## Teacher Answer Key

### Case Study

1. The email was convincing because it mentioned Marcus's accountant by name, referenced a real ongoing project, and matched the accountant's writing style — information the AI likely gathered from Marcus's company website, LinkedIn profile, and public business filings.

2. Marcus used the 'independent contact rule' — he contacted Linda through her existing phone number rather than any contact information in the suspicious email. This was effective because even a perfectly convincing fake message cannot survive verification through a channel the scammer doesn't control.

### Multiple Choice

1. B

2. C

3. D

### Matching

1-D, 2-E, 3-A, 4-C, 5-B

### Fill-in-the-Blank

1) 10, 2) verification (or code/secret), 3) language

### Short Answer (Sample Responses)

Q1: Traditional phishing emails were generic and easy to identify through poor grammar and impersonal language. AI-powered scams use publicly available data to include accurate personal details — names, projects, relationships — making each message appear genuinely targeted at the recipient.

Q2: The independent contact rule works because it bypasses the fraudulent communication channel entirely. No matter how convincing a fake email or text appears, calling the real person through a number you already have will immediately expose the deception, as the real person will have no knowledge of the request.

Q3: Sample — Both share responsibility. Technology companies have engineering tools to detect and block AI fraud at scale, but individual judgment — pausing before wiring money, verifying unexpected requests — remains the final and most reliable line of defense because no automated system can perfectly filter every deceptive message in real time.