# Module 2 Quiz: Emerging AI Threat Vectors

1. 1. You receive a highly personalized email about a recent company project. It references real timelines and team members and asks you to review a link. The tone is friendly, and the sender’s name matches someone you’ve worked with. What should you do?

* A) Click the link—it's clearly internal
* B) Respond and ask them to resend it from their work email
* C) Open it in a private browser to check first
* D) Verify the request using a separate internal channel

1. 2. You’re in HR, and a promising job candidate sends a video introduction. Their answers seem polished, but something about their facial expressions feels off. What’s the most secure next step?

* A) Ignore your instincts and continue the hiring process
* B) Forward the video to a colleague for a second opinion
* C) Request a live video call to verify identity
* D) Use face recognition software to confirm the applicant

1. 3. You get a WhatsApp message from a known supplier asking you to confirm a new invoice. It’s friendly, casual, and personalized—but it’s not their usual channel. What’s the best course of action?

* A) Ask them to switch back to email
* B) Confirm the invoice to keep things moving
* C) Verify the request through the contact listed in your system
* D) Screenshot the message and forward it to your team

1. 4. An internal chatbot asks you to log in again to “refresh credentials” and gives you a link that looks like your SSO portal. It’s integrated into your daily tools. What do you do?

* A) Enter your credentials since the chatbot is internal
* B) Check with IT if the chatbot has been updated
* C) Report it to security—this could be a chatbot spoof
* D) Ignore it unless it reappears again later

1. 5. A coworker shows you an AI-generated image they received with your company logo and a new product you’ve never heard of. The sender claims to be a marketing consultant. What’s your first move?

* A) Forward it to marketing to confirm if it's legit
* B) Respond asking who they were in contact with internally
* C) Delete it—it’s probably spam
* D) Report it to security—it could be a brand impersonation test

1. 6. A department head asks you (via email) to “review a sensitive video” regarding a compliance issue. The email includes a Dropbox link and is signed with their full title. What’s a red flag here?

* A) The use of Dropbox instead of internal systems
* B) The professional language in the message
* C) The absence of an actual issue description
* D) The full title in the email signature

1. 7. Your finance teammate receives a call from someone who sounds just like the CFO asking to verify a payment. It’s urgent and aligns with an open vendor file. What's the safest next step?

* A) Ask for the request to be emailed
* B) Confirm the payment since it matches a real invoice
* C) Notify the CFO’s office and confirm via internal call
* D) Delay the request and check with Accounts Payable later

1. 8. In a team call, someone shares an AI-written campaign brief that references your department’s confidential data—even though it hasn’t been shared externally yet. What does this suggest?

* A) The AI tool had insider access to company data
* B) Someone might have copied internal notes into a public AI tool
* C) The campaign is further along than you were told
* D) It's just coincidence—AI tools guess based on keywords

1. 9. A phishing email you received yesterday now shows up again—but this time it includes references to your LinkedIn profile. What does this indicate?

* A) It’s a coincidence—many emails reuse names
* B) Your account may have been cloned
* C) The attacker is using AI to personalize threats
* D) You mistakenly accepted a connection from the attacker

1. 10. What makes AI-powered social engineering more dangerous than traditional attacks?

* A) AI messages are easier to detect due to their volume
* B) AI lacks emotional nuance, so it’s less persuasive
* C) AI can scale deception with personalization in seconds
* D) AI-generated attacks mostly happen in forums