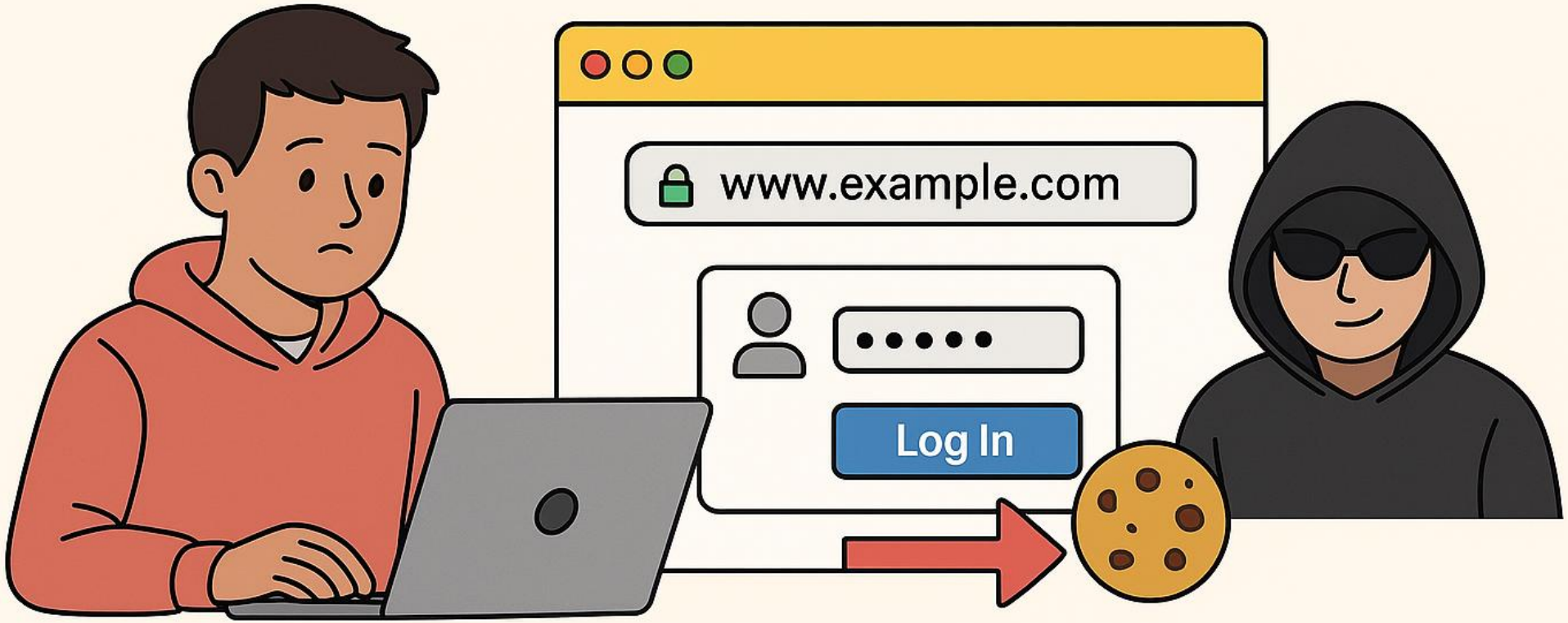
# 3. SESSION HIJACKING / COOKIE THEFT

Attackers steal your active login session instead of your password. By capturing or guessing your session cookie, they can enter your account without needing to log in. With just one stolen cookie, they can browse, send messages, or perform actions exactly as if they were you, often without triggering any alerts.

# What Is Session Hijacking?




Attackers steal your active login session instead of your password.

With one stolen cookie, they can access your account as if they were you.

# Scenario: Arham Checks Email on Public Wi-Fi

Arham logs into his company email using an open airport Wi-Fi.

The attacker captures his session cookie using a packet-sniffing tool.

Within seconds, the attacker logs into Arham’s email without needing the password.

Arham stays logged in the whole time, completely unaware.

Lesson: Never access sensitive accounts on open Wi-Fi.
Use a VPN or mobile hotspot to protect session data from being intercepted.

## Arham Checks Email on Public Wi-Fi

Arham logs into his company email using an open airport Wi-fi.


The attacker captures his session cookie using a packet-sniffing tool.

# How Session Hijacking Works?

- Attacker captures session cookies on open Wi-Fi
- Uses cookie to take over active login
- No password needed
- Attack happens silently in the background

# Signs Arham Should Notice

- Random logout from email
- “New login detected” security alerts
- Emails sent that he didn’t write
- Browser behaving unusually slow or glitchy

# Prevention Tips

- Never log into company accounts on open Wi-Fi
- Always use VPN to encrypt sessions
- Log out after sensitive work
- Enable MFA to limit session theft impact