✓ Congratulations! You passed!

Grade received 100%

Latest Submission Grade 100%

To pass 70% or higher

Go to next item

1. What does confidentiality of data refer to?   **1 / 1 point**

   ◯ Rules which hide data

   ◯ Rules which prevent data from being changed

   ◯ Rules which allow access only to all parties

   ⦿ Rules which restrict access only to those who need to know

   ⊘ **Correct**
   Correct! Confidentiality of data refers to restricting access to only those users that need it. The principle of least privilege (PoLP) is the idea that any user, program, or process should have only minimum privileges necessary to perform its function.

2. Maria has taken her college entry exam and is waiting for her results via email.   **1 / 1 point**
   By accident, the university sent Maria's results to Alexander. What part of the CIA Triad did the university break?

   ◯ Accessibility

   ◯ Availability

   ◯ Data breach

   ⦿ Confidentiality

⊘ **Correct**

Correct! Confidentiality involves keeping data private, often meaning that only authorized users and processes should be able to access or modify data.

3. Your company's marketing team will take a group of people to tour your facility. The company has emailed all employees requiring them to clean all white boards and ensure they clear their desktops. What is the company trying to protect against?

1 / 1 point

◯ Exposure to login credentials

◯ Damage to the company's reputation

◉ A loss of intellectual property

◯ Social engineering

⊘ **Correct**

Correct! IP theft can result in severe economic damage, loss of competitive edge, and decreased business growth.

4. What does the acronym PII stand for?

1 / 1 point

◯ Protected identity information

◯ Private Internet Identifier

◉ Personally Identifiable Information

◯ Personnel Internal Information

⊘ **Correct**

Correct! Personally Identifiable Information (PII) is data that could be used to identify a specific individual. It's considered sensitive data and the information used in identity theft. PII includes information like a person's name, address, social security or other government-issued ID number, and financial data.

5. You are investigating fraudulent activities committed by two employees at your company. You're asked to provide non-refutable evidence to confirm it. What type of evidence will you provide?

1 / 1 point

◯ Authorization logs

○ Access Control

○ Authentication records

⦿ Non-repudiation

⊘ **Correct**
Correct! Non-repudiation is the assurance that someone cannot deny the validity of something. This includes video, biometrics, digital signatures, and digital receipts that confirm the origin and integrity of the data and also confirm the recipient of the data.

6. Which two authentication methods require more than one authentication process for a login?

1 / 1 point

☐ Fingerprint reader

☐ Biometrics

☐ Access badge

☑ 2FA

⊘ **Correct**
Correct! 2FA means two-factor authorization. Besides the username and password, an additional piece of identifying data is required for authentication. It could be using a security key, a one-time password, or a security code.

☑ Multifactor authentication

⊘ **Correct**
Correct! Multifactor authentication requires additional identifying information beyond a username and password. These are typically answers to security questions you've defined, a one-time password, a security key, or biometric information such as a fingerprint scan or facial recognition.

7. You received an email from your bank alerting you to suspicious activity on your bank account. They inform you that you should change your password immediately to keep your account safe. They provide you with a link to change

1 / 1 point

your password. Which type of social engineering attack was used against you?

- ⦿ Phishing
- ◯ Session hijacking
- ◯ Identity theft
- ◯ Impersonation

⊘ **Correct**
Correct! Phishing is a social engineering attack used to steal your data, login credentials, and other personal information. An attacker masquerades, for example, as a trusted entity such as your bank, law enforcement, or government official to trick you into clicking a malicious link in an email, text, or instant message to install malware further. They try to steal your identity or could even launch a ransomware attack against you by installing additional malware.

8. Which of the following is a strong password? **1 / 1 point**

- ⦿ X5j13$#eCM19
- ◯ IluvMyCat
- ◯ ToBeorNotToBe
- ◯ BlackJack1963

⊘ **Correct**
Correct! Passwords using a combination of 12 letters, numbers, and special characters are the strongest. A password generator can help create extremely strong passwords, and password managers can help you manage and remember them.

9. Which of the following statements about cookies is true? **1 / 1 point**

- ◯ Cookies can fill up my hard drive and make my computer run slower.
- ◯ Cookies do not track my activities on a website.
- ⦿ I can get a cookie from a website I've never visited.
- ◯ Cookies contain viruses that can damage my computer.

✓ **Correct**

Correct! Certain websites you visit allow code from another website to place a cookie on your machine. Thus, the name 3rd party. These are also called trackers or tracking cookies. While not dangerous, it is believed that this is a violation of a web user's privacy. Apple Safari and Mozilla Firefox browsers automatically block 3rd party cookies while others do not.

10. What is SSL (Secure Socket Layer) used for?   **1 / 1 point**

○ Stopping certificate expiration warning messages.

◉ Preventing the interception and tampering of data.

○ Protecting the website from drive-by malware installations.

○ Protecting the website from SQL injection attacks.

✓ **Correct**

Correct! SSL encrypts data through a secure end-to-end connection. Even if a hacker sniffs the packets on the network, the data is scrambled and not human-readable.