# Module 1 Quiz: The Shift from Traditional to AI-Powered Threats

1. 1. You receive a voice message on your work phone from someone who sounds exactly like your department head, urgently requesting a wire transfer to a new vendor. They mention a meeting you're aware of and use your name. What’s the best next step?

* A) Approve the payment since they referenced a real meeting
* B) Reply by voice confirming you’ll handle it right away
* C) Call them back using the number in the voicemail
* D) Pause and verify the request using a known internal contact method

1. 2. An email lands in your inbox with your name, job title, and specific project details. It’s requesting a quick file upload for review. The writing is flawless, and the tone is professional. What’s the most security-aware move?

* A) Review the signature and reply if the name matches someone familiar
* B) Open the attachment or link since the details are clearly customized
* C) Reply asking, “Is this really you?” to confirm identity
* D) Cross-verify the request with the person through an independent channel

1. 3. You overhear someone mention “AI-as-a-Service” in a team security briefing. What does that term usually refer to?

* A) Companies using AI to improve software
* B) AI tools made for HR and hiring
* C) Criminals renting AI tools to run scams and attacks
* D) Your organization’s approved AI chatbot

1. 4. Which of the following might help you identify that a message is NOT truly AI-generated?

* A) It’s written in awkward English with spelling errors
* B) It includes company-specific project references
* C) It mimics an internal tone and references your manager
* D) It’s overly polite and uses complex sentence structures

1. 5. Why is AI considered a “threat multiplier” when combined with IoT and cloud technologies?

* A) It improves team collaboration across departments
* B) It creates more job opportunities in tech
* C) It expands potential attack surfaces through automation
* D) It helps smart devices run more efficiently

1. 6. Your coworker copies sensitive customer data into a free AI tool to generate a presentation summary. They say it’s “just internal.” What would be the right thing to do?

* A) Let it go—they’re trying to work more efficiently
* B) Ask them to clear it with IT before using such tools again
* C) Suggest using the same tool but with only anonymized data
* D) Report the behavior discreetly to your data/privacy lead

1. 7. An AI system is used to send thousands of phishing messages, each customized with real company names and employee roles. This is an example of:

* A) Traditional phishing
* B) Human error
* C) AI-driven personalization and scale
* D) A harmless marketing bot

1. 8. Your teammate receives a calendar invite from “Head of Legal” with a video message about an urgent compliance review. The video looks real, but the tone feels off. What should you advise?

* A) Proceed carefully—it’s likely a real initiative
* B) Reply to the invite and ask for more context
* C) Share the video internally and ask for opinions
* D) Verify the meeting request independently with Legal or a manager

1. 9. Why are traditional spam filters often ineffective against AI-generated phishing?

* A) AI content is too long to be scanned
* B) AI messages are poorly written and get ignored
* C) AI-generated emails mimic human tone and avoid obvious red flags
* D) Spam filters are no longer supported by most email providers

1. 10. What is the most important mindset shift employees must adopt to stay safe in the age of AI-driven threats?

* A) Let IT handle anything suspicious
* B) Assume anything familiar is safe
* C) Be fast in reacting to all messages
* D) Stay alert, slow down, and verify everything—even if it seems normal