9. OAUTH CONSENT PHISHING

Instead of stealing your password, attackers trick you into granting access to a malicious app.

You click “Allow” and the attacker gets:

- Email access
- Drive files
- Contacts
- Calendar

without ever needing your login.

What Is OAuth Consent Phishing?

Instead of stealing your password, attackers trick you into granting access to a malicious app.

Scenario: Hassan Approves a “PDF Viewer App”

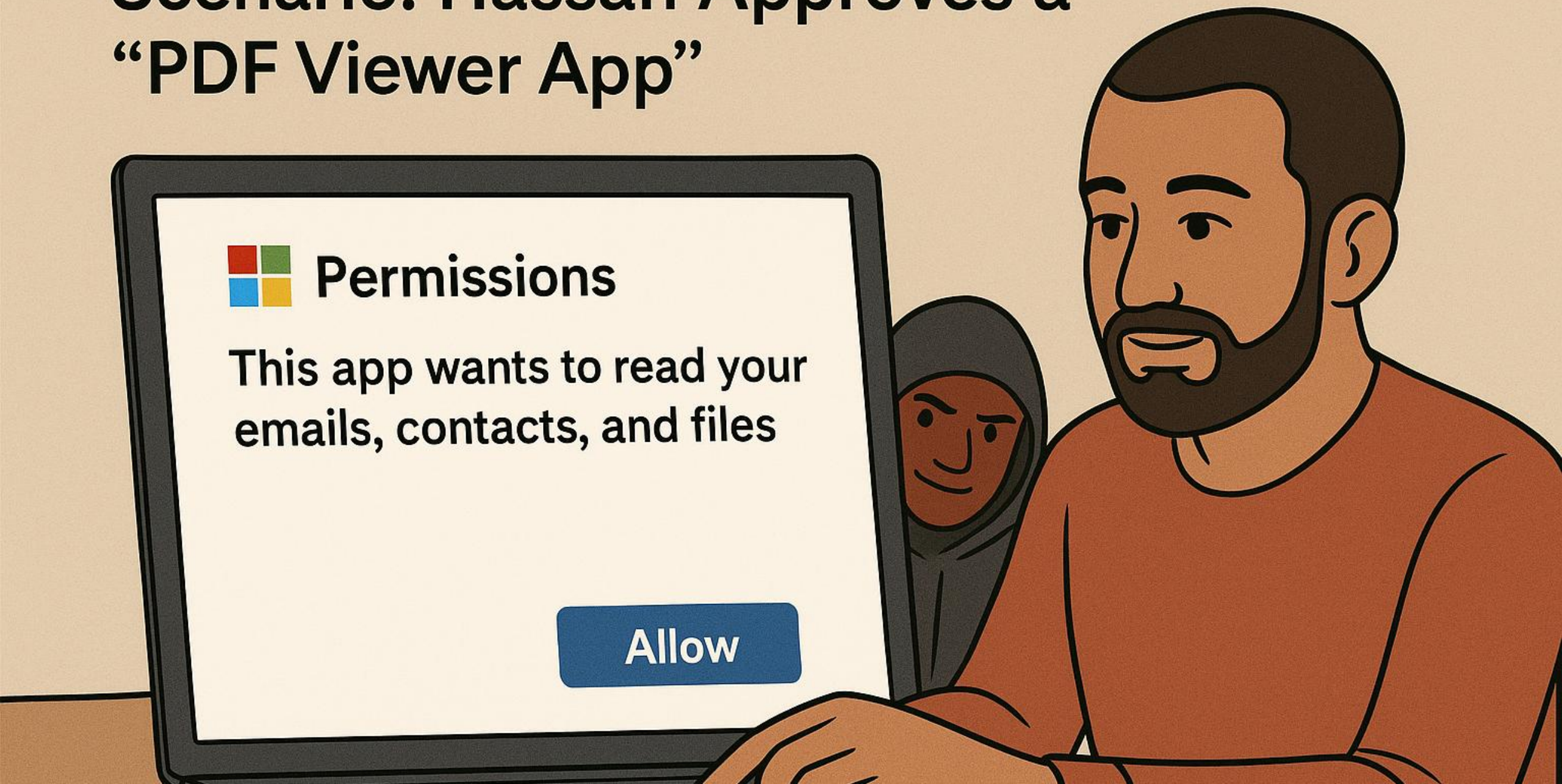
Hassan receives an email:
“Sign this urgent document. Open in Office PDF Viewer.”

When he clicks, he sees a real Microsoft permissions page:
This app wants to read your emails, contacts, and files.
He clicks Allow, thinking it's normal.

The attacker now reads his entire inbox.

Lesson: Always verify app permission requests and avoid granting access to unknown or unexpected applications.

Scenario: Hassan Approves a “PDF Viewer App”



How OAuth Attacks Work?

- Attackers register a fake app
- They send a link requesting permissions
- The page is real (Microsoft/Google)
- Employees approve automatically

Red Flags for OAuth Abuse

- Unknown apps
- Excessive permissions requested
- “This app is not verified” warning
- Request coming unexpectedly

Prevention Tips

- Never approve apps you don’t recognize
- Report unknown permission prompts
- Use admin-approved app policies
- Only sign documents via official portals