

# 220-1102<sup>Q&As</sup>

CompTIA A+ Certification Exam: Core 2

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

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

<https://www.pass2lead.com/220-1102.html>

100% Passing Guarantee  
100% Money Back Assurance

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

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



### QUESTION 1

A technician installed a known-good, compatible motherboard on a new laptop. However, the motherboard is not working on the laptop. Which of the following should the technician MOST likely have done to prevent damage?

- A. Removed all jewelry
- B. Completed an inventory of tools before use
- C. Practiced electrical fire safety
- D. Connected a proper ESD strap

Correct Answer: D

The technician should have connected a proper ESD strap to prevent damage to the motherboard. ESD (electrostatic discharge) can cause damage to electronic components, and an ESD strap helps to prevent this by grounding the technician and preventing the buildup of static electricity. Removing all jewelry is also a good practice, but it is not the most likely solution to this problem.

---

### QUESTION 2

Which of the following macOS features can help a user close an application that has stopped responding?

- A. Finder
- B. Mission Control
- C. System Preferences
- D. Force Quit

Correct Answer: D

---

### QUESTION 3

A wireless network is set up, but it is experiencing some interference from other nearby SSIDs. Which of the following can BEST resolve the interference?

- A. Changing channels
- B. Modifying the wireless security
- C. Disabling the SSID broadcast
- D. Changing the access point name

Correct Answer: A

Changing channels can best resolve interference from other nearby SSIDs. Wireless networks operate on different channels, and changing the channel can help to avoid interference from other nearby networks.

---

**QUESTION 4**

A technician just completed a Windows 10 installation on a PC that has a total of 16GB of RAM. The technician notices the Windows OS has only 4GB of RAM available for use. Which of the following explains why the OS can only access 4GB of RAM?

- A. The UEFI settings need to be changed.
- B. The RAM has compatibility issues with Windows 10.
- C. Some of the RAM is defective.
- D. The newly installed OS is x86.

Correct Answer: D

The newly installed OS is x86. The x86 version of Windows 10 can only use up to 4GB of RAM. The x64 version of Windows 10 can use up to 2TB of RAM

---

**QUESTION 5**

Maintaining the chain of custody is an important part of the incident response process. Which of the following reasons explains why this is important?

- A. To maintain an information security policy
- B. To properly identify the issue
- C. To control evidence and maintain integrity
- D. To gather as much information as possible

Correct Answer: C

---

**QUESTION 6**

A technician is replacing the processor in a desktop computer prior to opening the computer, the technician wants to ensure the internal components are protected. Which of the following safety procedures would BEST protect the components in the PC? (Select TWO).

- A. Utilizing an ESD strap
- B. Disconnecting the computer from the power source
- C. Placing the PSU in an antistatic bag
- D. Ensuring proper ventilation
- E. Removing dust from the ventilation fans
- F. Ensuring equipment is grounded

Correct Answer: AC

The two safety procedures that would best protect the components in the PC are:

1.

Utilizing an ESD strap

2.

Placing the PSU in an antistatic bag

<https://www.professormesser.com/free-a-plus-training/220-902/computer-safety-procedures-2/> <https://www.skillssoft.com/course/comptia-a-core-2-safety-procedures-environmental-impacts-cbdf0f2c-61c0-4f4a-a659-dc98f1f00158>

---

### QUESTION 7

A technician is preparing to remediate a Trojan virus that was found on a workstation. Which of the following steps should the technician complete BEFORE removing the virus?

- A. Disable System Restore.
- B. Schedule a malware scan.
- C. Educate the end user.
- D. Run Windows Update.

Correct Answer: A

Before removing a Trojan virus from a workstation, a technician should disable System Restore. System Restore is a feature that allows users to restore their system to a previous state in case of problems or errors. However, System Restore can also restore infected files or registry entries that were removed by antivirus software or manual actions. By disabling System Restore, a technician can ensure that the Trojan virus is completely removed and does not reappear after a system restore operation. Scheduling a malware scan may help detect and remove some malware but may not be effective against all types of Trojan viruses. Educating the end user may help prevent future infections but does not address the current issue of removing the Trojan virus. Running Windows Update may help patch some security vulnerabilities but does not guarantee that the Trojan virus will be removed. References: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 1.3

---

### QUESTION 8

A police officer often leaves a workstation for several minutes at a time. Which of the following is the BEST way the officer can secure the workstation quickly when walking away?

- A. Use a key combination to lock the computer when leaving.
- B. Ensure no unauthorized personnel are in the area.
- C. Configure a screensaver to lock the computer automatically after approximately 30 minutes of inactivity.
- D. Turn off the monitor to prevent unauthorized visibility of information.

Correct Answer: A

The BEST way to secure the workstation quickly when walking away is to use a key combination to lock the computer when leaving

---

**QUESTION 9**

Sensitive data was leaked from a user's smartphone. A technician discovered an unapproved application was installed, and the user has full access to the device's command shell.

Which of the following is the NEXT step the technician should take to find the cause of the leaked data?

- A. Restore the device to factory settings.
- B. Uninstall the unapproved application.
- C. Disable the ability to install applications from unknown sources.
- D. Ensure the device is connected to the corporate WiFi network.

Correct Answer: B

The technician should disable the user's access to the device's command shell. This will prevent the user from accessing sensitive data and will help to prevent further data leaks. The technician should then investigate the unapproved application to determine if it is the cause of the data leak. If the application is found to be the cause of the leak, the technician should uninstall the application and restore the device to factory settings. If the application is not the cause of the leak, the technician should investigate further to determine the cause of the leak. Disabling the ability to install applications from unknown sources can help to prevent future data leaks, but it is not the next step the technician should take in this scenario. Ensuring the device is connected to the corporate WiFi network is not relevant to this scenario

---

**QUESTION 10**

A company would like to implement multifactor authentication for all employees at a minimal cost. Which of the following best meets the company's requirements?

- A. Biometrics
- B. Soft token
- C. Access control lists
- D. Smart card

Correct Answer: B

---

**QUESTION 11**

A user enabled a mobile device's screen lock function with pattern unlock. The user is concerned someone could access the mobile device by repeatedly attempting random patterns to unlock the device. Which of the following features BEST addresses the user's concern?

- A. Remote wipe
- B. Anti-malware
- C. Device encryption
- D. Failed login restrictions

Correct Answer: A

The feature that BEST addresses the user's concern is remote wipe. This is because remote wipe allows the user to erase all data on the mobile device if it is lost or stolen, which will prevent unauthorized access to the device

---

### QUESTION 12

A user's corporate phone was stolen, and the device contains company trade secrets. Which of the following technologies should be implemented to mitigate this risk? (Select TWO).

- A. Remote wipe
- B. Firewall
- C. Device encryption
- D. Remote backup
- E. Antivirus
- F. Global Positioning System

Correct Answer: AC

Remote wipe is a feature that allows data to be deleted from a device or system remotely by an administrator or owner. It is used to protect data from being compromised if the device is lost, stolen, or changed hands<sup>1</sup>. Device encryption is a

feature that helps protect the data on a device by making it unreadable to unauthorized users<sup>2</sup>. It requires a key or a password to access the data. Both features can help mitigate the risk of losing company trade secrets if a corporate phone

is stolen.

References:

How to remote wipe Windows laptop

(<https://www.thewindowsclub.com/remote-wipe-windows-10>)

Device encryption in Windows (<https://support.microsoft.com/en-us/windows/device-encryption-in-windows-ad5dcf4b-dbe0-2331-228f-7925c2a3012d>)

---

### QUESTION 13

All the desktop icons on a user's newly issued PC are very large. The user reports that the PC was working fine until a recent software patch was deployed. Which of the following would BEST resolve the issue?

- A. Rolling back video card drivers
- B. Restoring the PC to factory settings
- C. Repairing the Windows profile
- D. Reinstalling the Windows OS

Correct Answer: A

Rolling back video card drivers is the best way to resolve the issue of large desktop icons on a user's newly issued PC. This means restoring the previous version of the drivers that were working fine before the software patch was deployed. The software patch may have caused compatibility issues or corrupted the drivers, resulting in display problems

---

#### QUESTION 14

An administrator has received approval for a change request for an upcoming server deployment. Which of the following steps should be completed NEXT?

- A. Perform a risk analysis.
- B. Implement the deployment.
- C. Verify end user acceptance
- D. Document the lessons learned.

Correct Answer: A

Before making any changes to the system, it is important to assess the risks associated with the change and determine whether it is worth implementing. Risk analysis involves identifying potential risks, assessing their likelihood and impact, and determining what steps can be taken to mitigate them. It is important to perform this step before making any changes, as this allows the administrator to make an informed decision about whether or not the change should be implemented. Once the risks have been assessed and the administrator has decided to go ahead with the change, the next step is to implement the deployment.

---

#### QUESTION 15

A technician downloaded software from the Internet that required the technician to scroll through a text box and at the end of the text box, click a button labeled Accept

Which of the following agreements IS MOST likely in use?

- A. DRM
- B. NDA
- C. EULA
- D. MOU

Correct Answer: C

The most likely agreement in use here is a EULA (End User License Agreement). This is a legally binding agreement between the user and the software developer, outlining the terms and conditions that the user must agree to in order to use the software. It is important that the user understands and agrees to the EULA before they can proceed with downloading and installing the software. As stated in the CompTIA A+ Core 2 exam objectives, users should be aware of the EULA before downloading any software.

[220-1102 VCE Dumps](#)

[220-1102 Practice Test](#)

[220-1102 Exam Questions](#)