📘 Day 2 – Social Engineering & Phishing (Summary Notes)

1. 🎭 What is Social Engineering?

- Social engineering is the act of **manipulating people** into making security mistakes.
- Attacks target **humans, not computers**, using psychological tricks like:
  - **Urgency**
  - **Curiosity**
  - **Authority**
- Goal: make victims **share passwords, open malware, or perform harmful actions**.
- Also known as **"human hacking"**.

---

2. 🎣 Phishing (A Subset of Social Engineering)

- Phishing uses **messages** to trick targets into clicking, opening, or replying.
- Common delivery methods:
  - Email
  - SMS (smishing)
  - Voice calls (vishing)
  - QR codes (quishing)
  - Social media DMs
- Purpose: steal **credentials, money, or access**.

---

3. 🧠 Anti-Phishing Awareness – Two S.T.O.P. Mnemonics

🔍 S.T.O.P. #1 – Ask Yourself:

- **S**uspicious?
- **T**elling me to click?
- **O**ffering an amazing deal?

- **P**ushing urgency?

🛑 S.T.O.P. #2 – Safety Tips:

- **S**low down
- **T**ype the URL manually
- **O**pen nothing unexpected
- **P**rove the sender

---

4. 🕸️ Building the Trap (Fake Login Page)

- Attackers often craft a **fake login page** to steal credentials.
- Steps taken:
    - Run server.py to host fake page
    - Page listens on port **8000** and logs credentials

Victim visits a link like:
http://<IP>:8000

---

5. 📧 Delivering the Phishing Email with SET

- Use **Social-Engineer Toolkit (SET)** to send realistic-looking emails.
- Process:
    1. Launch tool: setoolkit
    2. Choose:
        - **1**: Social-Engineering Attacks
        - **5**: Mass Mailer Attack
        - **1**: Single email address
    3. Configure email details:
        - Fake sender name & email
        - SMTP server IP & port
        - Subject + message body
    4. Include link to fake login page
- Example subject:
  "Shipping Schedule Changes"
- Example body:
  Link to login: http://<IP>:8000

- SET sends the email to the target.

---

6. 📥 Monitoring for Captured Credentials

- Keep terminal running server.py
- Any credentials entered on the fake page will appear in the terminal

---

🧠 Key Learning Points

- Social engineering exploits **people**, not systems.
- Phishing is a major vector & increasingly convincing.
- Attackers rely on **psychology + technical setup**.
- Tools like SET help attackers **automate phishing campaigns**.
- Awareness training & slowing down helps prevent attacks.

🛡️ Defensive Takeaways

- Verify sender identity carefully.
- Never click unknown links.
- Always type URLs manually.
- Double-check emails that create urgency or fear.
- Organizations should **train staff regularly** and simulate attacks.

🚀 TL;DR

Day 2 focuses on **how phishing attacks are built, delivered, and detected**, and teaches both:

- Attack methodology
- Human defense strategies