Module 2 Exam

1. **The process of providing proof that the user is “genuine” or authentic is known as\_\_\_\_\_\_\_\_\_.**
2. identification
3. genuinization
4. authentication
5. registration
6. **Which of the following is NOT a characteristic of a weak password?**
7. Personal information in a password
8. A password with fewer than six characters

C. A password that uses both letters and numbers

D. A common dictionary word

1. **Relying on deceiving someone to obtain secure information is known as\_\_\_\_\_.**

A. social engineering

B. magic attack

C. brute force attack

D. sleight attack

1. **The goal of a phishing attack is\_\_\_\_\_.**
2. to capture keystrokes
3. to send a fraudulent email to a user

C. to trick a user into surrendering personal information

D. to duplicate a legitimate service

1. **Each of the following may be performed by an identity thief except:**

A. Produce counterfeit checks or debit cards and then remove all money from the bank account.

B. File for bankruptcy under the person’s name to avoid paying debts they have incurred or to avoid eviction.

C. Open a bank account in the person’s name and write bad checks on that account.

D. Send malware into a bank’s online accounting system.

1. **Each of the following is a step to deter identity theft except:**
2. Keep personal information in a secure location.
3. Carry a copy of a Social Security card in a wallet instead of the original.

C. Shred financial documents that contains personal information.

D. Do not provide personal information either over the phone or through an email message.

1. **Passwords are based on which means of authentication?**

A. What you have

B. What you do

C. What you know

D. What you are

1. **A(n) \_\_\_\_\_ is a unique name for identification.**
2. password
3. value
4. authentication
5. username
6. **Each of the following is a characteristic of a strong password except:**
7. It must be lengthy.
8. It must be easy to memorize.
9. It must be complex.
10. It must not be repeated on multiple accounts.
11. **Which technique do attackers use today to uncover a password?**
12. Online guessing
13. Offline cracking
14. Hash regeneration
15. Digest reproduction
16. **Which of these password attacks is the most thorough?**
17. Dictionary attack
18. Short crack attack
19. Brute force attack
20. Grill attack
21. **Observing someone entering a keypad code from a distance is known as \_\_\_\_\_\_\_.**
22. piggybacking
23. spoofing
24. shoulder surfing
25. cyber watching
26. **What is a vishing attack?**
27. An attack that uses a phone instead of email or a website
28. An attack that only targets “big fish”
29. A social engineering attack that uses text messages
30. An password attack designed to crack long passwords
31. **A user who enters *americanbank.net* into a web browser instead of the correct *americanbank.com* and is then taken to a fake look-alike site is the victim of \_\_\_\_\_.**
32. site redirection naming attack (SRNA)
33. URL targeting
34. typo squatting
35. jacket attacking
36. **How can an attacker use a hoax?**
37. By sending out a hoax, an attacker can convince a user to read his email more often.
38. A hoax could convince a user that malware is circulating and that he should change his security settings.
39. A user who receives multiple hoaxes could contact his supervisor for help.
40. Hoaxes are not used by attackers today.
41. **Michelle pretends to be a manager from another city and calls Eric to trick him into giving her his password. What social-engineering attack has Michelle performed?**
42. pretexting
43. aliasing
44. character spoofing
45. duplicity