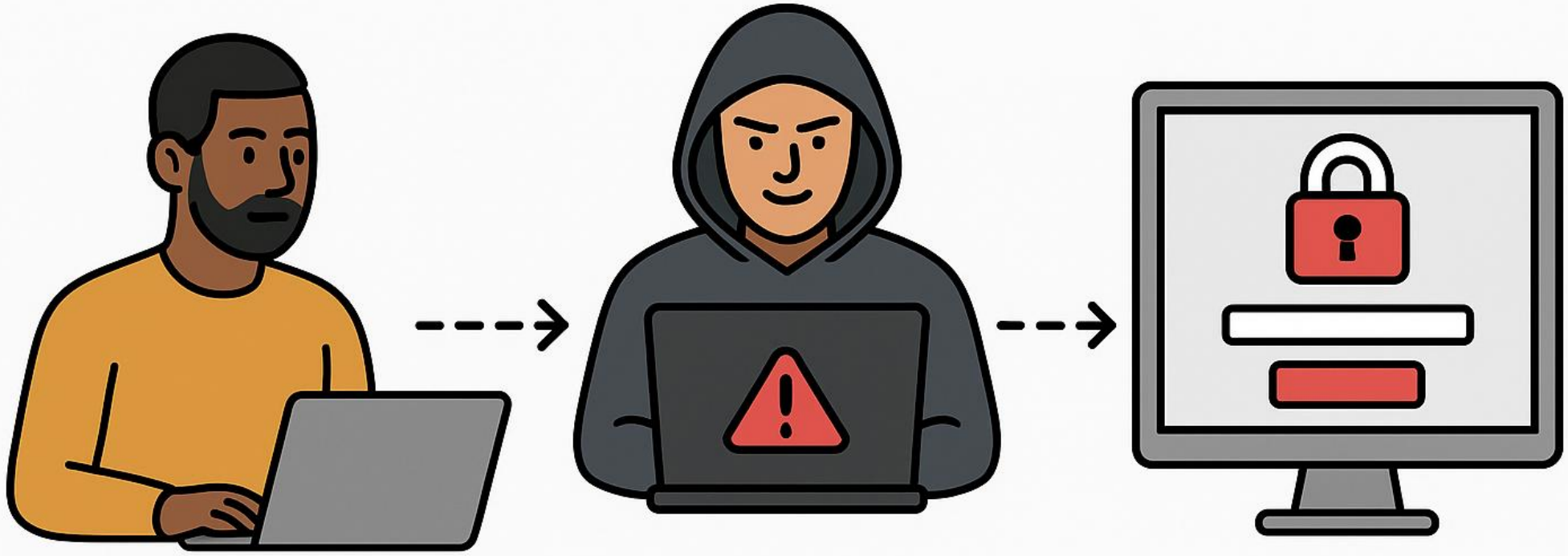
2. MAN-IN-THE-MIDDLE (MITM) PHISHING ATTACK

An attacker secretly positions themselves between the user and the real website or service. The user thinks they're communicating normally, but the attacker is intercepting everything. They can read data, modify what's being sent, or inject fake pages to steal passwords, banking details, or session tokens.

WHAT IS A MAN-IN-THE-MIDDLE ATTACK?

An attacker secretly places themselves between the user and the website. They intercept, modify, or inject fake pages to steal login credentials or sensitive data.



User Attacker Website

Scenario: Maryam Logs Into HR Portal at Home

Maryam opens the company HR portal from her home Wi-Fi.

Her router was previously compromised.

When she signs in, a fake password page appears right before the real website loads.

She enters her credentials, the attacker collects them instantly, and then forwards her to the real portal so nothing feels suspicious.

Lesson: If a login page looks unusual or appears twice, stop immediately.

Keep home routers updated and secured to prevent silent interception attacks.


HR PORTAL
Enter your credentials
Username
Password
Sign In

How MITM Tricks Employees?

- Attacker sits between Maryam ↔ the HR portal
- Intercepts all traffic quietly
- Injects fake “Please log in again” pages
- Redirects to the real site afterward to avoid suspicion

Red Flags Maryam Should Notice

- Browser shows certificate warnings
- Website takes unusually long to load
- Redirect loops or repeated login prompts
- Password suddenly required for routine pages

Prevention Tips

- Keep home router firmware updated
- Always check for HTTPS + valid certificate
- Use company VPN outside the office
- Report repeated login prompts immediately