1. EVIL-TWIN Wi-Fi ATTACK / ROGUE ACCESS POINT

Attackers set up a fake Wi-Fi network that looks identical to a trusted one, same name, same appearance, sometimes even stronger signal. When employees connect to it, attackers can capture their internet traffic, steal login credentials, inject malware, or redirect them to fake login pages.

WHAT IS AN EVIL-TWIN WI-FI ATTACK?

Attackers create a fake Wi-Fi network that looks identical to a real one. When employees connect, attackers capture all traffic and login attempts.

Scenario: Hassan Connects to “Café_WiFi-Free”

Hassan is working at a coffee shop.

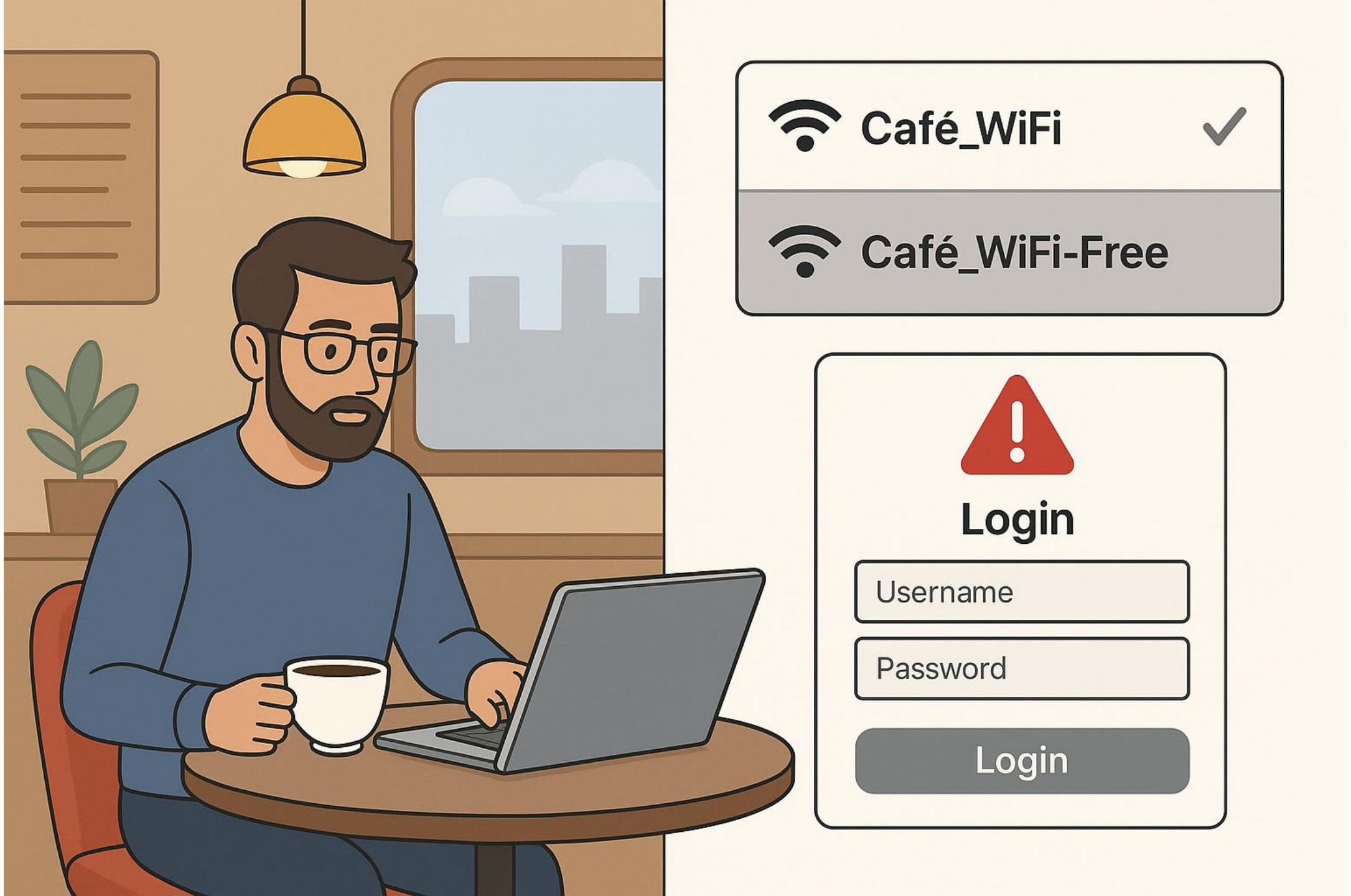
He sees two networks:

- Café_WiFi
- Café_WiFi-Free (Stronger Signal)

He chooses the second one.

After connecting, a “login” page appears, but it’s actually an attacker’s page, collecting usernames, passwords, and session data.

Lesson: Always verify the official Wi-Fi name with staff, and avoid connecting to networks just because they have a stronger signal.


Café_WiFi
Café_WiFi-Free
Login
Username
Password
Login

How Evil-Twin Wi-Fi Tricks Employees?

- Stronger signal than the real network
- Same or similar Wi-Fi name
- Fake captive portal that looks legitimate
- No password → easier to join

Red Flags Hassan Should Notice

- Two networks with nearly the same name
- Free network suddenly asking for login details
- Certificate warnings on websites
- Unusual pop-ups requesting credentials

Prevention Tips

- Avoid using public Wi-Fi for logins
- Use mobile hotspot when possible
- Confirm network name with staff before connecting
- Always use company VPN on public networks