Teacher Answer Key

Case Study

1. The phishing email used urgency (48-hour deadline) combined with a high-stakes consequence (losing portal access before finals). It was particularly effective because finals were approaching, making the threat feel immediately real and costly — exactly the condition that makes people act without thinking.

2. Priya used two techniques: hovering over the link to check the actual URL (which revealed the fraudulent domain) and contacting the institution independently using a number from the official website. Without these steps, she would likely have clicked the link and entered her credentials on a fake login page.

Multiple Choice

1. A

2. B

3. D

Matching

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

Fill-in-the-Blank

1) filter, 2) hover, 3) passwords

Short Answer (Sample Responses)

Q1: Content analysis (checking grammar and formatting) fails because AI now produces flawless content that looks identical to legitimate communications. Process analysis focuses on whether the request follows normal institutional procedures — and legitimate organizations consistently follow predictable, safe procedures like directing users to official websites rather than links in emails.

Q2: Traditional phishing sent identical automated messages that felt impersonal. AI can respond to a victim's specific questions with convincing answers, creating the illusion of a real human interaction. This extended 'conversation' builds trust and gives victims a false sense that they've verified the legitimacy of the request.

Q3: Sample — First, do not click any link in the email. Second, hover over any links to check the actual destination URL against the bank's real domain. Third, open a browser independently and navigate to the bank's official website by typing the address directly. Fourth, log in there to check for any real alerts. Fifth, call the

bank's number from their official site — not any number in the email — to confirm whether there is actually an issue.