

Exercise walk-through

AI-Based Cybersecurity Attacks ■ 1.4

eXercise

You must be able to

- explain how AI augments attacks (deepfakes, flawless phishing, data poisoning)
- describe defenses: a **shared secret** 共享秘密, MFA, verifying AI output

Method — How AI helps attackers

AI can clone a voice or face (a deepfake) to impersonate someone on a call, and can write phishing emails in perfect, native-sounding language - removing the bad grammar that once exposed scams.

Method — Defending against AI attacks

Agree a shared secret word with close contacts to verify identity, enable MFA so a cloned voice cannot log in, and never trust AI output without checking a reliable non-AI source.

Practice 2.1 ■ 2 marks

Explain how AI makes phishing emails harder to spot.

Solution 2.1

Method: How AI helps attackers

Worked steps

AI writes in perfect, native-sounding language **B1**, removing the poor grammar that used to reveal a scam **B1**.

Practice 2.2 ■ 2 marks

State one defense against a deepfake voice call and explain how it helps.

Solution 2.2

Method: How AI helps attackers

Worked steps

a shared secret question only the two parties know **B1**; the deepfake cannot answer it, exposing the fake **B1**.

Practice 2.3 ■ 2 marks

Why should you not type sensitive data into a chatbot?

Solution 2.3

Worked steps

some AI tools feed user input back into training **B1**, and an adversary could later extract that data **B1**.

Exam-style 3.1 ■ 1 mark

An AI clone of a person's voice, used to impersonate them, is called a

A honeypot

B deepfake

C keylogger

D baseline

Solution 3.1

Method: How AI helps attackers

A honeypot

B deepfake



C keylogger

D baseline

Worked steps

B. a deepfake clones a voice or face.

Exam-style 3.2 ■ 1 mark

Which defense best stops an adversary who has only cloned an employee's voice?

- A** a longer password
- B** multifactor authentication
- C** a brighter screen
- D** a faster network

Solution 3.2

Method: Defending against AI attacks

- A a longer password
- B multifactor authentication**
- C a brighter screen
- D a faster network



Worked steps

- B. a second factor blocks a voice-only attack.**

Exam-style 3.3 ■ 1 mark

An employee receives an urgent video call from the “CEO” asking to transfer money.

- (a) State what kind of attack this could be.
- (b) Describe one way the employee could verify the caller's identity.

Solution 3.3

Method: Defending against AI attacks

Worked steps

(a) an AI deepfake impersonation (B1). (b) ask a prearranged shared-secret question (B1) that only the real CEO would know (B1); or verify through a separate known channel.