

ADVANCE DATA PROTECTION AND PRIVACY CERTIFICATION EXAM

powell.alexander007@gmail.com

Nov. 3, 2023, 9:58 a.m.

Your score: 100% 100 / 100

Duration: 0:39:09

Congratulations on passing the Certification Exam . Your success is really well deserved. We congratulate you on your brilliant result.

1. Which of the following is the least strong security encryption standard? 4 / 4 points

Your Answer: ✓ Correct☐ WPA3☐ WPA2☐ WPA☒ WEPA**Explanation:**

Wireless security is an important aspect of cyber-security. Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2, and WPA3 are the most common kinds of wireless security. WEP is a famously insecure encryption protocol.

2. What is Cyber Security? 4 / 4 points

Your Answer: ✓ Correct☐ Cyber Security provides security against malware☐ Cyber Security provides security against cyber-terrorists☐ Cyber Security protects a system from cyber attacks☒ All of the mentioned**Explanation:**

Cyber Security provides security to a system against cyber-attacks by using various technologies, and processes.

3. Which of the following is defined as an attempt to steal, spy, damage or destroy computer systems, networks, or their associated information? 4 / 4 points

Your Answer: ✓ Correct☒ Cyber-attack☐ Computer security☐ Cryptography☐ Digital hacking**Explanation:**

An effort to steal, spy on, damage, or destroy diverse components of cyberspace, such as computer systems, related peripherals, network systems, and information, is known as a cyber-attack.

4. _____ is a special form of attack using which hackers' exploit – human psychology. 4 / 4 points

Your Answer: ✓ Correct☐ Cross Site Scripting

☐ Insecure network

✓ ☒ Social Engineering

☐ Reverse Engineering

Explanation:

Using social engineering techniques, hackers try to exploit the victim's mind to gain valuable information about that person such as his/her phone number, date of birth, pet name etc.

5. What are the features of cyber security?

4 / 4 points

Your Answer: ✓ **Correct**

☐ Compliance

☐ Defense against internal threats

☐ Threat Prevention

✓ ☒ All of the above

Explanation:

Compliance: Creating a program that meets the requirements and rules of the users.

Defense against internal threats: Should provide security against internal exploitation.

Threat Prevention: Should be capable of detecting the threat and preventing them.

6. Which of the following is not an example of social engineering?

4 / 4 points

Your Answer: ✓ **Correct**

☐ Dumpster diving

☐ Shoulder surfing

✓ ☒ Carding

☐ Spear phishing

Explanation:

Carding is the method of trafficking of bank details, credit cards or other financial information over the internet. Hence it's a fraudulent technique used by hackers and does not come under social engineering.

7. Which of the following is not a cybercrime?

4 / 4 points

Your Answer: ✓ **Correct**

☐ Denial of Service

☐ Man in the Middle

☐ Malware

✓ ☒ AES

Explanation:

Denial of Service, Man in the Middle, and Malware exploit the system causing a threat to security, hence they are considered as cybercrime. AES (Advanced Encryption Standard) provides security by encrypting the data.

8. Which of the following is not considering the adequate measure for physical security?

4 / 4 points

Your Answer: ✓ **Correct**

☐ Lock the drawers

☐ Keep strong passwords for corporate laptops and mobile phones

- ✓ ☒ Keep confidential organization's document file open in the desk
- ☐ Hide your hand against camera while inserting the PIN code

Explanation:

Keeping confidential files left open in the desk is not an adequate way of maintaining physical security; as anyone can pick these up and perform physical hacking.

9. A Federal Government Institution hired some highly skilled hackers for providing cyber security for the country or state. These types of hackers are termed as _____ 4 / 4 points

Your Answer: ✓ **Correct**

- ✓ ☒ Nation / State sponsored hackers
- ☐ CIA triad
- ☐ Special Hackers
- ☐ Government Hackers

Explanation:

Nation / State-sponsored hackers are those who are engaged or paid by a nation's or state's government to safeguard the country from cyber terrorists and other groups or individuals, as well as to expose their plans, communications, and activities.

10. _____ is an activity that takes place when cyber-criminals infiltrates any data source and takes away or alters sensitive information. 4 / 4 points

Your Answer: ✓ **Correct**

- ☐ Data-hack
- ☐ Data-stealing
- ☐ Database altering
- ✓ ☒ Data breach

Explanation:

Data breach an activity that takes place when cyber-criminals infiltrates any data source and takes away or alters sensitive information. This is either done using a network to steal all local files or get access physically to a system.

11. Which of the following is not a type of peer-to-peer cyber-crime? 4 / 4 points

Your Answer: ✓ **Correct**

- ☐ MiTM
- ☐ Injecting Trojans to a target victim
- ✓ ☒ Credit card details leak in the deep web
- ☐ Phishing

Explanation:

Peer-to-peer includes phishing, as well as the distribution of Trojans and worms to individuals. The leakage of a huge number of people's credit card data on the deep web, on the other hand, is classified as a computer-as-weapon cyber-crime.

12. A security manager needs to be able to regularly determine when operating system files change. What kind of tool is needed for this task? 4 / 4 points

Your Answer: ✓ **Correct**

- ☐ Event logging
- ☐ Intrusion detection tool
- ✓ ☒ File system integrity monitoring tool
- ☐ Log analysis tool

Explanation:

File integrity monitoring (FIM) refers to an IT security process and technology that tests and checks operating system (OS), database, and application software files to determine whether or not they have been tampered with or corrupted. FIM, which is a type of change auditing, verifies and validates these files by comparing the latest versions of them to a known, trusted “baseline.” If FIM detects that files have been altered, updated, or compromised, FIM can generate alerts to ensure further investigation, and if necessary, remediation, takes place. File integrity monitoring encompasses both reactive (forensic) auditing as well as proactive, rules-based active monitoring.

13. They are nefarious hackers, and their main motive is to gain financial profit by doing cyber-crimes. Who are “they” referred to here? 4 / 4 points

Your Answer: ✓ **Correct**

- ☐ White Hat Hackers
- ✓ ☒ Black Hat Hackers
- ☐ Hactivists
- ☐ Gray Hat Hackers

Explanation:

Black Hat hackers, often known as “crackers,” are a sort of cyber-crime that gain illegal access to a user’s account or system in order to steal confidential data or introduce malware into the system for personal gain or to harm the company.

14. A security-minded organization is relocating its business office into a shared-tenant building. How should the entrance of personnel be controlled? 4 / 4 points

Your Answer: ✓ **Correct**

- ☐ One key card system that is jointly operated by all of the tenants
- ✓ ☒ Separate key card systems that are operated by each tenant
- ☐ Security guards to control who can enter the building
- ☐ Video surveillance to monitor who enters the building

Explanation:

Separate key card systems that are operated by each tenant: Keycard entry systems are instrumental in securing and providing access to a commercial facility’s employees, inventory, and property. This includes corporate offices, healthcare facilities, retailers, fitness centers, warehouses, and more.

Designed to control, restrict, and manage unauthorized entry, this technology can also monitor employee activities and sign-in/out times, eliminate lost or stolen keys, and provide energy-saving smart technologies.

Similar to what you’d typically utilize to enter a hotel room, or other areas requiring personalized entry points, these electronic devices provide a host of benefits related to costs, security, and operations.

15. What is the existence of weakness in a system or network is known as?

4 / 4 points

Your Answer: ✓ **Correct**

- ☐ Attack
- ☐ Exploit
- ✓ ☒ Vulnerability
- ☐ Threat

Explanation:

Vulnerability is a term that refers to a weakness in a network or system that an attacker may exploit. Exploiting a weakness in security might have unintended and undesirable consequences.

16. After completing a risk assessment, an organization was able to reduce the risk through the addition of detective and preventive controls. However, these controls did not remove all risk. What options does the organization have for treating the remaining risk?

4 / 4 points

Your Answer: ✓ **Correct**

- ✓ ☒ Accept, avoid, reduce, or transfer
- ☐ None—the organization must accept the risk
- ☐ The organization must either accept or transfer the risk
- ☐ Does not apply: remaining risk cannot be treated further

Explanation:

In cases where the cost outweighs the benefit, most organizations choose to accept a risk rather than spend time or money mitigating it. Accepting a risk is sometimes referred to as the “do nothing” option. This may be a familiar concept for those of you familiar with project management fundamentals.

17. An information system that processes sensitive information is configured to require a valid user ID and strong password from any user. This process of accepting and validating this information is known as:

4 / 4 points

Your Answer: ✓ **Correct**

- ✓ ☒ Authentication
- ☐ Strong authentication
- ☐ Two-factor authentication
- ☐ Single sign-on

Explanation:

Authentication is the process of determining whether someone or something is, in fact, who or what it says it is. Authentication technology provides access control for systems by checking to see if a user's credentials match the credentials in a database of authorized users or in a data authentication server. In doing this, authentication assures secure systems, secure processes and enterprise information security.

18. CIA is known as:

4 / 4 points

Your Answer: ✓ **Correct**

- ✓ ☒ Confidentiality, Integrity, and Availability
- ☐ Computers, Information, and Assets
- ☐ Confidence In Applications

☐ Controls, Integrity, and Availability

Explanation:

The three letters in "CIA triad" stand for Confidentiality, Integrity, and Availability. The CIA triad is a common model that forms the basis for the development of security systems. They are used for finding vulnerabilities and methods for creating solutions.

19. What is true about data security?

4 / 4 points

Your Answer:  **Correct**

- ☐ Data security is the protection of programs and data in computers and communication systems against unauthorized access.
- ☐ It refers to the right of individuals or organizations to deny or restrict the collection and use of information
- ☐ Data security requires system managers to reduce unauthorized access to the systems by building physical arrangements and software checks.

 ☒ All of the above.

Explanation:

Data security is the process of safeguarding digital information throughout its entire life cycle to protect it from corruption, theft, or unauthorized access. It covers everything—hardware, software, storage devices, and user devices; access and administrative controls; and organizations' policies and procedures.

20. _____ means the protection of data from modification by unknown users.

4 / 4 points

Your Answer:  **Correct**

- ☐ Confidentiality
-  ☒ Integrity
- ☐ Authentication
- ☐ Non-repudiation

Explanation:

Integrity in cyber security means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. here...

21. What is called periodic assessment of security vulnerability in computer system?

4 / 4 points

Your Answer:  **Correct**

- ☐ Threat
- ☐ Attack
- ☐ Hacking
-  ☒ Security audit

Explanation:

Independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures.

22. Which of the following is an objective of network security?

4 / 4 points

Your Answer:  **Correct**

- ☐ Confidentiality

☐ Integrity

☐ Antivirus

✓ ☒ All of the above

Explanation:

The objectives of network security are Confidentiality, Integrity, and Availability.

23. Which of the following refers to the violation of the principle if a computer is no more accessible?

4 / 4 points

Your Answer: ✓ **Correct**

☐ Access control

☐ Confidentiality

✓ ☒ Availability

☐ All of the above

Explanation:

Availability refers to the violation of principle, if the system is no more accessible. The function of confidentiality is to keep sensitive company information safe from unwanted access. The confidentiality component of network security ensures that data is only accessible to those who are authorized to see it.

Integrity: This goal entails ensuring and preserving data accuracy and consistency. The purpose of integrity is to ensure that data is accurate and not tampered with by unauthorized individuals.

Availability: The purpose of availability in Network Security is to ensure that data, network resources, and services are always available to legitimate users, whenever they need them.

24. Which of the following is the technique used to look for information in trash or around dustbin container?

4 / 4 points

Your Answer: ✓ **Correct**

☐ Pretexting

☐ Baiting

☐ Quid Pro Quo

✓ ☒ Dumpster diving

Explanation:

In the technology world, where information about a person seems everywhere; dumpster diving is the name of the technique where the attacker looks for information in dustbins and trashes. For example, after withdrawing money from ATM, the user usually throw the receipt in which the total amount and account details are mentioned. These type of information becomes helpful to a hacker, for which they use dumpster diving.

25. Stealing pen drives and DVDs after tailgating is an example of lack of _____ security.

4 / 4 points

Your Answer: ✓ **Correct**

☐ network security

✓ ☒ physical security

☐ database security

☐ wireless security

Explanation:

When cyber-criminal gain access to an authorized area and steal pen drives and DVDs which contain sensitive information about an employee or about the organization, then it can be said that the physical security of the organization is weak.

