Knowledge Check: Module 1 Foundations

Component: Interactive Quiz
Goal: To formally assess students' foundational knowledge from Lesson 1.1 and Lesson 1.2 and reinforce key concepts through a formative assessment.

Part A: Quiz Content and Question Design

1. (SE Definition) According to Lesson 1.1, which of the following is the most accurate definition of social engineering?

A. The use of complex code to bypass a digital firewall.
B. The practice of analyzing social media to improve network security.
C. The art of manipulating people into giving up confidential information by exploiting psychological tricks.
D. The process of building better, more secure computer hardware.

2. (Key Distinction) What is the primary way social engineering differs from a traditional technical hack?

A. Social engineering is only used for pranks, while technical hacking is for serious crimes.
B. Social engineering targets the human user to bypass security, while technical hacking targets vulnerabilities in software or systems.
C. Social engineering requires advanced programming skills, while technical hacking does not.
D. Social engineering can only be done over the phone, not through email.

3. (Psychological Bias) You receive an email with the subject line "URGENT: Your Student Portal Password Will Expire in 24 Hours!" The email appears to be from the "Registrar's Office" and demands you click a link immediately. This attack primarily uses which two principles?

A. Liking and Social Proof
B. Scarcity and Liking
C. Authority and Urgency
D. Scarcity and Authority

4. (Common Motivation) Based on the examples in the lessons (Bitcoin scam, GCash requests), what is a common motivation for social engineers?

A. To test a company's firewall for weaknesses.
B. To make new friends and connections online.
C. To gain access to information or resources for personal or financial benefit.
D. To help users become more skeptical and informed.

5. (Concept Identification) True or False: The lessons state that a strong firewall and antivirus software are enough to stop all social engineering attacks.

A. True
B. False

6. (Psychological Bias) A pop-up ad for a mobile game says: "🔥 FREE 1000 GEMS! 🔥 Limited to the first 500 players! Claim yours before they're gone!" This tactic relies on the principle of:

A. Authority
B. Liking
C. Scarcity
D. Social Proof

7. (Psychological Bias) You get a message on Messenger from a classmate that says, "Hey, urgent! My GCash is down, please send ₱500 to this number. I'll pay you back tomorrow!" This scam primarily exploits which psychological principle?

A. Authority
B. Scarcity
C. Liking
D. Social Proof

8. (Concept Identification) The lessons refer to social engineering as "human hacking" because it:

A. Requires the hacker to be physically present.
B. Can only be done by very friendly and popular people.
C. Targets people's natural tendencies and psychology instead of computer code.
D. Is a legal method for testing security.

9. (Key Distinction) Which of these scenarios describes a social engineering attack, as explained in the module?

A. A hacker discovers a flaw in a website's code that allows them to access a database.
B. A scammer calls an employee, pretends to be from the IT department, and convinces them to reveal their password.
C. A programmer writes a script that automatically tries thousands of different passwords on a login page.
D. A network administrator installs a new firewall to block malicious traffic.

10. (Psychological Bias) A scammer creates a fake social media post for a giveaway, using bots to add thousands of likes and comments that say "It works! I got my prize!" to convince real users to participate. This is a clear example of an attacker using:

A. Authority
B. Social Proof
C. Urgency
D. Liking

Part B: Automated Feedback and Concluding Message

Feedback for Each Question:

1. Correct (C): "Correct! Lesson 1.1 defines social engineering as 'human hacking' that uses psychological tricks to manipulate people."
   Incorrect (A, B, D): "Not quite. Remember from Lesson 1.1, social engineering targets people and their psychology, not the technology itself."

2. Correct (B): "Exactly! The core idea is that social engineers bypass technology by targeting the person. It's like being convinced to hand over the key to your own house."
   Incorrect (A, C, D): "Incorrect. The key difference discussed in Lesson 1.1 is the target: people vs. systems."

3. Correct (C): "That's right! This attack uses Authority (pretending to be the Registrar) and Urgency (the 24-hour deadline) to make you act without thinking, just like the example

in Lesson 1.2."
Incorrect (A, B, D): "Good try, but the main tactics here are impersonating someone in power and creating a fake deadline. Review the principles of Authority and Urgency in Lesson 1.2."

4. Correct (C): "Correct. The examples consistently show that attackers are trying to get something valuable, whether it's money, account access, or personal information."
   Incorrect (A, B, D): "Incorrect. While attackers may use friendly language, their underlying motivation is typically selfish and malicious, aiming for some form of gain."

5. Correct (B): "Correct, this is false. Lesson 1.1 emphasizes that social engineering's main strength is its ability to bypass technical defenses by targeting the user directly."
   Incorrect (A): "Incorrect. A key theme of Module 1 is that technical tools are not enough. Your skeptical and informed mindset is the best defense."

6. Correct (C): "Perfect! By claiming the offer is 'limited to the first 500 players,' the scam creates a sense of Scarcity to pressure you into acting quickly."
   Incorrect (A, B, D): "Not this time. The feeling of 'I might miss out on a limited deal' is a direct appeal to the principle of Scarcity, as covered in Lesson 1.2."

7. Correct (C): "That's it! Because the message appears to be from someone you know and trust (a classmate), it is exploiting the principle of Liking to lower your guard."
   Incorrect (A, B, D): "Not quite. The primary trick here is using a trusted relationship. You're more likely to help a friend, which is why the Liking principle is so effective for scammers."

8. Correct (C): "Yes! This is the central concept from Lesson 1.1. It's called 'human hacking' because it exploits our brains 'shortcuts' and natural tendencies."
   Incorrect (A, B, D): "Incorrect. The term 'human hacking' refers to targeting human psychology, not physical presence or the hacker's personality."

9. Correct (B): "Correct! This is a classic example of social engineering where the attacker uses deception and impersonation to manipulate a person into compromising security."
   Incorrect (A, C, D): "Incorrect. Options A and C are technical hacks, and D is a defensive security measure. Only B involves manipulating a person."

10. Correct (B): "Exactly! This tactic uses Social Proof to make the scam seem legitimate because 'everyone else is doing it' and appears to be winning."
    Incorrect (A, C, D): "Good try, but the main factor here is the influence of the crowd (the fake likes and comments). This is a perfect example of the Social Proof principle from Lesson 1.2."

Final Message:

"Congratulations on completing the Module 1 Knowledge Check! You've successfully learned what social engineering is and the psychological principles that make it work. This knowledge is your most powerful tool in building a mental firewall.

Up next, we'll explore specific types of real-world attacks. See you in Module 2!"