Teacher Answer Key

Case Study

1. Priya showed phishing awareness by checking the sender's domain instead of trusting the message's look, and she reported rather than clicked. The utility's response — forced password resets and multi-factor authentication — closed the door a stolen credential would have opened.
2. Water systems are critical infrastructure: disrupting chemical dosing endangers public health, which gives attackers leverage. Small utilities are attractive precisely because they run on computers but rarely have large security staffs, as the Florida water incident showed.

Multiple Choice

1. A
2. B
3. C

Matching

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

Fill-in-the-Blank

1) hacking, 2) Pipeline, 3) private

Short Answer (Sample Responses)

Q1: After 9/11 the government hardened physical targets, but daily life — banking, health care, utilities — moved onto networks where attacks scale globally and cheaply. Officials came to rank cyber threats alongside terrorism because one intrusion can now disrupt physical life, as the Colonial Pipeline shutdown proved.
Q2: About 85 percent of critical infrastructure is privately owned, so the government cannot defend networks it does not control. Partnerships let companies report attacks they see while agencies like CISA return warnings, expertise, and shared standards — neither side has the full picture alone.

Q3: Answers will vary. Strong responses pick a habit (multi-factor authentication, unique passwords, phishing skepticism, prompt updates), explain the specific attack it blocks, and note that most breaches begin with one person's small mistake.