# 220-1102 Q&As

CompTIA A+ Certification: Core 2

## Pass CompTIA 220-1102 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

**https://www.pass4itsure.com/220-1102.html**

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

**QUESTION 1**

Which of the following could be used to implement secure physical access to a data center?

A. Geofence

B. Alarm system

C. Badge reader

D. Motion sensor

Correct Answer: C

Badge readers are used to implement secure physical access to a data center. They are used to read the identification information on an employee\\'s badge and grant access to the data center if the employee is authorized2. This system requires individuals to have an access badge that contains their identification information or a unique code that can be scanned by a reader. After the badge is scanned, the system compares the information on the badge with the authorized personnel database to authenticate if the individual has the required clearance to enter that area. The other options listed, such as a geofence, alarm system, or motion sensor are security measures that may be used in conjunction with badge readers, but do not provide identification and authentication features.

**QUESTION 2**

An administrator configured security features on company-owned mobile devices to help protect against data loss. Which of the following is the best way to protect data on a misplaced device?

A. Remote wipe

B. Device encryption

C. PIN codes

D. Locator applications

Correct Answer: B

**QUESTION 3**

Which of the following is used to generate passcodes necessary to access applications or systems that require an extra layer of security?

A. Authenticator application

B. Access control lists

C. Biometrics

D. Smart card readers

Correct Answer: A

Authenticator applications are designed to enhance security by generating temporary, time-sensitive passcodes used in two-factor authentication (2FA) processes. These passcodes are used in conjunction with traditional credentials (like usernames and passwords) to grant access to systems or applications. This extra layer of security ensures that even if primary login credentials are compromised, unauthorized access is still prevented without the dynamically generated code from the authenticator app.

**QUESTION 4**

Which of the following file extensions are commonly used to install applications on a macOS machine? (Select THREE).

A. .mac

B. .Pkg

C. .deb

D. .dmg

E. .msi

F. .appx

G. .app

H. .apk

Correct Answer: BDG

https://support.microsoft.com/en-us/windows/common-file-name-extensions-in-windows-da4a4430-8e76-89c5-59f7-1cdbbc75cb01

.pkg and .dmg are files used to distribute and install applications on macOS. .pkg files are installer packages that may contain multiple files and executable code, while .dmg files are disk images that can contain a single bundled application or multiple applications. .app files are typically the main executable files for macOS applications. The other options listed are file extensions for applications or installers on other platforms (such as .deb for Debian- based Linux systems, .msi for Windows, and .apk for Android). This information is covered in the Comptia A+ Core2 documents/guide under the Mac OS section.

**QUESTION 5**

A call center handles inquiries into billing issues for multiple medical facilities. A security analyst notices that call center agents often walk away from their workstations, leaving patient data visible for anyone to see. Which of the following should a network administrator do to BEST prevent data theft within the call center?

A. Encrypt the workstation hard drives.

B. Lock the workstations after five minutes of inactivity.

C. Install privacy screens.

D. Log off the users when their workstations are not in use.

Correct Answer: B

The BEST solution for preventing data theft within the call center in this scenario would be to lock the workstations after a period of inactivity. This would prevent unauthorized individuals from accessing patient data if call center agents were to step away from their workstations without logging out.

**QUESTION 6**

A technician is installing RAM in a new workstation and needs to protect against electrostatic discharge. Which of the following will best resolve this concern?

A. Battery backup

B. Thermal paste

C. ESD strap

D. Consistent power

Correct Answer: C

**QUESTION 7**

Which of the following environments allows for the testing of critical systems without the risk of them being negatively impacted by changes?

A. Regression

B. Cloud

C. Production

D. Sandbox

Correct Answer: D

A sandbox is an isolated environment that allows for the testing of critical systems without the risk of them being negatively impacted by changes. A sandbox can be used to simulate real-world scenarios, experiment with new features, debug errors, or evaluate the performance and security of a system. A sandbox can be created using virtualization, emulation, or containerization technologies. A sandbox prevents any changes made in the testing environment from affecting the production environment, which is the actual system that is used by the end users. https://www.comptia.org/training/books/a-core-2-220-1102-study-guide

**QUESTION 8**

A technician is concerned about a large increase in the number of whaling attacks happening in the industry. The technician wants to limit the company\\'s risk to avoid any issues. Which of the following items should the technician implement?

A. Screened subnet

B. Firewall

C. Anti-phishing training

D. Antivirus

Correct Answer: C

**QUESTION 9**

Which of the following is an advantage of MOST tablets over laptops?

A. Larger storage space

B. Upgradeable parts

C. GPS tracking software

D. Multi-touch screens

Correct Answer: D

**QUESTION 10**

A technician wants to harden Windows workstations after a recent security audit indicated the company is vulnerable to brute-force attacks. Which of the following features should the technician implement to mitigate such attacks?

A. System screen lock

B. Failed log-in lockout

C. Restricted user permissions

D. Data-at-rest encryption

Correct Answer: B

To mitigate brute-force attacks, implementing a failed log-in lockout feature is effective. This security measure temporarily disables user accounts after a specified number of unsuccessful login attempts, preventing attackers from continuously trying different password combinations to gain unauthorized access.

**QUESTION 11**

Which of the following physical security controls can prevent laptops from being stolen?

A. Encryption

B. LoJack

C. Multifactor authentication

D. Equipment lock

E. Bollards

Correct Answer: D

**QUESTION 12**

A technician is modifying the default home page of all the workstations in a company. Which of the following will help to implement this change?

A. Insist that the customer is correct and document the concern.

B. Listen to the customer and do not speak at all.

C. Escalate the issue to the next tier.

D. Apologize and ask what would help resolve the issue.

Correct Answer: D

**QUESTION 13**

Every time a user tries to open the organization\\'s proprietary application on an Android tablet, the application immediately closes. Other applications are operating normally. Which of the following troubleshooting actions would MOST likely resolve the issue? (Choose two.)

A. Uninstalling the application

B. Gaining root access to the tablet

C. Resetting he web browser cache

D. Deleting the application cache

E. Clearing the application storage

F. Disabling mobile device management

Correct Answer: DE

**QUESTION 14**

During an enterprise rollout of a new application, a technician needs to validate compliance with an application\\'s EULA while also reducing the number of licenses to manage. Which of the following licenses would best accomplish this goal?

A. Personal use license

B. Corporate use license

C. Open-source license

D. Non-expiring license

Correct Answer: B

**QUESTION 15**

A user is setting up a new Windows 10 laptop. Which of the following Windows settings should be used to input the SSID and password?

A. Network and Internet

B. System

C. Personalization

D. Accounts

Correct Answer: A

The Network and Internet settings in Windows 10 allow the user to input the SSID and password of a Wi-Fi network, as well as manage other network-related options, such as airplane mode, mobile hotspot, VPN, proxy, etc1. To access the Network and Internet settings, the user can select the Start button, then select Settings > Network and Internet2. Alternatively, the user can right-click the Wi-Fi icon on the taskbar and click "Open Network and Internet Settings"3. The System settings in Windows 10 allow the user to configure the display, sound, notifications, power, storage, and other system-related options1. The Personalization settings in Windows 10 allow the user to customize the background, colors, lock screen, themes, fonts, and other appearance-related options1. The Accounts settings in Windows 10 allow the user to manage the user accounts, sign-in options, sync settings, and other account-related options1. None of these settings can be used to input the SSID and password of a Wi-Fi network. References: The Official CompTIA A+ Core 2 Study Guide1, page 221, 222, 223, 224.