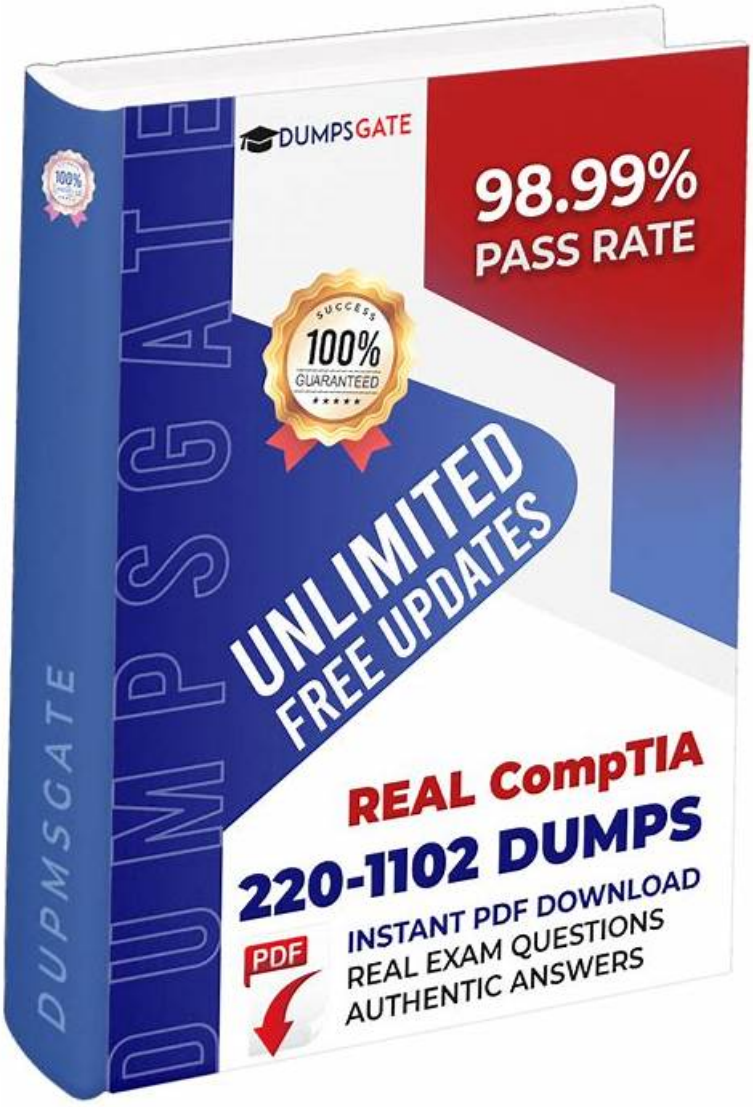
# 2025 Trustable 220-1102 Dumps Guide Help You Pass 220-1102 Easily




BONUS!!! Download part of PassLeaderVCE 220-1102 dumps for free: https://drive.google.com/open?id=1FgduCmQyf0xVDiHOFgjoR78z4X4flF2p

PassLeaderVCE's 220-1102 exam training materials evoke great repercussions in the examinees, and has established a very good reputation, which means that choosing PassLeaderVCE 220-1102 exam training materials is to choose success. After you buy our 220-1102 VCE Dumps, if you fail to pass the certification exam or there are any problems of learning materials, we will give a full refund. What's more, after you buy our 220-1102 exam, we will provide one year free renewal service.

To prepare for the CompTIA 220-1102 Exam, candidates can take advantage of various resources, including online courses, study guides, practice exams, and virtual labs. It is essential to have practical experience in the field and a thorough understanding of the exam objectives to pass the exam successfully. Once certified, IT professionals can expect to earn a higher salary, have more job opportunities, and advance their careers in the IT industry.

**>> 220-1102 Dumps Guide <<**

## Quiz CompTIA - Reliable 220-1102 - CompTIA A+ Certification Exam: Core 2 Dumps Guide

Perhaps you have had such an unpleasant experience about what you brought in the internet was not suitable for you in actual use, to avoid this, our company has prepared 220-1102 free demo in this website for our customers. The content of the free demo is part of the content in our real 220-1102 Study Guide. Therefore, you can get a comprehensive idea about our real 220-1102 study materials. And you will find there are three kinds of versions of 220-1102 learning materials for you to choose from namely, PDF Version Demo, PC Test Engine and Online Test Engine.

CompTIA 220-1102 Exam is an essential certification for IT professionals who want to advance their careers. 220-1102 exam tests the candidates' knowledge and skills in managing and maintaining IT systems, including troubleshooting, security, and networking issues. CompTIA A+ Certification Exam: Core 2 certification is globally recognized and is highly valued in the IT industry. It provides an opportunity for individuals to enhance their knowledge and skills in the IT field and demonstrate their expertise to potential employers.

## CompTIA A+ Certification Exam: Core 2 Sample Questions (Q425-Q430):

**NEW QUESTION # 425**
The camera and microphone on an iPhone user's device are activating without any user input.
The user's friend recently modified the device to allow applications to be installed outside the normal App Store.
Which of the following is the issue?

- A. The iPhone has an out-of-date operating system.
- B. The user connected a counterfeit Lightning cable to the iPhone.
- C. The device was jailbroken to remove internal security protections.
- D. The device is unenrolled from Mobile Device Management.

**Answer: C**

Explanation:
The camera and microphone on an iPhone activating without user input, especially after allowing applications to be installed outside the normal App Store, is a classic sign of the device being jailbroken. Jailbreaking an iPhone removes many of the built-in security features and restrictions, allowing the installation of apps from third-party sources. These third-party apps can be malicious and can gain unauthorized access to system resources like the camera and microphone.
* A. The user connected a counterfeit Lightning cable to the iPhone. While counterfeit cables can be harmful, they typically cause charging or connectivity issues rather than security vulnerabilities that would enable camera and microphone activation without user input.
* B. The device is unenrolled from Mobile Device Management. Unenrolling from MDM removes organizational controls but does not directly cause unauthorized camera and microphone activation.
* D. The iPhone has an out-of-date operating system. An outdated OS can have vulnerabilities, but the scenario specifically mentions modifications to allow third-party app installations, pointing to jailbreaking as the primary cause.
References:
* CompTIA A+ Core 2 (220-1102) Exam Objectives, Section 2.3: Security measures and their purposes including mobile device security.

**NEW QUESTION # 426**
A technician successfully removed malicious software from an infected computer after running updates and scheduled scans to mitigate future risks. Which of the following should the technician do next?

- A. Create a system restore point.
- B. Investigate how the system was infected with malware.
- C. Educate the end user on best practices for security.
- D. Quarantine the host in the antivirus system.

**Answer: C**

Explanation:
Explanation
Educating the end user on best practices for security is the next step that the technician should take after successfully removing malicious software from an infected computer. Educating the end user on best practices for security is an important part of preventing future infections and mitigating risks. The technician should explain to the end user how to avoid common sources of malware, such as phishing emails, malicious websites, or removable media. The technician should also advise the end user to use strong passwords, update software regularly, enable antivirus and firewall protection, and backup data frequently. Educating the end

user on best practices for security can help the end user become more aware and responsible for their own security and reduce the likelihood of recurrence of malware infections. Quarantining the host in the antivirus system, investigating how the system was infected with malware, and creating a system restore point are not the next steps that the technician should take after successfully removing malicious software from an infected computer. Quarantining the host in the antivirus system is a step that the technician should take before removing malicious software from an infected computer. Quarantining the host in the antivirus system means isolating the infected computer from the network or other devices to prevent the spread of malware.
Investigating how the system was infected with malware is a step that the technician should take during or after removing malicious software from an infected computer. Investigating how the system was infected with malware means identifying the source, type, and impact of malware on the system and documenting the findings and actions taken. Creating a system restore point is a step that the technician should take before removing malicious software from an infected computer. Creating a system restore point means saving a snapshot of the system's configuration and settings at a certain point in time, which can be used to restore the system in case of failure or corruption. References:
Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 15 CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide, page 458

**NEW QUESTION # 427**
A technician needs to recommend the best backup method that will mitigate ransomware attacks. Only a few files are regularly modified, however, storage space is a concern. Which of the following backup methods would BEST address these concerns?

- A. Full
- B. Off-site
- C. Grandfather-father-son
- D. Differential

**Answer: D**

Explanation:
Explanation
The differential backup method would best address these concerns. Differential backups only back up files that have changed since the last full backup, which means that only a few files would be backed up each time. This would help to mitigate the risk of ransomware attacks, as only a few files would be affected if an attack occurred. Additionally, differential backups require less storage space than full backups.

**NEW QUESTION # 428**
A technician removed a virus from a user's device. The user returned the device a week later with the same virus on it. Which of the following should the technician do to prevent future infections?

- A. Educate the end user.
- B. Disable System Restore.
- C. Clean the environment reinstallation.
- D. Install the latest OS patches.

**Answer: A**

Explanation:
Educating the end user is the best way to prevent future infections by viruses or other malware. The technician should teach the user how to avoid risky behaviors, such as opening suspicious attachments, clicking on unknown links, downloading untrusted software, etc. Disabling System Restore, installing the latest OS patches and performing a clean installation are possible ways to remove existing infections, but they do not prevent future ones. Verified References:
https://www.comptia.org/blog/how-to-prevent-malwarehttps://www.comptia.org/certifications/a

**NEW QUESTION # 429**
A technician needs to configure a computer for a user to work from home so the user can still securely access the user's shared files and corporate email. Which of the following tools would best accomplish this task*?

- A. FTP
- B. VPN

- C. RMM
- D. MSRA

**Answer: B**

Explanation:
A Virtual Private Network (VPN) creates a secure connection over the internet to a network, allowing a user to access shared files and corporate email as if they were directly connected to the network. This makes VPN the best tool for secure remote work access, compared to the other options which do not offer the same level of secure, remote network access.

**NEW QUESTION # 430**
.....