



# CompTIA

## Exam Questions 220-1202

CompTIA A+ Certification Exam: Core 2

**NEW QUESTION 1**

Recently, the number of users sharing smartphone passcodes has increased. The management team wants a technician to deploy a more secure screen lock method. Which of the following technologies should the technician use?

- A. Pattern lock
- B. Facial recognition
- C. Device encryption
- D. Multifactor authentication

**Answer: B**

**Explanation:**

Comprehensive and Detailed Explanation From Exact Extract:  
Facial recognition is a biometric authentication method that ties access to a unique physical feature of the user. Unlike passcodes or pattern locks—which can be easily shared—facial recognition provides a more secure and non-transferable form of access. It also enhances user convenience and is widely supported by modern smartphones.

- \* A. Pattern locks can still be shared and are less secure.
- \* C. Device encryption protects data but does not prevent screen access if a passcode is shared.
- \* D. Multifactor authentication typically applies to app or account access, not basic phone unlocking.

Reference:

CompTIA A+ 220-1102 Objective 2.2: Compare and contrast common security measures and authentication technologies.  
Study Guide Section: Biometric screen lock technologies (e.g., facial recognition, fingerprint)

=====

**NEW QUESTION 2**

After a recent mobile OS upgrade to a smartphone, a user attempts to access their corporate email, but the application does not open. A technician restarts the smartphone, but the issue persists. Which of the following is the most likely way to resolve the issue?

- A. Updating the failed software
- B. Registering the smartphone with an MDM solution
- C. Installing a third-party client
- D. Clearing the cache partition

**Answer: A**

**Explanation:**

Comprehensive and Detailed Explanation From Exact Extract:  
Mobile OS updates can sometimes cause compatibility issues with specific apps, including corporate email clients. The most likely resolution is to check for and apply an update to the affected application, especially if it hasn't been updated to support the latest OS version.

- \* B. Registering with MDM might be required for access but wouldn't address app crashes due to incompatibility.
- \* C. A third-party client might help, but it's not the best first step if the default app is expected to work.
- \* D. Clearing the cache can help resolve some minor issues, but updating the app directly addresses compatibility concerns.

Reference:

CompTIA A+ 220-1102 Objective 3.3: Troubleshoot mobile OS and application issues. Study Guide Section: App compatibility and mobile software updates

=====

**NEW QUESTION 3**

A company would like to deploy baseline images to new computers as they are started up on the network. Which of the following boot processes should the company use for this task?

- A. ISO
- B. Secure
- C. USB
- D. PXE

**Answer: D**

**Explanation:**

Comprehensive and Detailed Explanation From Exact Extract:  
PXE (Preboot Execution Environment) allows workstations to boot over the network and download an OS image from a server. It is ideal for automating mass deployments using baseline images across many machines without the need for physical media.

- \* A. An ISO is a disk image file but requires mounting or physical media.
- \* B. Secure Boot is a security feature, not a method of deploying OS images.
- \* C. USB requires manual installation and is not suitable for automated deployment at scale. Reference:

CompTIA A+ 220-1102 Objective 1.4: Given a scenario, use appropriate Microsoft operating system installation methods.  
Study Guide Section: Remote installation methods — PXE boot deployment

=====

**NEW QUESTION 4**

Which of the following is an example of an application publisher including undisclosed additional software in an installation package?

- A. Virus
- B. Ransomware
- C. Potentially unwanted program
- D. Trojan

**Answer: C**

**Explanation:**

Comprehensive and Detailed Explanation From Exact Extract:

A Potentially Unwanted Program (PUP) is software that a user may not have knowingly installed. It often gets bundled with legitimate software and installs without full disclosure. PUPs can affect performance, change system settings, or display unwanted ads but are not necessarily malicious like viruses or ransomware.

\* A. Viruses replicate and spread; they are generally more harmful and not "bundled" in the same way.

\* B. Ransomware encrypts files for payment and is deliberately malicious.

\* D. A Trojan disguises itself as legitimate software to perform malicious actions but is not typically pre-bundled by legitimate publishers.

Reference:

CompTIA A+ 220-1102 Objective 2.5: Given a scenario, detect, remove, and prevent malware using appropriate tools and methods.

Study Guide Section: Types of malware — PUPs and bundled software

=====

**NEW QUESTION 5**

A technician needs to configure laptops so that only administrators can enable virtualization technology if needed. Which of the following should the technician configure?

- A. BIOS password
- B. Guest account
- C. Screen lock
- D. AutoRun setting

**Answer: A**

**Explanation:**

Comprehensive and Detailed Explanation From Exact Extract:

Virtualization settings are typically found within the BIOS/UEFI firmware configuration. To prevent unauthorized users from changing these settings, the technician should set a BIOS password. This ensures only administrators with the password can access or modify BIOS settings, including virtualization support.

\* B. The guest account is a user-level feature in Windows and doesn't control BIOS access.

\* C. A screen lock prevents casual access to the desktop but doesn't protect firmware settings.

\* D. AutoRun controls how media and devices behave when inserted — unrelated to BIOS security.

Reference:

CompTIA A+ 220-1102 Objective 2.2: Compare and contrast security measures and administrative controls.

Study Guide Section: BIOS/UEFI settings protection — password implementation

**NEW QUESTION 6**

A technician is setting up a Windows server to allow remote desktop connections for multiple users. Which of the following should the technician configure on the workstation?

- A. Firewall
- B. Computer Management
- C. User Accounts
- D. Ease of Access

**Answer: A**

**Explanation:**

Comprehensive and Detailed Explanation From Exact Extract:

To allow Remote Desktop Protocol (RDP) access, the firewall must be configured to allow inbound connections on TCP port 3389. If the Windows Firewall blocks RDP, users will not be able to connect remotely even if the feature is enabled in system settings.

\* B. Computer Management allows configuration of services and local users, but not network access.

\* C. User Accounts is for account setup and control, but enabling remote access requires firewall configuration.

\* D. Ease of Access is unrelated to remote connectivity—it's for accessibility features. Reference:

CompTIA A+ 220-1102 Objective 2.2: Compare and contrast security measures and firewall settings.

Study Guide Section: Enabling and securing RDP via firewall settings

=====

**NEW QUESTION 7**

A technician thinks that an application a user downloaded from the internet may not be the legitimate one, even though the name is the same. The technician needs to confirm whether the application is legitimate. Which of the following should the technician do?

- A. Compare the hash value from the vendor.
- B. Run Task Manager and compare the process ID.
- C. Run the application in safe mode.
- D. Verify the file name is correct.

**Answer: A**

**Explanation:**

Comprehensive and Detailed Explanation From Exact Extract:

To ensure the authenticity of a downloaded application, the most reliable method is to verify the file's hash (e.g., SHA256, MD5) against the value provided by the legitimate

vendor. If the hash values match, the file has not been altered or tampered with. This verification confirms the integrity and authenticity of the executable.

\* B. Process IDs are dynamic and not unique to specific software.

\* C. Running in safe mode doesn't validate legitimacy—it only runs the app in a minimal environment.

\* D. File names can be spoofed; matching the name does not prove authenticity. Reference:

CompTIA A+ 220-1102 Objective 2.2: Compare and contrast authentication and software integrity verification methods.

Study Guide Section: Hash verification for software authenticity and digital integrity

**NEW QUESTION 8**

A technician is using a credential manager to safeguard a large number of credentials. Which of the following is important for using this application?

- A. Restricted log-in times
- B. Secure master password
- C. TPM module
- D. Windows lock screen

**Answer: B**

**Explanation:**

Comprehensive and Detailed Explanation From Exact Extract:

Credential managers or password vaults (e.g., Windows Credential Manager, KeePass, or LastPass) store passwords securely. The integrity of such tools heavily depends on the strength of the master password protecting the vault. If compromised, all saved credentials could be exposed. Therefore, setting a secure master password is crucial.

- \* A. Login time restrictions are general user account settings, not specific to credential managers.
- \* C. TPM is used more commonly for full disk encryption, not specifically required for password managers.
- \* D. The lock screen protects general access but does not protect stored credentials alone. Reference: CompTIA A+ 220-1102 Objective 2.2: Compare and contrast authentication technologies and secure credential storage. Study Guide Section: Password management and protection best practices

**NEW QUESTION 9**

A technician installs VPN client software that has a software bug from the vendor. After the vendor releases an update to the software, the technician attempts to reinstall the software but keeps getting an error message that the network adapter for the VPN already exists. Which of the following should the technician do next to mitigate this issue?

- A. Run the latest OS security updates.
- B. Map the network adapter to the new software.
- C. Update the network adapter's firmware.
- D. Delete hidden network adapters.

**Answer: D**

**Explanation:**

Comprehensive and Detailed Explanation From Exact Extract:

VPN clients often create virtual network adapters. If the software wasn't uninstalled properly or crashed during install, leftover (often hidden) virtual adapters can prevent reinstallation. The proper solution is to delete hidden network adapters using Device Manager (with ??Show hidden devices?? enabled).

- \* A. OS updates won't fix a leftover driver or adapter issue.
- \* B. Mapping an adapter to the software is not a standard or viable solution.
- \* C. Firmware updates apply to physical adapters, not virtual VPN adapters. Reference: CompTIA A+ 220-1102 Objective 3.1: Troubleshoot common Windows OS and network issues. Study Guide Section: Troubleshooting network adapter conflicts and VPN client errors

**NEW QUESTION 10**

A user is attempting to open on a mobile phone a HD video that is hosted on a popular media streaming website. The user is receiving connection timeout errors. The mobile reception icon area is showing two bars next to 3G. Which of the following is the most likely cause of the issue?

- A. The user does not have Wi-Fi enabled.
- B. The website's subscription has run out.
- C. The bandwidth is not fast enough.
- D. The mobile device storage is full.

**Answer: C**

**Explanation:**

Comprehensive and Detailed Explanation From Exact Extract:

3G networks generally do not provide the bandwidth required for seamless HD video streaming. With only two signal bars and a 3G connection, the mobile device likely cannot maintain the necessary data throughput, resulting in timeouts or buffering failures. This is a classic symptom of insufficient network speed or signal strength.

- \* A. Lack of Wi-Fi may contribute, but the root cause is the low mobile bandwidth, not the Wi-Fi state.
- \* B. A website subscription lapse would return an account error, not a timeout.
- \* D. Full device storage can affect downloads but not streaming from the internet. Reference: CompTIA A+ 220-1102 Objective 3.3: Troubleshoot mobile OS and application issues. Study Guide Section: Connectivity and network performance issues on mobile devices

**NEW QUESTION 10**

A customer is unable to open some files on their system. Each time the customer attempts to open a file, the customer receives a message that the file is encrypted. Which of the following best describes this issue?

- A. Keylogger
- B. Ransomware
- C. Phishing
- D. Cryptominer

**Answer: B**

**Explanation:**

Comprehensive and Detailed Explanation From Exact Extract:

Ransomware is a type of malware that encrypts the user's files and demands a payment (ransom) for the decryption key. When a user receives a message stating

that their files are encrypted and cannot be accessed, ransomware is the most likely cause. The attacker's goal is to hold the data hostage until the victim pays to restore access.

- \* A. Keylogger records keystrokes and doesn't encrypt files.
- \* C. Phishing is a social engineering tactic to gather credentials, not to encrypt data.
- \* D. Cryptominer uses system resources to mine cryptocurrency, not encrypt files. Reference: CompTIA A+ 220-1102 Objective 2.3: Compare and contrast common types of malware and threats. Study Guide Section: Ransomware behavior and user impact

**NEW QUESTION 11**

Which of the following filesystem types does the Linux OS use?

- A. exFAT
- B. APFS
- C. ext4
- D. NTFS

**Answer: C**

**Explanation:**

Comprehensive and Detailed Explanation From Exact Extract:  
 The ext4 (Fourth Extended Filesystem) is the most widely used default filesystem in modern Linux distributions. It is designed for high performance, scalability, and reliability, and is supported by all mainstream Linux kernels.

- \* A. exFAT is used for cross-platform external drives, not native Linux systems.
- \* B. APFS is Apple's proprietary filesystem for macOS and iOS.
- \* D. NTFS is the default filesystem for Windows, not Linux. Reference: CompTIA A+ 220-1102 Objective 1.9: Identify common features and tools of the Linux client/desktop OS. Study Guide Section: Filesystem types in Linux — ext3, ext4, and their characteristics

**NEW QUESTION 14**

An employee is using a photo editing program. Certain features are disabled and require a log-in, which the employee does not have. Which of the following is a way to resolve this issue?

- A. License assignment
- B. VPN connection
- C. Application repair
- D. Program reinstallation

**Answer: A**

**Explanation:**

Comprehensive and Detailed Explanation From Exact Extract:  
 Many modern commercial software applications (including photo editors like Adobe Photoshop) offer tiered features based on user subscriptions or license levels. If certain features are locked and prompt for a login, the issue is likely due to a missing or unassigned software license. Assigning the correct license through a centralized license management system (such as Adobe Admin Console or Microsoft 365 portal) will enable those features.

- \* B. VPN connection does not affect local software licensing.
- \* C. Repairing the application does not resolve license entitlement.
- \* D. Reinstalling the software won't help unless the license is assigned. Reference: CompTIA A+ 220-1102 Objective 3.3: Troubleshoot common software and application issues. Study Guide Section: Troubleshooting licensing and access control for applications

**NEW QUESTION 15**

Which of the following is the quickest way to move from Windows 10 to Windows 11 without losing data?

- A. Using gpupdate
- B. Image deployment
- C. Clean install
- D. In-place upgrade

**Answer: D**

**Explanation:**

Comprehensive and Detailed Explanation From Exact Extract:  
 An in-place upgrade is the fastest and most efficient way to upgrade from Windows 10 to Windows 11 while keeping all user data, applications, and settings intact. This method is often used when the hardware meets Windows 11 requirements and no system reconfiguration is necessary.

- \* A. gpupdate is used to refresh Group Policy settings — unrelated to OS upgrades.
- \* B. Image deployment typically replaces the current OS and may not retain user data unless specifically customized.
- \* C. A clean install requires formatting the drive and starting fresh, which removes all data. Reference: CompTIA A+ 220-1102 Objective 1.4: Given a scenario, use appropriate Microsoft operating system installation methods. Study Guide Section: In-place upgrade vs. clean install methods

**NEW QUESTION 18**

Which of the following methods would make data unrecoverable but allow the drive to be repurposed?

- A. Deleting the partitions
- B. Implementing EFS
- C. Performing a low-level format

D. Degaussing the device

**Answer: C**

**Explanation:**

Comprehensive and Detailed Explanation From Exact Extract:

A low-level format (also referred to as a zero-fill or full format) writes over every sector on a storage device, effectively destroying the existing data and making recovery nearly impossible. Unlike degaussing, which renders the drive unusable, a low-level format maintains the integrity of the device, allowing it to be repurposed or reused.

- \* A. Deleting partitions does not fully erase data; it only removes references in the partition table.
- \* B. EFS (Encrypting File System) encrypts files but does not securely wipe them.
- \* D. Degaussing destroys the magnetic structure of a drive, making it inoperable and not reusable.

Reference:

CompTIA A+ 220-1102 Objective 4.3: Given a scenario, implement basic change management best practices.

Study Guide Section: Drive sanitation methods — low-level format vs. degaussing vs. deletion

=====

**NEW QUESTION 23**

A user receives a new personal computer but is unable to run an application. An error displays saying that .NET Framework 3.5 is required and not found. Which of the following actions is the best way to resolve this issue?

- A. Resolve the dependency through the 'Turn Windows features on or off' menu.
- B. Download the dependency via a third-party repository.
- C. Ignore the dependency and install the latest version 4 instead.
- D. Forward the trouble ticket to the SOC team because the issue poses a great security risk.

**Answer: A**

**Explanation:**

Comprehensive and Detailed Explanation From Exact Extract:

NET Framework versions are often required for applications to run. If an older app requires .NET Framework 3.5, it must be explicitly installed as it is not included by default in newer versions of Windows. The best method to do this safely is through the built-in "Turn Windows features on or off" utility, which downloads and installs it via official Microsoft services.

- \* B. Using third-party repositories is unsafe and not recommended.
- \* C. Installing .NET 4 does not include 3.5; versions are not fully backward compatible.
- \* D. The issue is technical, not a security incident for the SOC team. Reference:

CompTIA A+ 220-1102 Objective 3.3: Troubleshoot common software, application, and OS security issues.

Study Guide Section: Managing application dependencies (e.g., .NET Framework, Java)

=====

**NEW QUESTION 25**

A network technician notices that most of the company's network switches are now end-of-life and need to be upgraded. Which of the following should the technician do first?

- A. Implement the change
- B. Approve the change
- C. Propose the change
- D. Schedule the change

**Answer: C**

**Explanation:**

Comprehensive and Detailed Explanation From Exact Extract:

The first step in the IT change management process is to identify and propose the change. In this case, the technician notices a need (end-of-life network switches), so the appropriate action is to formally propose a change. This proposal would be documented and submitted for approval before any planning or implementation occurs. According to the CompTIA A+ 220-1102 objectives under Operational Procedures (Domain 4.0), the change management process follows these typical steps:

- ? Submit a change request (Propose the change)
- ? Review and approval (Approve the change)
- ? Planning and scheduling (Schedule the change)
- ? Implementation
- ? Documentation and review

Therefore, proposing the change is the correct first step in accordance with standard ITIL- based change management practices.

Reference:

CompTIA A+ 220-1102 Objective 4.1: Given a scenario, implement best practices associated with documentation and support systems information management.

Study Guide Section: Change Management Process

=====

**NEW QUESTION 26**

**SIMULATION**

As a corporate technician, you are asked to evaluate several suspect email messages on a client's computer. Corporate policy requires the following:

- >All phishing attempts must be reported.
  - >Future spam emails to users must be prevented. INSTRUCTIONS
- Review each email and perform the following within the email:
- >Classify the emails
  - >Identify suspicious items, if applicable, in each email
  - >Select the appropriate resolution

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

## Inbox

<p><b>Account Locked</b> Dear User, We have detected unusual activity com...</p>	 <h3 style="margin: 0;">No Mail Selected</h3> <p>Select an email to view its contents</p>	<p><b>Email Classification Menu</b></p> <p><b>Classification</b></p> <div style="border: 1px solid #ccc; padding: 2px; width: 100%; margin-bottom: 5px;"> <span style="float: right;">▼</span> </div> <p><b>Resolution</b></p> <ul style="list-style-type: none"> <li><input type="radio"/> Report email to Information Security</li> <li><input type="radio"/> Perform no additional actions</li> <li><input type="radio"/> Unsubscribe</li> <li><input type="radio"/> Open attachment</li> </ul>
<p><b>Share Your Feedback</b> It only takes 4 minutes of your time! In partnersh...</p>		
<p><b>Employee Orientation</b> Dear Joe, Welcome to CompTIA! We are excited...</p>		
<p><b>Security Update</b> We need to install an urgent patch to your Windows...</p>		
<p><b>Interview</b> Good afternoon Joe, I just wanted to thank you for...</p>		

## Inbox

<p><b>Account Locked</b> Dear User, We have detected unusual activity com...</p>	<p><b>From:</b> ithelpdesk@comptia.co  <b>Subject:</b> Account Locked  <b>To:</b> joe@comptia.org</p>	<p><b>Email Classification Menu</b></p> <p><b>Classification</b></p> <div style="border: 1px solid #ccc; padding: 2px; width: 100%; margin-bottom: 5px;"> <span style="float: right;">▼</span> </div> <ul style="list-style-type: none"> <li style="background-color: #0070c0; color: white; padding: 2px;">Phishing</li> <li style="padding: 2px;">Spam</li> <li style="padding: 2px;">Legitimate</li> </ul> <p><b>Resolution</b></p> <ul style="list-style-type: none"> <li><input type="radio"/> Report email to Information Security</li> <li><input type="radio"/> Perform no additional actions</li> <li><input type="radio"/> Unsubscribe</li> <li><input type="radio"/> Open attachment</li> </ul>
<p><b>Share Your Feedback</b> It only takes 4 minutes of your time! In partnersh...</p>	<p>Dear User,</p> <p style="text-align: right;">↩ ↶ ↷</p> <p>We have detected unusual activity coming from your corporate account joe@comptia.org. To protect your account, please click <a href="#">HERE</a> to change your password.</p>	
<p><b>Employee Orientation</b> Dear Joe, Welcome to CompTIA! We are excited...</p>	<p>Regards,</p> <p>CompTIA IT Help Desk</p>	
<p><b>Security Update</b> We need to install an urgent patch to your Windows...</p>		
<p><b>Interview</b> Good afternoon Joe, I just wanted to thank you for...</p>		


## Inbox

<p><b>Account Locked</b> Dear User, We have detected unusual activity com...</p>	<p><b>From:</b> survey@researchco.net  <b>Subject:</b> Share Your Feedback And Get Free Wireless Headphones!  <b>To:</b> joe@comptia.org  <b>Signed By:</b> survey@researchco.net</p> <p style="text-align: right;"></p>	<p><b>Email Classification Menu</b></p> <p><b>Classification</b></p> <div style="border: 1px solid #ccc; padding: 2px;"> <span style="background-color: #0070C0; color: white; display: block; text-align: center;">[Selected]</span> </div> <p>Phishing Spam Legitimate</p> <p><b>Resolution</b></p> <p><input type="radio"/> Report email to Information Security</p> <p><input type="radio"/> Perform no additional actions</p> <p><input type="radio"/> Unsubscribe</p> <p><input type="radio"/> Open attachment</p>
<p><b>Share Your Feedback</b> It only takes 4 minutes of your time! In partnersh...</p>	<p style="background-color: #FF8C00; padding: 2px;"><b>External Email</b></p> <p>It only takes 4 minutes of your time!</p> <p>In partnership with Research &amp; Co. we are conducting a survey regarding your cellular service. As an expert in your field, we'd love to get your feedback!</p> <p>This quick survey will only take a few minutes of your time, and as a token of our appreciation for sharing your insight, you will receive a pair of wireless headphones.</p> <p>Take the Survey <a href="#">here!</a></p> <p><a href="#">Manage Email Preferences</a></p>	
<p><b>Employee Orientation</b> Dear Joe, Welcome to CompTIA! We are excited...</p>		
<p><b>Security Update</b> We need to install an urgent patch to your Windows...</p>		
<p><b>Interview</b> Good afternoon Joe, I just wanted to thank you for...</p>		

## Inbox

<p><b>Account Locked</b> Dear User, We have detected unusual activity com...</p>	<p><b>From:</b> Human Resources &lt;hr@comptia.org&gt;  <b>Subject:</b> Employee Orientation  <b>To:</b> joe@comptia.org</p> <p> Employee_Reference_Guide.PDF</p>	<p><b>Email Classification Menu</b></p> <p><b>Classification</b></p> <div style="border: 1px solid #ccc; padding: 2px;"> <span style="background-color: #0070C0; color: white; display: block; text-align: center;">[Selected]</span> </div> <p>Phishing Spam Legitimate</p> <p><b>Resolution</b></p> <p><input type="radio"/> Report email to Information Security</p> <p><input type="radio"/> Perform no additional actions</p> <p><input type="radio"/> Unsubscribe</p> <p><input type="radio"/> Open attachment</p>
<p><b>Share Your Feedback</b> It only takes 4 minutes of your time! In partnersh...</p>	<p>Dear Joe,</p> <p>Welcome to CompTIA!</p> <p>We are excited that you are here, and we know you will be a valuable asset to the company.</p> <p>Please review the attached orientation material to get started with the onboarding experience.</p> <p>Regards, CompTIA Human Resources</p>	
<p><b>Employee Orientation</b> Dear Joe, Welcome to CompTIA! We are excited</p>		
<p><b>Security Update</b> We need to install an urgent patch to your Windows...</p>		
<p><b>Interview</b> Good afternoon Joe, I just wanted to thank you for...</p>		

**Inbox**

<p><b>Account Locked</b> Dear User, We have detected unusual activity com...</p>	<p><b>From:</b> CompTIA Information Security &lt;infosec@comptiaa.org&gt;  <b>Subject:</b> Security Update  <b>To:</b> joe@comptia.org   patch1.exe</p>	<p><b>Email Classification Menu</b></p> <p><b>Classification</b></p> <div style="border: 1px solid #ccc; padding: 2px;"> <span style="background-color: #0070c0; color: white; padding: 2px;">Phishing</span>              Spam              Legitimate         </div> <p><b>Resolution</b></p> <p><input type="radio"/> Report email to Information Security</p> <p><input type="radio"/> Perform no additional actions</p> <p><input type="radio"/> Unsubscribe</p> <p><input type="radio"/> Open attachment</p>
<p><b>Share Your Feedback</b> It only takes 4 minutes of your time! In partnersh...</p>	<p>We need to install an urgent patch to your Windows Operating System. Please download and run the included attachment to install the security patch as soon as possible!</p>	
<p><b>Employee Orientation</b> Dear Joe, Welcome to CompTIA! We are excited...</p>	<p>Regards, CompTIA Information Security infosec@comptia.org</p>	
<p><b>Security Update</b> We need to install an urgent patch to your Windows...</p>		
<p><b>Interview</b> Good afternoon Joe, I just wanted to thank you for...</p>		

**Inbox**

<p><b>Account Locked</b> Dear User, We have detected unusual activity com...</p>	<p><b>From:</b> Alex &lt;alex@gmail.com&gt;  <b>Subject:</b> Interview  <b>To:</b> joe@comptia.org</p>	<p><b>Email Classification Menu</b></p> <p><b>Classification</b></p> <div style="border: 1px solid #ccc; padding: 2px;"> <span style="background-color: #0070c0; color: white; padding: 2px;">Phishing</span>              Spam              Legitimate         </div> <p><b>Resolution</b></p> <p><input type="radio"/> Report email to Information Security</p> <p><input type="radio"/> Perform no additional actions</p> <p><input type="radio"/> Unsubscribe</p> <p><input type="radio"/> Open attachment</p>
<p><b>Share Your Feedback</b> It only takes 4 minutes of your time! In partnersh...</p>	<p>Good afternoon Joe,</p>	
<p><b>Employee Orientation</b> Dear Joe, Welcome to CompTIA! We are excited...</p>	<p>I just wanted to thank you for your time during my interview last week. It was exciting to hear about the position and possible opportunity at CompTIA. Please don't hesitate to reach out to me with any questions or concerns you may have about me or my qualifications. Regardless of the outcome, it was a pleasure speaking with you, and I hope to have the opportunity to work with you in the future.</p>	
<p><b>Security Update</b> We need to install an urgent patch to your Windows...</p>	<p>Regards, Alex</p>	
<p><b>Interview</b> Good afternoon Joe, I just wanted to thank you for...</p>		

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Inbox mail 1 -Account Locked- Phishing - Report email to Information Security  
 Inbox mail 2 -Share your feedback - Legitimate - Perform no additional actions  
 Inbox mail 3 -Employee orientation - Legitimate - Perform no additional actions  
 Inbox mail 4 -Security Update - Spam - Report email to Information Security  
 Inbox mail 5 -Interview - Legitimate - Perform no additional actions

**NEW QUESTION 29**

A help desk technician needs to remove RAM from retired workstations and upgrade other workstations that have applications that use more memory with this RAM. Which of the following actions would the technician most likely take?

- A. Demagnetize memory for security.
- B. Use antistatic bags for storage and transport.
- C. Plug in the power supply to ground each workstation.
- D. Install memory in identical pairs.

**Answer: B**

**Explanation:**

Comprehensive and Detailed Explanation From Exact Extract:

RAM is an electrostatic-sensitive component. When removing or transporting RAM modules, they should be stored in antistatic bags to protect against electrostatic discharge (ESD), which can damage the memory. This is a standard best practice in hardware handling.

\* A. Demagnetization is not applicable to RAM.

\* C. Plugging in power to ground is not safe or recommended for static protection.

\* D. Installing identical memory pairs is applicable for dual-channel configuration, but not directly related to transporting or handling RAM.

Reference:

CompTIA A+ 220-1102 Objective 4.3: Explain environmental impacts and procedures. Study Guide Section: ESD safety practices and component handling procedures

**NEW QUESTION 30**

Which of the following is used to detect and record access to restricted areas?

- A. Bollards
- B. Video surveillance
- C. Badge readers
- D. Fence

**Answer: C**

**Explanation:**

Comprehensive and Detailed Explanation From Exact Extract:

Badge readers are electronic access control systems that require authorized users to scan a badge (e.g., RFID or magnetic strip cards) to gain access to restricted physical locations. These systems typically log all access attempts—successful or denied—providing both detection and recording of access events.

\* A. Bollards are physical barriers to prevent vehicle access.

\* B. Video surveillance can record access visually but does not track identity unless integrated with access control systems.

\* D. A fence restricts access but doesn't detect or record who entered. Reference:

CompTIA A+ 220-1102 Objective 2.4: Compare and contrast physical security measures.

Study Guide Section: Physical access controls (e.g., badge readers, mantraps)

**NEW QUESTION 32**

A technician needs to install an operating system on a large number of workstations. Which of the following is the fastest method?

- A. Physical media
- B. Mountable ISO
- C. Manual installation
- D. Image deployment

**Answer: D**

**Explanation:**

Comprehensive and Detailed Explanation From Exact Extract:

Image deployment is the fastest and most efficient method for installing operating systems on multiple machines. It involves creating a pre-configured image of an OS and deploying it across systems using tools like Windows Deployment Services (WDS) or third-party imaging solutions. This method saves time and ensures consistency across all devices.

\* A. Physical media is slow and not scalable.

\* B. Mountable ISOs are useful but still require manual installation.

\* C. Manual installation is time-consuming and not suitable for large-scale deployment. Reference:

CompTIA A+ 220-1102 Objective 1.4: Given a scenario, use appropriate Microsoft operating system installation methods.

Study Guide Section: Deployment methods — image deployment, automation

**NEW QUESTION 36**

A support specialist needs to decide whether to install a 32-bit or 64-bit OS architecture on a new computer. Which of the following specifications will help the specialist determine which OS architecture to use?

- A. 16GB RAM
- B. Intel i7 CPU
- C. 500GB HDD
- D. 1Gbps Ethernet

**Answer: A**

**Explanation:**

Comprehensive and Detailed Explanation From Exact Extract:

The amount of installed RAM is the key factor in determining whether a 64-bit OS is needed. A 32-bit operating system cannot effectively address more than 4GB of RAM. Since this system has 16GB of RAM, a 64-bit OS is required to utilize the full memory.

\* B. An Intel i7 CPU supports both 32-bit and 64-bit OS installations, so it alone doesn't determine the need.

\* C. HDD size does not influence OS architecture selection.

\* D. Ethernet speed is a network consideration and not related to OS architecture. Reference:

CompTIA A+ 220-1102 Objective 1.4: Given a scenario, choose the appropriate Microsoft OS installation methods and configurations.

Study Guide Section: 32-bit vs. 64-bit system requirements and memory limitations

=====

**NEW QUESTION 41**

A help desk technician is setting up speech recognition on a Windows system. Which of the following settings should the technician use?

- A. Time and Language
- B. Personalization
- C. System
- D. Ease of Access

**Answer: D**

**Explanation:**

Comprehensive and Detailed Explanation From Exact Extract:

In Windows, accessibility tools such as speech recognition are found under the Ease of Access settings. This section includes options for users who require assistive technologies, including screen readers, magnifiers, and voice control interfaces like speech recognition. Setting up speech recognition allows users to control the system and input text using voice commands.

- \* A. Time and Language is for setting regional preferences and language packs.
- \* B. Personalization adjusts themes, backgrounds, and colors.
- \* C. System includes display, storage, notifications, and power settings, but not accessibility tools.

Reference:

CompTIA A+ 220-1102 Objective 1.3: Given a scenario, use appropriate Microsoft operating system features and tools.

Study Guide Section: Accessibility tools and system configuration

=====

**NEW QUESTION 46**

A user reports getting a BSOD (Blue Screen of Death) error on their computer at least twice a day. Which of the following should the technician use to determine the cause?

- A. Event Viewer
- B. Performance Monitor
- C. System Information
- D. Device Manager

**Answer: A**

**Explanation:**

Comprehensive and Detailed Explanation From Exact Extract:

Event Viewer is the primary tool used to investigate system-level errors and logs, including BSODs. When a BSOD occurs, Windows logs the error codes and associated system behavior under System logs in Event Viewer. This allows the technician to review crash events, identify error codes (e.g., STOP codes), and pinpoint hardware or driver issues.

- \* B. Performance Monitor is used for real-time performance tracking and trend analysis, not crash logs.
- \* C. System Information displays system specs but not crash logs or events.
- \* D. Device Manager shows device status and driver issues but doesn't retain error logs related to BSODs.

Reference:

CompTIA A+ 220-1102 Objective 3.1: Given a scenario, troubleshoot common Windows OS problems.

Study Guide Section: Troubleshooting BSODs using Event Viewer and system logs

=====

**NEW QUESTION 50**

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### 220-1202 Practice Exam Features:

- \* 220-1202 Questions and Answers Updated Frequently
- \* 220-1202 Practice Questions Verified by Expert Senior Certified Staff
- \* 220-1202 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* 220-1202 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
[Order The 220-1202 Practice Test Here](#)