CSH6 CH 19 REVIEW QUESTIONS

1. Can audit controls detect social-engineering attacks in progress?
2. Which of the following illustrate(s) (a) classic error(s) that allow(s) social engineers to acquire confidential information surreptitiously?
3. Fundamental security training to resist social engineering should include which of the following principles?
4. Smaller organizations tend to show which characteristic among those listed?
5. What is _piggybacking_ or _tailgating_?
6. Who was Frank Abagnale?
7. How should an organization plan to respond to notification of social engineering attacks?
8. How can one reasonably protect against theft of confidential documents?
9. What can the organization do to ensure that employees can cope with a social engineer who tries to intimidate an employee by pretending to be an angry high-placed executive irritated by the published security policies?
10. When should the investigation team interview employees who have reported a potential social-engineering attack?
11. Billy Bob, a dumpy 32-year-old, offers happily married 65-year-old Martha a case of valuable French wine if Martha will simply supply him with the personnel files for the top executives, supposedly because he is a recruiter and will give her a percentage of his placement fees if any of the executives accept offers from Billy Bob's clients. Actually he's planning to use the information to bully HelpDesk agents into revealing a key password on the company's network. Billy Bob is using _____?
12. How does DLP support barriers to social engineering?
13. Larger organizations tend to show which characteristic among those listed?
14. Salim receives an urgent instant message apparently from his boss telling him that his corporate userID and password may have been hacked and that he has to log into a specific Website < http://dkfr.394kd40.lv > he's never heard of to enter his current credentials and get the problem fixed. This is an example of scam involving _____?
15. Social engineers often rummage through discarded papers and other materials in the garbage containers outside their targets' buildings. What is this technique informally called?
16. The _knight-in-shining-armor attack_ involves _____?
17. Which of the following is/are (an) aspects of the psychology of the victim of social engineering?
18. A pleasant, friendly social engineer exploits which fundamental cognitive error?
19. A criminal sends a victim an email message claiming to be from the Internal Revenue Service (with impressive logo) and asking the target to provide a userID and password for their own bank account _under penalty of law_. The HTML email shows a link that appears to be for fbi.gov, but inspection shows it's actually < http://394275.34834234723.ru/3957;?gb=0348217 >. What kind of attack is this?
20. How can a social engineer use the Internet Archives in pursuit of his or her evil intentions?
21. Which of the following illustrate(s) (a) classic error(s) that allow(s) social engineers to acquire confidential information surreptitiously?
22. When someone uses coercion or deceit to obtain information or resources from other people, we say they are using _____?
23. Why is a Trojan Horse called that?

24. What is the technique in which criminals or agents form a bond of apparent friendship with a target who can provide insider information and progress to a sexual relationship as they strengthen (false) trust?

25. Which of the following technical defenses can best reduce the success of social-engineering attacks?

26. What kind of encryption can support better resistance to social engineering?

27. What is/are (an) ATE activity/activities that can be helpful in preparing a workforce to oppose social-engineering attacks?

28. What is the term applied to the way social engineers typically wear uniforms, carry badges, learn insider vocabulary, and assume a confident air of entitlement as they pretend to belong to an organization or have positional authority?

29. Which of the following is/are (a) notoriously successful social engineer(s)?

30. What can the organization do to ensure that employees can cope with a social engineer who tries to intimidate an employee by pretending to be an angry high-placed executive irritated by the published security policies?

31. What is the informal professional consensus about social engineering attack rates and success rates?