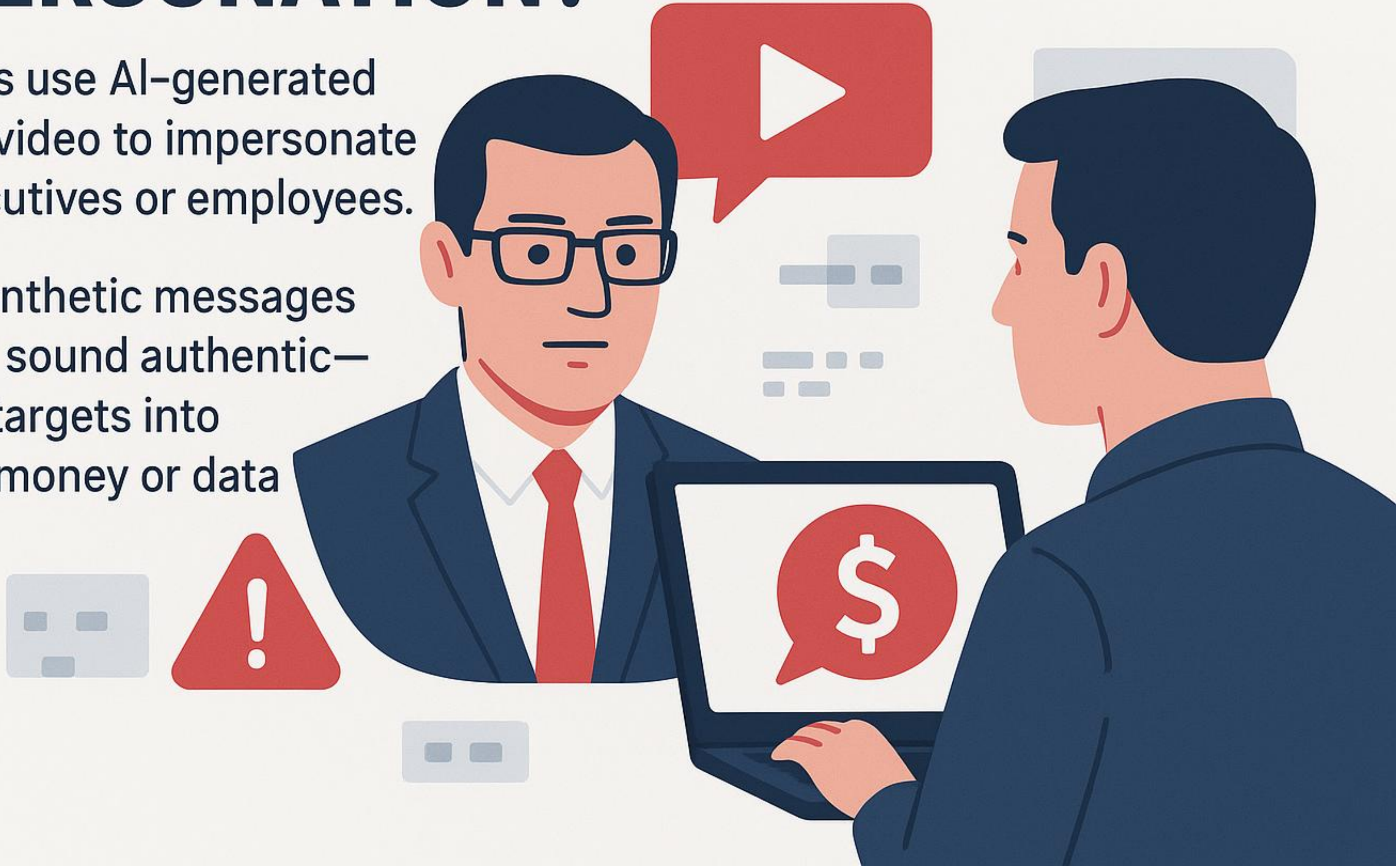
1. DEEPFAKE / SYNTHETIC MEDIA IMPERSONATION

Attackers use AI-generated voice or video to impersonate real executives, employees, or trusted contacts. These synthetic messages look, sound, and even behave like the real person, making them highly convincing. Targets can be tricked into transferring money, revealing sensitive information, or approving fraudulent requests.

WHAT IS DEEPFAKE IMPERSONATION?

Attackers use AI-generated voice or video to impersonate real executives or employees.

These synthetic messages look and sound authentic—tricking targets into sending money or data



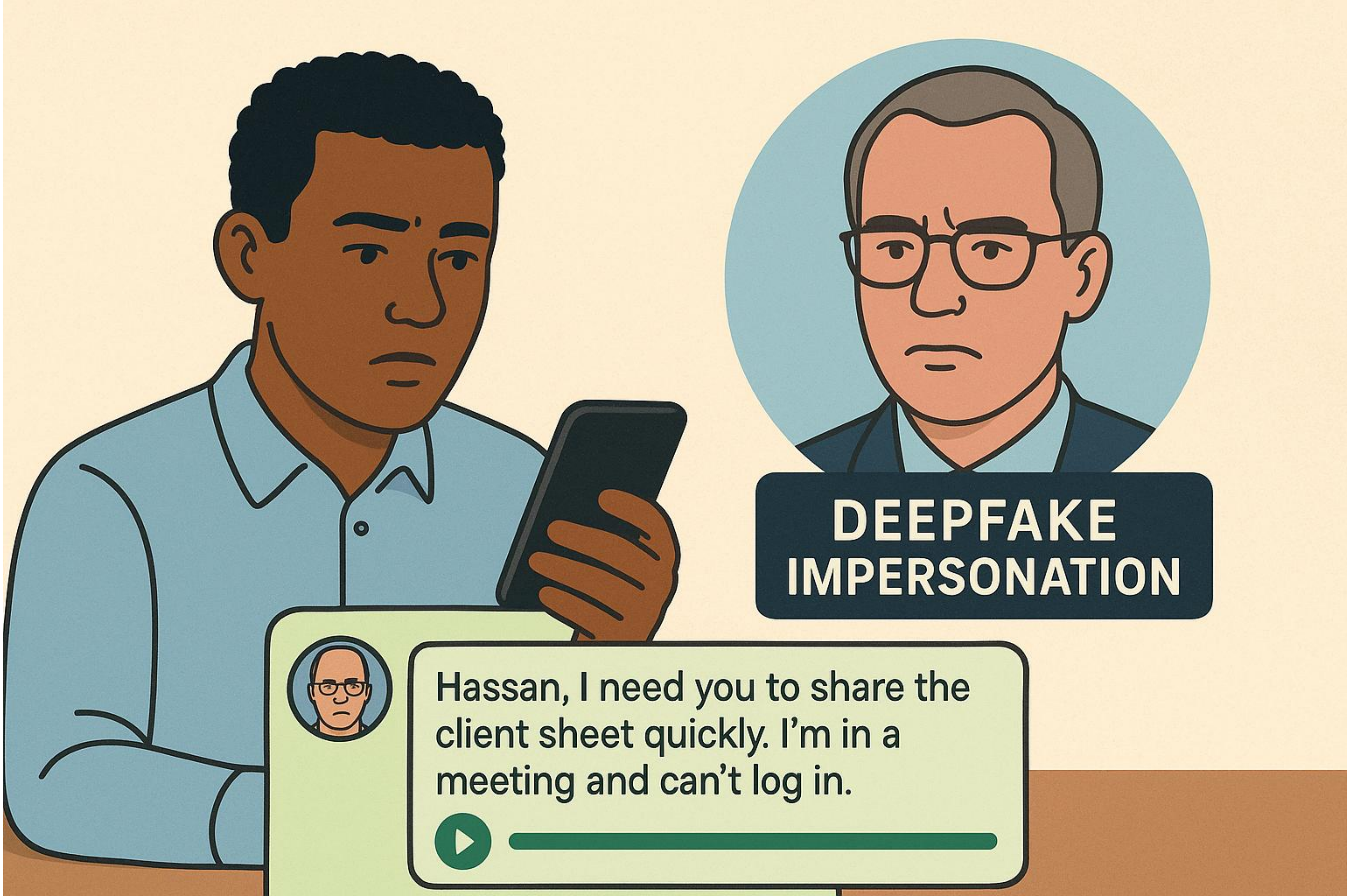
Scenario: Hassan Receives a “Voice Note” From His Manager

Hassan gets a WhatsApp voice message that sounds exactly like his manager:

“Hassan, I need you to share the client sheet quickly. I’m in a meeting and can’t log in.”

It’s a deepfake audio created by scammers using public audio clips of his manager.

Lesson: Always verify urgent requests through a separate channel, call or message the person directly.
Do not act solely on voice messages, even if they sound real.



Hassan, I need you to share the client sheet quickly. I’m in a meeting and can’t log in.

How Deepfakes Trick Employees?

- Voice timbre sounds identical
- Background noise added for realism
- Urgent tone to force quick action
- Uses publicly available audio/video of leaders

Red Flags Hassan Should Notice

- Unusual request outside normal process
- Manager never requests files via WhatsApp
- Pressure to “do it urgently” without verification
- Poor lip-sync or robotic tone (for videos)

Prevention Tips

- Always verify surprising requests via official channels
- Use known phone numbers, not message reply
- Report suspicious audio/video to security
- Never share internal data via personal apps