Solutions

Each answer shows the steps, then the **result**.

2.1

- AI writes in perfect, native-sounding language, removing the poor grammar that used to reveal a scam

2.2

- a shared secret question only the two parties know; the deepfake cannot answer it, exposing the fake

2.3

- some AI tools feed user input back into training, and an adversary could later extract that data

3.1 B

- a deepfake clones a voice or face

3.2 B

- a second factor blocks a voice-only attack

3.3

(a)

- an AI deepfake impersonation

(b)

- ask a prearranged shared-secret question that only the real CEO would know; or verify through a separate known channel

3.4

(a)

- it writes fluent, personalized messages in any language, so the spelling and grammar errors users look for are missing

(b)

- by publishing websites, or changing existing ones, so that they contain false information that is collected into training sets

(c)

- crafting prompts that trick the model into revealing data from earlier user input or from its training data

(d)

- verify it against reputable, stable sources that are not AI-based

3.5 A

- reconnaissance collects publicly available information about the target