (e.g., Host-Only Adapter).

Warnings:

- Ensure this is in a **closed lab network**
- **NEVER** send malicious files or emails to real users
- Use only for **educational demonstration**

Let students reflect on what they learned using these tools and what ethical guidelines must always be followed.