Teacher Answer Key

Case Study

1. The text matched his real situation (he had multiple orders), used a familiar delivery company name, and the fake site copied the company's logo and colors, making it feel legitimate.

2. The web address didn't match the company's official URL, and when he checked his real delivery app there was no problem listed—both clues that the message was a phishing attempt.

Multiple Choice

1. A

2. C

3. D

Matching

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

Fill-in-the-Blank

1) phishing, 2) spoofed, 3) chargeback

Short Answer (Sample Responses)

Q1: During the holidays, many people are expecting multiple packages and are worried about delays or lost gifts. Scammers exploit that anxiety by sending vague "problem with your delivery" messages that feel believable and urgent, pushing people to click without thinking.

Q2: A consumer can check the web address carefully (looking for spelling, extra words, or wrong endings), search for reviews or complaints about the site, verify that the charity appears on an official registry or watchdog site, and look for clear contact information and return or donation policies.

Q3: They should contact their card issuer immediately to report possible fraud and request that the card be blocked or replaced, and review recent transactions for any unauthorized charges. They can also monitor their accounts closely, change passwords for any related logins, and avoid clicking more links from the suspicious message.