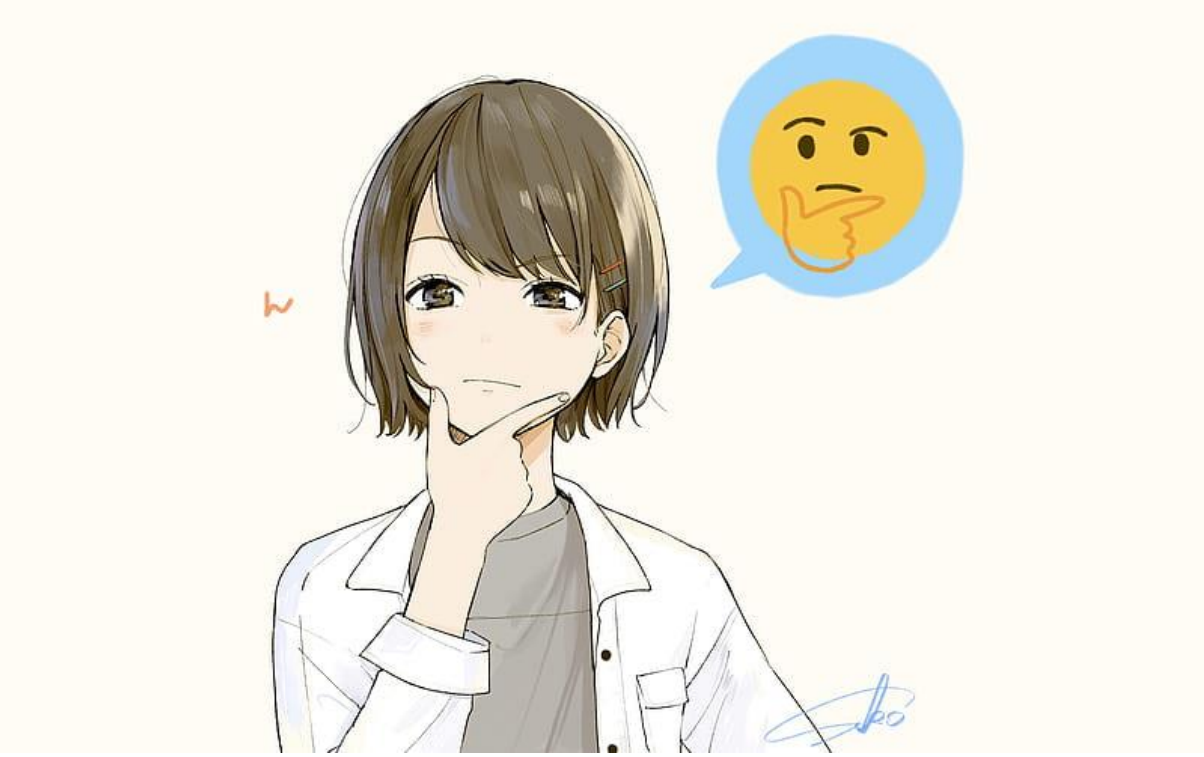
Asking Effective Questions Guide



Social Engineering and Phishing Workshop

👋 Introduction

In this workshop, you're learning how phishing attacks are created and tested using tools like **Evilginx** or by sending a **phishing email with a malicious attachment**. Sometimes, when things don't work as expected, it's easy to just say:

- "It doesn't work."
- "I followed the steps but it's not working."
- "I did everything correctly."

However, these statements don't help your trainer (or yourself!) figure out what's wrong. To troubleshoot effectively and learn faster, it's better to ask **specific questions** by clearly stating:

- What you were trying to do
- What you did (exactly)
- What you expected to happen
- What actually happened
- Any error messages or strange results

❌ Why "It doesn't work" is not helpful

Let's say you're running Evilginx and something goes wrong. Saying "It doesn't work" could mean many things:

- Evilginx didn't start?
- You couldn't access your phishing site?
- Credentials weren't captured?
- Target didn't click the link?

Each of these needs a different fix. That's why you need to break it down.

✅ A Better Way to Ask

Here's a simple format you can follow every time you get stuck:

---

1. What were you trying to do?

"I was trying to open the phishing link generated by Evilginx on the victim's browser."

---

2. What steps did you take?

“I ran the Evilginx setup commands, added the phishing site using phishlets, and shared the generated link via email.”

---

3. What did you expect to happen?

“When the link was opened, I expected Evilginx to capture the username and password.”

---

4. What actually happened?

“The phishing page showed a 404 error when clicked on the link.”

---

5. Did you receive any error messages?

“Yes, Evilginx says: Phishlet not loaded due to DNS mismatch.”

💡 **Sample Question Format**

Not helpful:
“The phishing link doesn’t work.”

Helpful:
“I used Evilginx to generate a link for Office365. When I opened the link on the victim VM, I got a 404 error. Evilginx logs mention a DNS mismatch. I think I might have misconfigured my domain settings. Could you help me check the DNS part?”

📩 **Example: Malicious Email Scenario**

You sent a phishing email with a zip file attachment that contains a payload, and the victim didn't get hacked.

Unhelpful:

“I clicked the file but nothing happened.”

Helpful:

“I crafted a phishing email with a zip file containing the payload created using msfvenom. I set the listener using Metasploit and shared the link to download it. The victim clicked the attachment, but no reverse shell came back. There were no logs on Metasploit, so I suspect the file was blocked or didn’t execute properly.”

🔍 Checklist Before Asking

Use this quick checklist:

- ✅ Did I follow each step one-by-one?
- ✅ Did I copy any error messages or logs?
- ✅ Did I try to describe what's actually happening?
- ✅ Did I test on the correct machine (attacker/victim)?
- ✅ Did I note down what works vs. what doesn't?

👊 Final Tips

- It's okay to make mistakes. What matters is how you describe them.
- Be honest: "I'm not sure what this part does" is better than staying silent.
- Screenshots help too! Show exactly what you see.

🧠 Remember

Learning offensive security or phishing doesn't require being a tech expert — it requires **curiosity** and **clear communication**. The better you explain your problem, the faster you'll find the solution — and the more you'll learn in the process.