# 6. QR CODE PHISHING

QR code phishing happens when attackers place malicious QR codes in public places, emails, or documents.
When scanned, these codes redirect users to fake login pages, malware downloads, or payment scam sites.
Because QR codes hide the actual URL, victims often don’t realize they’re being redirected to something unsafe.


QR CODE
PHISHING
Fake
login page
Malware
download
Payment
scams

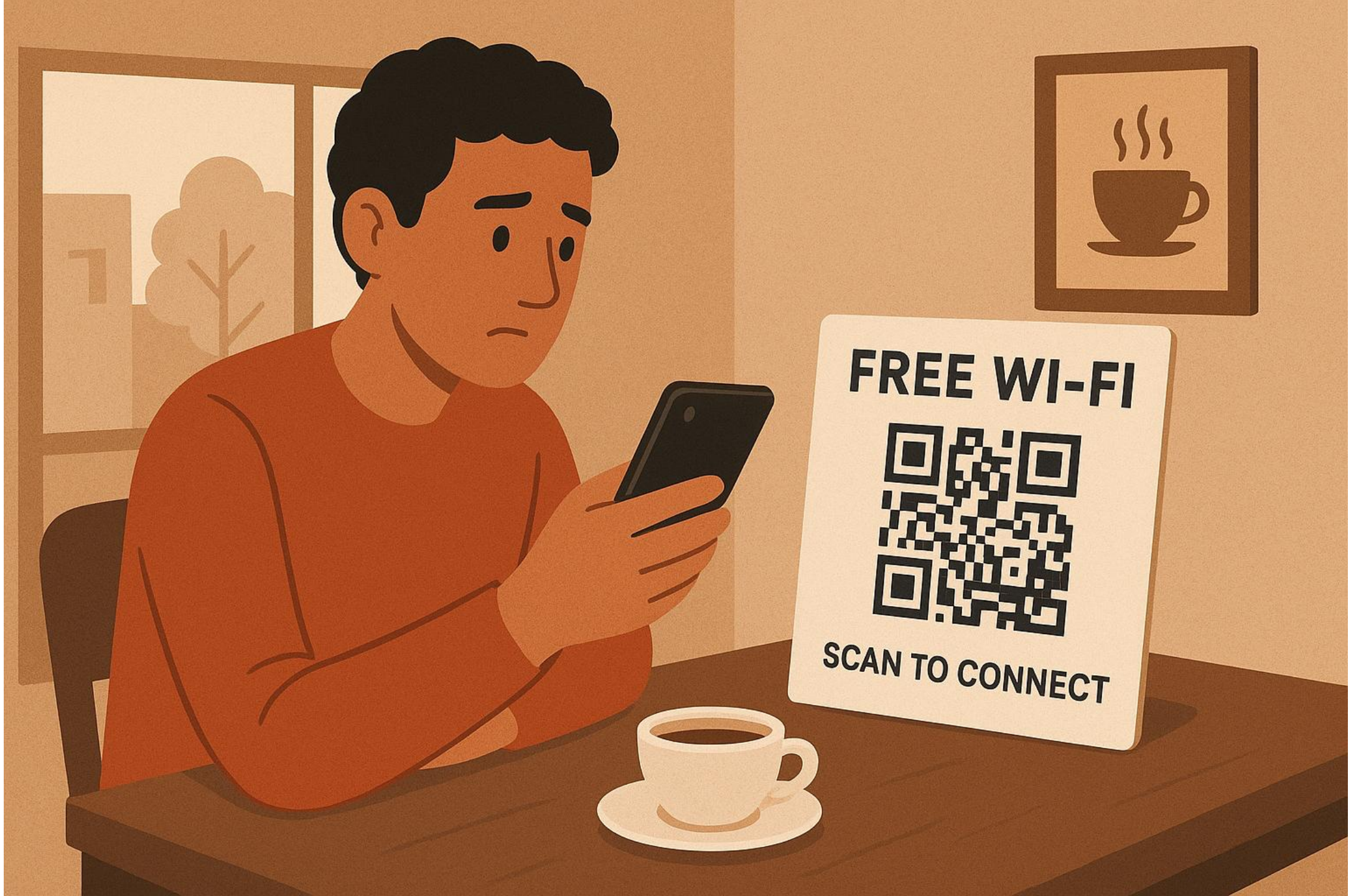
# Scenario: Hassan Scans a QR at a Coffee Shop

Hassan notices a QR code on the coffee shop table labeled, “Free WiFi !! Scan to connect.”

Trusting it, he scans the code with his phone, expecting to get WiFi access.

Instead, the QR code redirects him to a fake login portal that looks legitimate, and when he enters his credentials, the attacker captures them immediately.

Lesson: Be cautious when scanning QR codes in public places. Always verify the source before entering any personal information or login details.


FREE WI-FI
SCAN TO CONNECT

# Why QR Attacks Work?

- QR stickers can be replaced
- Employees trust physical signs
- Mobile screens hide full URLs

# How to Identify Malicious QRs?

- Check if QR sticker looks pasted
- Beware QRs in public places
- URL looks strange after scanning

# Prevention Tips

- Use secure QR scanning apps
- Always preview link before opening
- Never enter credentials after scanning random codes