1. **An example of a(n) \_\_C\_\_\_ is a software defect in an operating system that allows an unauthorized user to gain access to a computer without a password.**
2. asset exploit (AE)
3. threat agent
4. vulnerability
5. threat
6. **\_\_\_C\_\_ requires banks and financial institutions to alert customers of their policies and practices in disclosing customer information and to protect all electronic and paper containing personally identifiable financial information.**
7. California Savings and Loan Security Act (CS&LSA)
8. Sarbanes-Oxley Act (Sarbox)
9. Gramm-Leach-Bliley Act (GLBA)
10. USA Patriot Act
11. **\_A\_\_\_\_ ensures that the information is correct and no unauthorized person or malicious software has altered that data.**
12. integrity
13. obscurity
14. layering
15. confidentiality
16. **Protecting information is accomplished by A**
17. protecting the devices on which the information is found
18. securing only local servers
19. hiring an Information Security Officer (CISO)
20. reducing risk factors
21. **Why are long passwords stronger than short passwords? B**
22. Long passwords are confusing to attackers who cannot read them.
23. Long passwords require attackers to make many more attempts to uncover the password.
24. Long passwords always use letters, number, and special characters so they are more puzzling to attackers
25. Short passwords take up less storage space which makes them easier to break.
26. **Each of the following is a password manager except: D**
27. password management application
28. password generator
29. online vault
30. hashing repository
31. **Each of the following is typically found in an email used for a phishing attack except: D**
32. Official logos of the actual site.
33. Web links that are close variations of a legitimate address.
34. An urgent request to take immediate action.
35. The telephone number of the actual site.
36. **Each of the following could be performed in a shoulder surfing attack except: A**
37. Watching the victim insert her plastic card into an ATM
38. Observing a person entering a password on a computer keyboard
39. Viewing a person writing down his Social Security number on a paper form
40. Watching a person enter a PIN at a register in a store
41. **Which type of firewall is an external hardware device? C**
42. personal firewall
43. remote firewall
44. network firewall
45. application resource firewall
46. **The database that contains the sequence of characters of a virus is called the \_\_\_D\_\_.**
47. string file
48. malware DB
49. virus resource file
50. signature file
51. **Each of the following is a question that the user should ask regarding data backups except \_B\_\_\_\_.**
52. What content should be backed up?
53. Who should do the backup?
54. Where should the backup be stored?
55. How frequently should be backup be performed?
56. **A \_\_B\_\_\_ is a downloadable image that can be used to scan a computer for malware.**
57. system repair disc
58. rescue disc
59. resource disc
60. clean disc
61. **The most secure option when configuring a web browser for security is \_\_\_\_\_D\_\_\_\_\_.**

A. Accept first-party cookies.

B. Accept first-party cookies but deny third-party cookies.

C. Reject locally shared objects but accept second-party cookies.

D. Deny first-party and third-party cookies.

1. **Which of the following is not a web browser addition to enhance security? C**

A. website reputation

B. local intranet flash signal

C. URL expander

D. plug-in validation

1. **Why would you want to block external content from downloading into your email client? A**

A. To prevent spammers from knowing that your email address is valid

B. To take advantage of the remote reading pane

C. To slow down your email client so you can read the message

D. To prevent your computer’s graphics processor utility buffer from filling too quickly

1. **Which of the following is not a secure Internet practice? D**
2. Restrict cookies in web browsers through browser settings.
3. Double-check spelling on a typed web address before submitting.
4. Do not click on embedded hyperlinks in an email.
5. Run JavaScript code to prevent attacks.
6. **Each of the following is a sound security practice when using a public Wi-Fi network except\_\_B\_\_\_.**

A. watching out for an evil twin

B. using the network for less than one hour per day

C. using a virtual private network (VPN)

D. not using a public network when entering confidential information on a website

1. **Which of the following is not a step to reduce the risk of theft or loss of a mobile device? A**

A. recording the MAC address of the device before using it

B. keeping the mobile device out of sight when traveling in a high-risk area

C. using both hands to hold a device, making it more difficult for a thief to snatch

D. not using the device on escalators or near transit train doors

1. **\_\_A\_\_\_ protects a mobile device when it has not been used for a set period of time.**

A. Auto-lock

B. Screen refresh

C. Manager tie down (MTD)

D. Remote security

1. **Which of the following is *not* a best practice for using a mobile device? C**
2. Back up data stored on the mobile device on a regular basis.
3. Do not jailbreak a mobile device.
4. Wait 24 hours before reporting a lost device.
5. Be aware of current threats affecting mobile devices.
6. **What is the most important advantage of hardware encryption over software encryption? C**
7. Software encryption cannot be used on older computers.
8. Hardware encryption is up to ten times faster than software encryption.
9. Software that performs encryption can be subject to attacks.
10. There are no advantages of hardware encryption over software encryption.
11. **Which of the following appears in the web browser when you are connected to a secure website that is using a digital certificate? C**
12. *http://*
13. wrench
14. padlock
15. a yellow warning message
16. **Which of the following is NOT a privacy best practice? D**
17. Use the private browsing option in your web browser.
18. Shred financial documents and paperwork that contains personal information before discarding it.
19. Use strong passwords on all accounts that contain personal information.
20. Carry your Social Security number with you so that it cannot be stolen you are not home.
21. **Each of these is a responsibility of an organization regarding user private data EXCEPT: C**
22. Collect only necessary personal information.
23. Use industry-tested and accepted methods.
24. Keep personal information for no longer than 365 days.
25. Do not use personal information when it is not necessary