



2021 DAS/EIS Information Security Training – Foundations Assessment

1. Which of the following actions could make our sensitive information vulnerable to cybercrime?
 - a. Connecting to secure wireless connections
 - b. Opening e-mail attachments from unknown source
 - c. Refraining from posting information about our organization on your personal social networking sites
 - d. Keeping security software up-to-date
2. Which of the following actions could result in loss or theft of personal information?
 - a. Carrying your laptop on your person at all times when traveling
 - b. Keeping track of your USB drive at all times
 - c. Loaning an unauthorized person, such as a messenger or visitor, your security badge to our building
 - d. Discussing sensitive information only in a private setting so passersby cannot overhear the conversation
3. Which could be a warning sign of social engineering?
 - a. Ambiguous messages requiring clarification
 - b. Any communication from individuals outside our organization
 - c. Unsolicited message appealing to your fear, sympathy, or trust
 - d. Customers, clients, or business partners with foreign accents
4. Which of the following forms of communication can experience social engineering?
 - a. Any form of communication
 - b. Telephone
 - c. Electronic Messages
 - d. In person
5. Verify the source of any electronic communication that contains a hyperlink. This includes communication via:
 - a. E-mail.
 - b. Instant messenger.
 - c. Texting and social networking.
 - d. All of the above.
6. Once you have posted information to the Internet, you can always retrieve or delete it.
 - a. True
 - b. False
7. Look out for which security threat specifically when using a cloud-based service?
 - a. Expired passwords
 - b. Out of date security software.

- c. Using only the cloud-based storage to save your files.
 - d. Phishing attempts from people impersonating a third party.
8. Which should be a security consideration before sending sensitive information using a cloud-based service?
- a. Has the information been fact-checked?
 - b. Is the information subject to compliance requirements?
 - c. Do you have prior experience working with the recipient?
 - d. Is the recipient in a different time-zone?
9. If you fall victim to hacking, the only step you need to take to regain access to your account—and prevent another attack—is to alert the IT department.
- a. True
 - b. False
10. Which of the following steps should you take to prevent hackers from gaining access to your accounts?
- a. Use a reputable antivirus software and keep it up-to-date.
 - b. Use a secure password and change it frequently.
 - c. Use different passwords for each of your accounts.
 - d. All of the above.
11. Which of these activities is recommended when working at home?
- a. Using a cross-cut shredder to dispose of documents.
 - b. Inserting personal peripheral devices into your work computer.
 - c. Allowing family members to use your work devices.
 - d. Connecting "smart" devices to your home network.
12. Using a VPN to connect to our organization's network is recommended when working from home.
- a. True
 - b. False
13. You should use your professional username and password as credentials for a personal account.
- a. True
 - b. False
14. Which is the best definition of "data minimization"?
- a. Collecting, accessing, and retaining the least amount of information necessary.
 - b. Compressing data so that it fits more efficiently into network storage.
 - c. Editing out unnecessary elements of our policies.
 - d. Possessing too little information to get the job done.
15. Which best describes the concept of "data minimization"?
- a. Big data requires big risks.

- b. Small quantities of data, large levels of efficiency.
 - c. The less data we handle, the less risk we create.
 - d. Minimized data, maximized profit.
16. Under what circumstances is it most ideal for you to change your password?
- a. Your coworker gives you a suggestion for a very strong password.
 - b. If your password, or your computer system, has been compromised.
 - c. It's been at least 90 days since the time you last changed your password.
 - d. You've heard about a data breach affecting one of our competitors.
17. You should share your password only with a member of our IT department, and even then, only when they are in your presence.
- a. True
 - b. False
18. Which of the following is a good practice for device passwords?
- a. Use a different password for each device.
 - b. Store passwords as contacts in a smartphone's address book.
 - c. Use cached information to recall passwords.
 - d. Keep your password written near your devices.
19. It is unacceptable to let a client or vendor use your device, even if you are watching them.
- a. True
 - b. False