Past-paper walk-through

Cyber Foundations ▪ 2.1

eXercise

Questions in this set

- 2026 Q9 ▪ 1 mark
- 2026 Q17 ▪ 1 mark

Question 9

2026 ▪ Q9 ▪ 1 mark

Referring to the same phishing email, how does the claim that "Over 92% of employees have already completed the verification" attempt to pressure the recipient into responding? **[1]**

A By framing the request as routine HR communication that seems safe, showing the use of familiarity

B By implying that the opportunity to comply is limited and may soon be lost, showing the use of scarcity

C By presenting the request as coming from those in power and intimidating the recipient, showing the use of authority

Question 9

D By applying social pressure and making the recipient believe most coworkers have already acted, showing the use of consensus

Solution 9

A By framing the request as routine HR communication that seems safe, showing the use of familiarity

B By implying that the opportunity to comply is limited and may soon be lost, showing the use of scarcity

C By presenting the request as coming from those in power and intimidating the recipient, showing the use of authority

D By applying social pressure and making the recipient believe most coworkers have already acted, showing the use of consensus ✅

Answer: **D**

Question 17

2026 ▪ Q17 ▪ 1 mark

Refer to the news article about Fairgrove Community Bank, which stopped a cyber intrusion of its customer database. A network administrator said one submitted string included ' OR '1'='1';– and added, "This wasn't some advanced adversary. They were copying code from the internet and testing to see if anything would work." Which of the following best describes the adversary in this scenario? **[1]**

A Cyberterrorist

B Script kiddie

C State actor

D Insider

Question 17

Questions 17 through 20 refer to the following.

Consider the following article.

Small Town Bank Disrupts Attempted Cyber Attack on Customer Database

Fairgrove Community Bank, a local financial institution serving residents of central Kentucky, reported that it successfully stopped a cyber intrusion attempt earlier this week aimed at its customer database.

The attack was detected on Tuesday afternoon when automated security systems flagged unusual database queries originating from the bank's online loan application form. Investigators determined that the form was being used to input malicious code.

"One of the strings the adversary submitted included `' OR '1'='1';--`," said James Holloway, a network administrator at Fairgrove Community Bank. "'That's a common trick pulled from online tutorials."

Holloway said the attacker did not succeed in accessing any customer data, but the attempt revealed a flaw in the bank's web application.

Fairgrove Community Bank's security team has since patched the vulnerability. No data was compromised, and banking operations continued without interruption.

"'This wasn't some advanced adversary," Holloway added. "'They were copying code from the internet and testing to see if anything would work. But even simple attacks like this can work if we don't implement

Question 17

work. But even simple attacks like this can work if we don't implement best practices."

Fairgrove Community Bank says it is conducting a full audit of its customer-facing applications to ensure proper protections are in place.

Solution 17

A Cyberterrorist

B Script kiddie ✓

C State actor

D Insider

Answer: **B**