CompTIA

Exam Questions 220-1202

CompTIA A+ Certification Exam: Core 2

NEW QUESTION 1
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 2
A technician uses AI to draft a proposal about the benefits of new software. When reading the draft, the technician notices that the draft contains factually incorrect information. Which of the following best describes this scenario?

A. Data privacy
B. Hallucinations
C. Appropriate use
D. Plagiarism

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
In the context of artificial intelligence, "hallucinations" refer to instances where an AI system generates information that is plausible-sounding but factually incorrect or entirely fabricated. This is a known limitation of large language models, including generative AI tools.
* A. Data privacy refers to the protection of personal or sensitive data, not content accuracy.
* C. Appropriate use relates to ethical and policy-based concerns, not factual correctness.
* D. Plagiarism involves presenting someone else's work as your own — this situation is about accuracy, not ownership.
Reference:
CompTIA A+ 220-1102 Objective 4.4: Identify basic concepts of scripting and automation. Study Guide Section: AI tools and responsible usage — hallucinations and fact-checking outputs
==========

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 user frequently misplaces their Windows laptop and is concerned about it being stolen. The user would like additional security controls on their laptop. Which of the following is a built-in technology that a technician can use to enable full drive encryption?

A. Active Directory
B. New Technology File System
C. Encrypting File System
D. BitLocker

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract: BitLocker is Microsoft??s full disk encryption technology built into Windows Pro and Enterprise editions. It encrypts the entire drive, protecting data if the device is lost or stolen. BitLocker can use TPM (Trusted Platform Module) and can be configured with PINs or USB keys for added security.
* A. Active Directory is for centralized user and policy management in domains.
* B. NTFS is the file system format and doesn't provide encryption by itself.
* C. EFS (Encrypting File System) encrypts individual files or folders, not the entire drive. Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast security measures and encryption tools.
Study Guide Section: Encryption options — BitLocker vs. EFS
==========

NEW QUESTION 6
A technician needs to map a shared drive from a command-line interface. Which of the following commands should the technician use?

A. pathping
B. nslookup
C. net use
D. tracert

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The net use command in Windows is used to map (assign) a shared drive from the command line. The syntax typically looks like: net use X: \server\share where X is the drive letter and \server\share is the network path.
* A. pathping tests network latency and packet loss.
* B. nslookup is used for DNS troubleshooting.
* D. tracert shows the route packets take to reach a destination — not for drive mapping. Reference:
CompTIA A+ 220-1102 Objective 1.7: Given a scenario, troubleshoot common operating system problems.
Study Guide Section: Command-line tools — net use for drive mapping
==========

NEW QUESTION 7
Which of the following methods involves requesting a user's approval via a push notification to verify the user's identity?

A. Call
B. Authenticator
C. Hardware token
D. SMS

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Authenticator apps (e.g., Microsoft Authenticator, Google Authenticator, Duo) often support push notifications. When the user logs in, the app sends a push to their mobile device, prompting the user to approve or deny the authentication request — a common and user- friendly form of multi-factor authentication (MFA).
* A. Phone call verification is a separate method involving voice-based confirmation.
* C. Hardware tokens generate one-time codes but do not send push notifications.
* D. SMS sends a text message with a code — again, no push mechanism. Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast multi-factor authentication methods.
Study Guide Section: Authentication apps and push notification verification
==========

NEW QUESTION 8
Which of the following is used in addition to a password to implement MFA?

A. Sending a code to the user's phone
B. Verifying the user's date of birth
C. Prompting the user to solve a simple math problem
D. Requiring the user to enter a PIN

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Multi-Factor Authentication (MFA) requires at least two different types of authentication factors:
? Something you know (e.g., password or PIN)
? Something you have (e.g., smartphone or hardware token)
? Something you are (e.g., fingerprint or facial recognition)
Option A, sending a code to the user??s phone, is an example of "something you have" — a physical device that receives a one-time passcode. Combined with a password, this forms a proper MFA implementation.
* B. Date of birth is another knowledge-based factor (like a password), not a second factor type.
* C. Solving a math problem is not a recognized authentication factor.
* D. A PIN is also "something you know" and does not count as a distinct MFA factor when paired with a password.
Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast common security measures and authentication technologies.
Study Guide Section: Authentication factors — password, biometrics, tokens, MFA
==========

NEW QUESTION 9
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 10
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 10
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 11
A help desk team was alerted that a company-owned cell phone has an unrecognized password-cracking application. Which of the following should the help desk team do to prevent further unauthorized installations from occurring?

A. Configure Group Policy.
B. Implement PAM.
C. Install anti-malware software.
D. Deploy MDM.

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Mobile Device Management (MDM) is used to control, monitor, and enforce policies on mobile devices. It allows IT teams to restrict app installations, push approved apps, and monitor device compliance. Deploying MDM would prevent unauthorized applications, such as password crackers, from being installed on company-managed devices.
* A. Group Policy is for managing Windows environments and not applicable to smartphones.
* B. PAM (Privileged Access Management) controls administrative access, not app installation.
* C. Anti-malware can help detect malicious apps but doesn??t prevent their installation proactively.
Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast common security measures and tools.
Study Guide Section: Mobile Device Management (MDM) capabilities — app control, security enforcement

NEW QUESTION 16
A security administrator teaches all of an organization's staff members to use BitLocker To Go. Which of the following best describes the reason for this training?

A. To ensure that all removable media is password protected in case of loss or theft
B. To enable Secure Boot and a BIOS-level password to prevent configuration changes
C. To enforce VPN connectivity to be encrypted by hardware modules
D. To configure all laptops to use the TPM as an encryption factor for hard drives

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
BitLocker To Go is a Microsoft encryption feature specifically designed for removable drives such as USB flash drives and external hard drives. It allows users to protect the data on these devices by requiring a password to decrypt the contents, thereby preventing unauthorized access in the event the device is lost or stolen.
A is correct because BitLocker To Go is directly tied to password-protecting removable media.
B and C are unrelated to BitLocker To Go; Secure Boot and VPN encryption are entirely
different security layers.
D applies to BitLocker (not BitLocker To Go) and full disk encryption on internal drives using TPM.
Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast common security measures and tools.
Study Guide Section: Encryption technologies (BitLocker, BitLocker To Go)
==========

NEW QUESTION 19
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 21

Which of the following is found in an MSDS sheet for a battery backup?

A. Installation instructions
B. Emergency procedures
C. Configuration steps
D. Voltage specifications

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
An MSDS (Material Safety Data Sheet), now commonly referred to as SDS (Safety Data Sheet), is a document that provides detailed information on the properties of a particular substance. It includes safety guidelines and emergency procedures related to handling, exposure, fire hazards, and first aid—not installation or configuration instructions.
For a battery backup (UPS device), the MSDS would include emergency procedures such as what to do in case of a chemical spill, exposure to battery acid, or fire hazard due to overheating or chemical leakage. This ensures the safety of personnel and complies with hazardous materials handling regulations.
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: MSDS/SDS usage and safety documentation

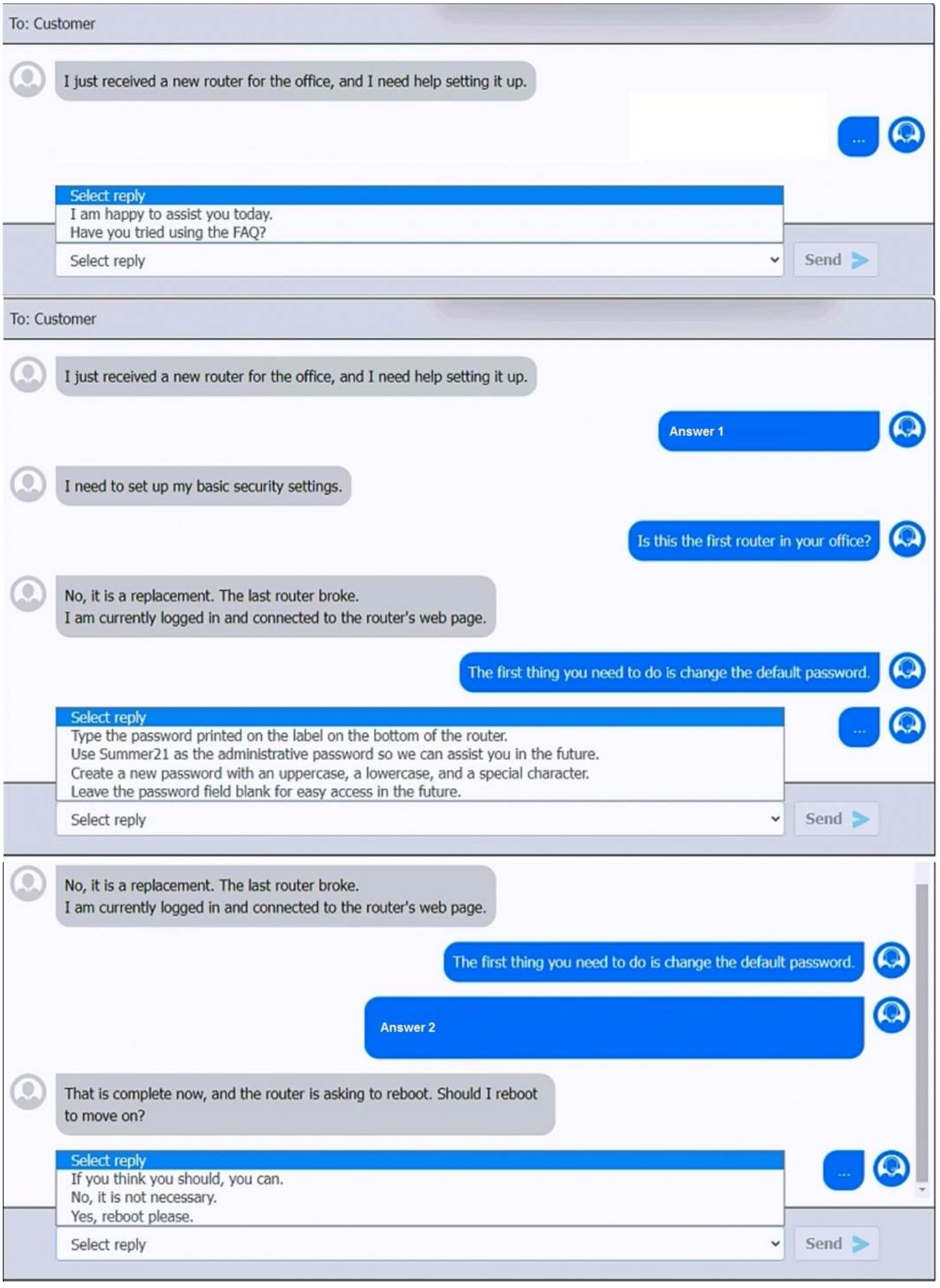
NEW QUESTION 24
A customer is unable to open some files on their system. Each time the customer attempts to open a file, the customer receives a message that the file is encrypted. Which of the following best describes this issue?

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 28
SIMULATION
You have been contacted through the help desk chat application. A user is setting up a replacement SOHO router. Assist the user with setting up the router.
INSTRUCTIONS
Select the most appropriate statement for each response. Click the send button after each response to continue the chat.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
First Chat Response:When the user mentions setting up a new router, the best initial response to maintain a helpful and professional tone is:
>Select reply:"I am happy to assist you today."
Second Chat Response:When the user states that they need to set up basic security settings:
>Select reply:"Is this the first router in your office?"
Third Chat Response:After learning it's a replacement router and the user is logged into the router's web page:
>Select reply:"The first thing you need to do is change the default password."
Fourth Chat Response:For the response about password settings:
>Select reply:"Create a new password with an uppercase, a lowercase, and a special character."
Fifth Chat Response:When the router prompts to reboot:
>Select reply:"Yes, reboot please."
Study Guide Reference: The CompTIA A+ Core 2 guide highlights the importance of changing default credentials and using strong password policies, particularly in SOHO environments where routers are often targeted.

NEW QUESTION 32
A technician is troubleshooting an issue in which a service runs momentarily and stops at certain points in the process. The technician needs to determine the root cause of this issue. Which of the following tools should the technician use?

A. Event Viewer
B. Task Manager
C. Internet Options
D. Process Explorer

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Event Viewer is the best tool to analyze the root cause of service failures in Windows. It provides detailed logs from system processes, including errors, warnings, and crash reports related to services and applications. When a service starts and stops unexpectedly, Event Viewer will often record the cause, such as dependency failures or access violations.
* B. Task Manager shows active processes but doesn't retain logs or causes of failure.
* C. Internet Options is used for configuring browser settings, not troubleshooting services.
* D. Process Explorer is powerful but more suited for live monitoring and detailed process trees, not post-failure log analysis.
Reference:
CompTIA A+ 220-1102 Objective 3.1: Given a scenario, troubleshoot common Windows OS problems.
Study Guide Section: Log file analysis using Event Viewer
==========

NEW QUESTION 34
A technician notices that the weekly backup is taking too long to complete. The daily backups are incremental. Which of the following would most likely resolve the issue?

A. Changing the backup window
B. Performing incremental weekly backups
C. Increasing the backup storage
D. Running synthetic full weekly backups

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
A synthetic full backup combines the last full backup with subsequent incremental backups to create a new full backup without re-reading data from the source system. This method significantly reduces the backup window and network impact. It is especially useful when traditional full backups are too time-consuming.
* A. Changing the backup window only shifts timing, not duration.
* B. Incremental weekly backups would lack a proper full recovery point and aren't ideal alone.
* C. Storage space isn't the bottleneck in backup speed—it??s read/write operations and network load.
Reference:
CompTIA A+ 220-1102 Objective 4.2: Summarize backup and recovery concepts.
Study Guide Section: Backup types — full, incremental, differential, and synthetic backups
==========

NEW QUESTION 39
An application's performance is degrading over time. The application is slowing, but it never gives an error and does not crash. Which of the following tools should a technician use to start troubleshooting?

A. Reliability history
B. Computer management
C. Resource monitor
D. Disk

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract: Resource Monitor provides real-time monitoring of system performance and resource usage, including CPU, memory, disk, and network usage. It helps technicians identify
performance bottlenecks (e.g., high memory or CPU usage) that can cause slowdowns in applications over time without producing crash errors.
* A. Reliability history logs application crashes or errors — not helpful if the app doesn??t crash.
* B. Computer Management is a broad utility with limited real-time monitoring capability.

* D. Disk is too vague — tools like CHKDSK can help with disk errors but not general performance degradation.
Reference:
CompTIA A+ 220-1102 Objective 3.2: Given a scenario, troubleshoot common personal computer issues.
Study Guide Section: System performance tools — Resource Monitor, Task Manager
==========

NEW QUESTION 43
Which of the following types of social engineering attacks sends an unsolicited text message to a user's mobile device?

A. Impersonation
B. Vishing
C. Spear phishing
D. Smishing

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Smishing (SMS phishing) is a type of social engineering attack where attackers send fraudulent text messages to trick users into revealing sensitive information or downloading malware. These messages often impersonate banks, delivery services, or official institutions to lure the victim into clicking malicious links.
* A. Impersonation is an in-person or voice-based tactic.
* B. Vishing refers to voice phishing over phone calls.
* C. Spear phishing is a targeted email-based phishing method. Reference:
CompTIA A+ 220-1102 Objective 2.3: Compare and contrast social engineering techniques.
Study Guide Section: Smishing as a type of phishing via SMS or mobile messaging.
==========

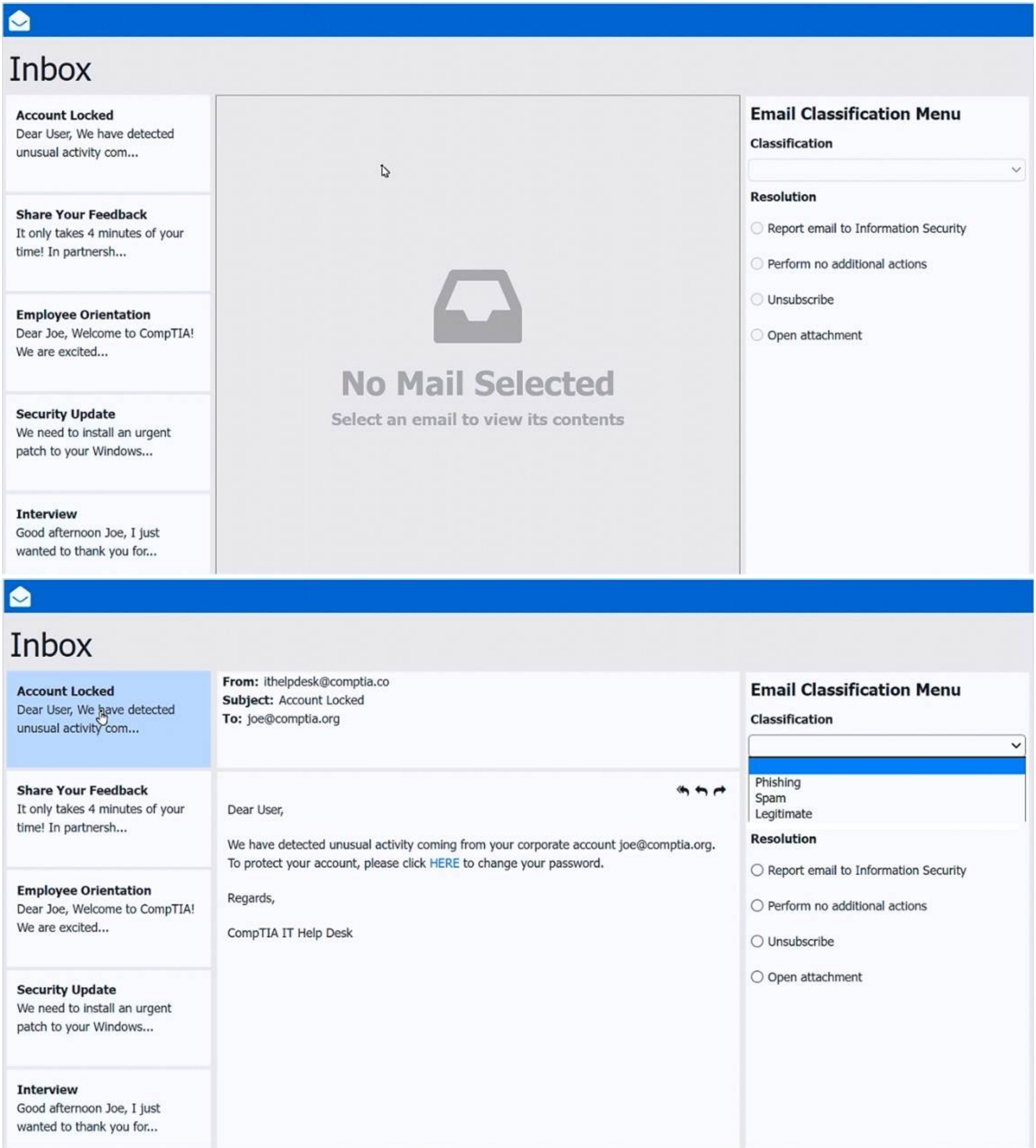
NEW QUESTION 44
An administrator received an email stating that the OS they are currently supporting will no longer be issued security updates and patches. Which of the following is most likely the reason the administrator received this message?

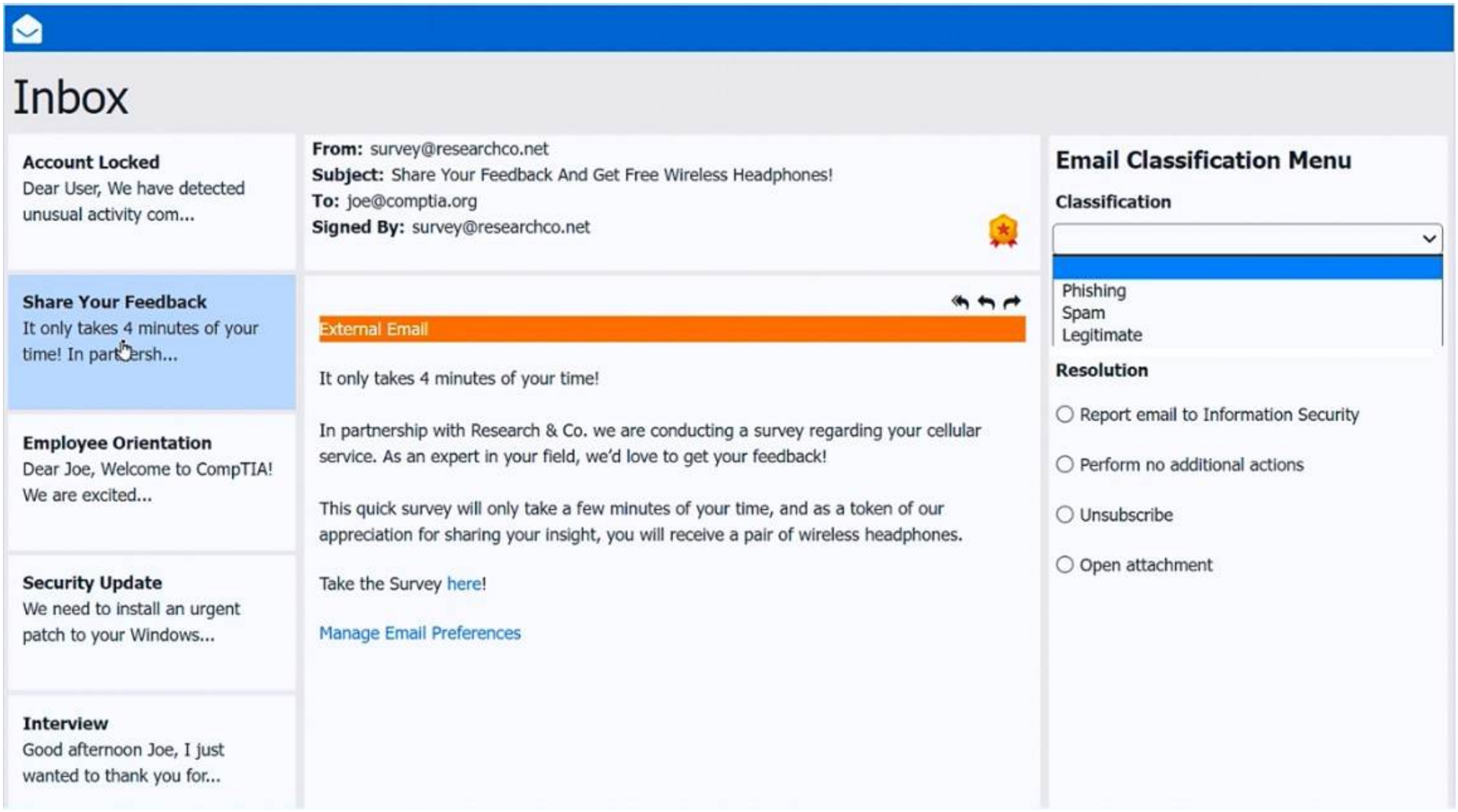
A. Support from the computer's manufacturer is expiring
B. The OS will be considered end of life
C. The built-in security software is being removed from the next OS version
D. A new version of the OS will be released soon

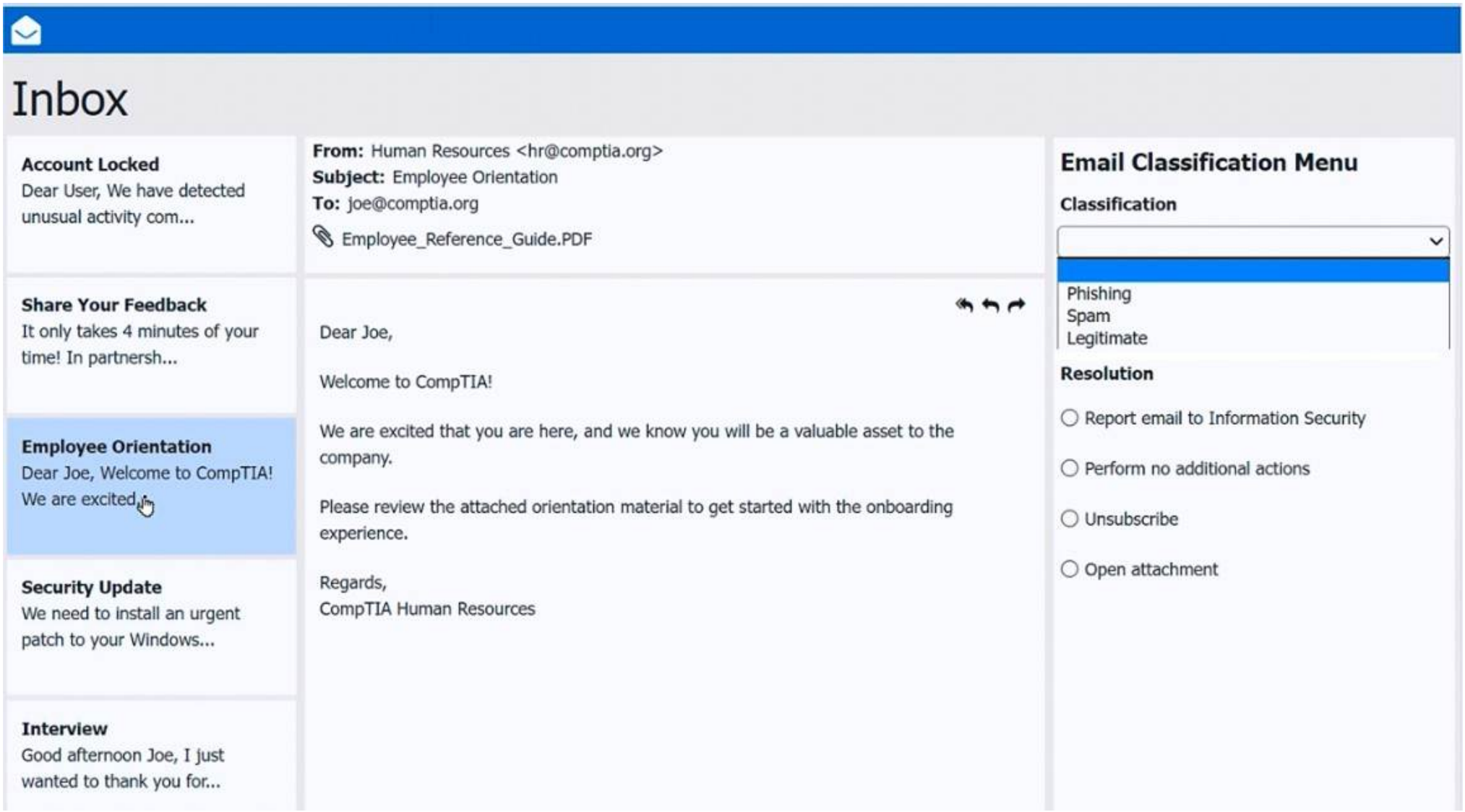
Answer: B

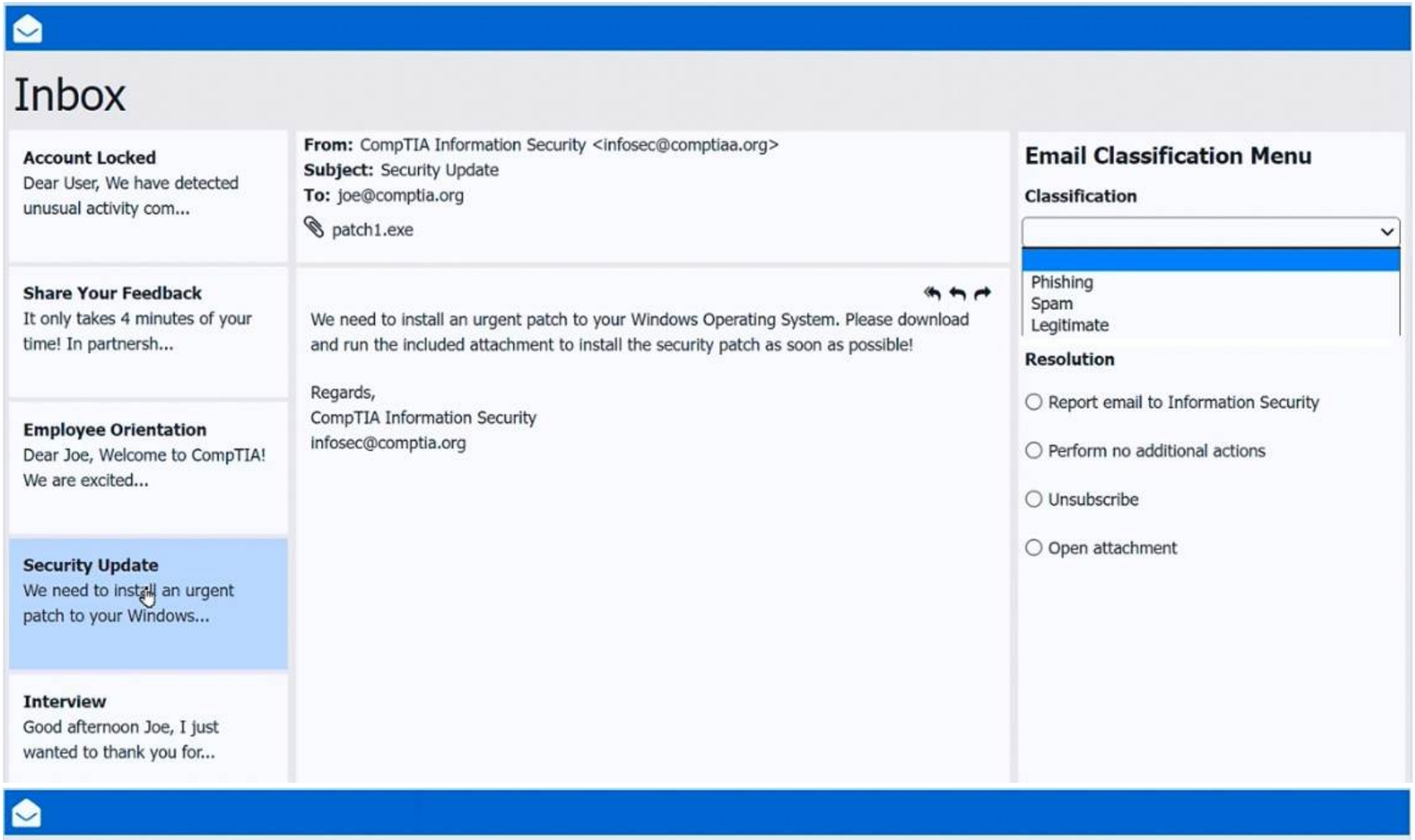
Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Operating systems periodically reach a status known as "end of life" (EOL), at which point the developer (e.g., Microsoft, Apple) ceases to provide security updates, patches, or technical support. When this happens, the OS becomes vulnerable and non-compliant with security best practices, which is why organizations typically receive advance notifications from vendors or support teams.
* A. Manufacturer support expiration only applies to hardware, not OS patching.
* C. Security software may be upgraded or removed, but that does not affect patching the OS itself.
* D. The release of a new version doesn??t automatically stop updates for the current version. Reference:
CompTIA A+ 220-1102 Objective 1.3: Given a scenario, use appropriate Microsoft operating system features and tools.
Study Guide Section: OS lifecycle management and vendor support phases (e.g., EOL)
==========

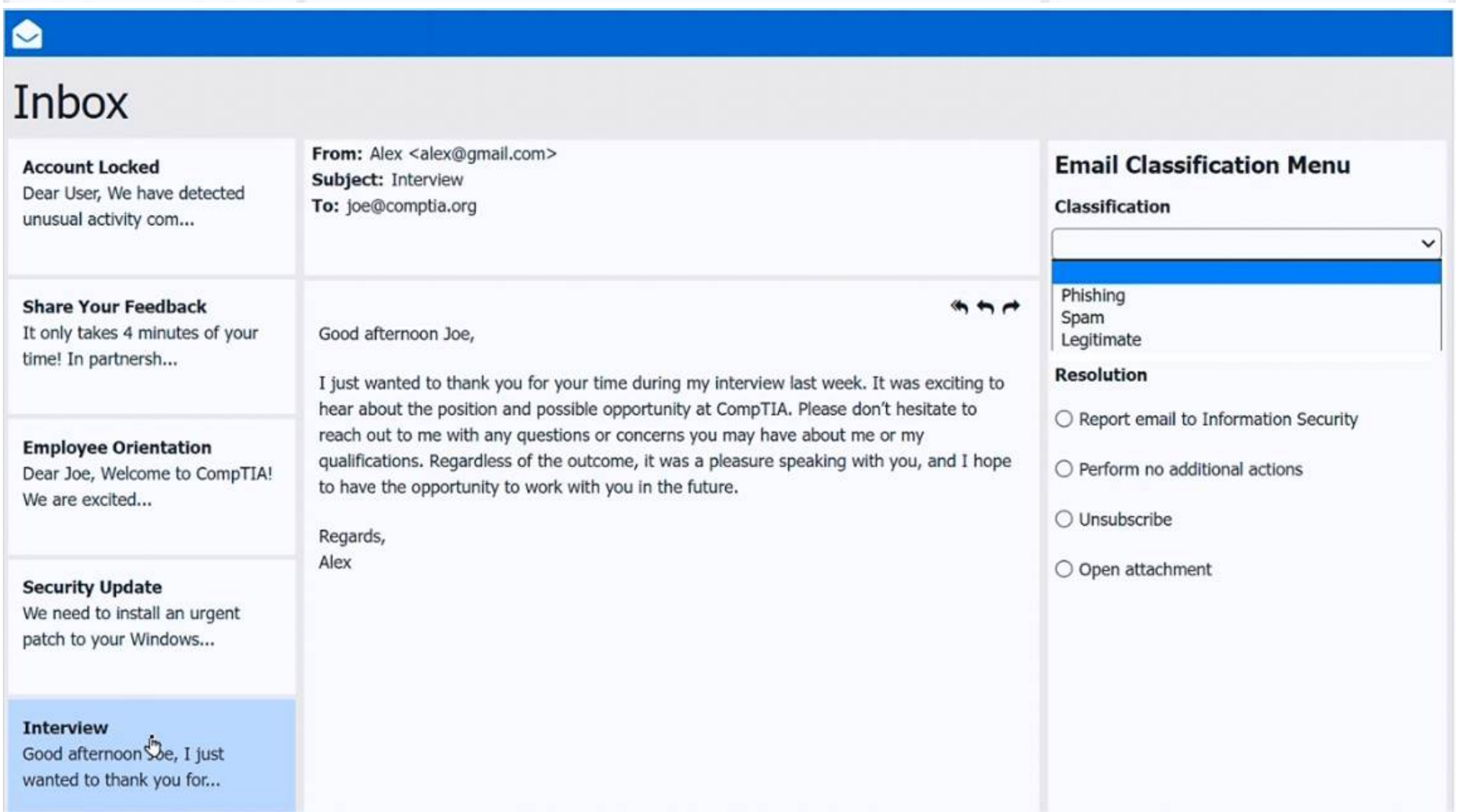
NEW QUESTION 48
SIMULATION
As a corporate technician, you are asked to evaluate several suspect email messages on a client's computer. Corporate policy requires the following:
>All phishing attempts must be reported.
>Future spam emails to users must be prevented. INSTRUCTIONS
Review each email and perform 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
Account Locked
Dear User, We have detected unusual activity com...
Share Your Feedback
It only takes 4 minutes of your time! In partnersh...
Employee Orientation
Dear Joe, Welcome to CompTIA! We are excited...
Security Update
We need to install an urgent patch to your Windows...
Interview
Good afternoon Joe, I just wanted to thank you for...
No Mail Selected
Select an email to view its contents
Email Classification Menu
Classification
Resolution
Report email to Information Security
Perform no additional actions
Unsubscribe
Open attachment
Inbox
Account Locked
Dear User, We have detected unusual activity com...
Share Your Feedback
It only takes 4 minutes of your time! In partnersh...
Employee Orientation
Dear Joe, Welcome to CompTIA! We are excited...
Security Update
We need to install an urgent patch to your Windows...
Interview
Good afternoon Joe, I just wanted to thank you for...
From: ithelpdesk@comptia.co
Subject: Account Locked
To: joe@comptia.org
Dear User,
We have detected unusual activity coming from your corporate account joe@comptia.org.
To protect your account, please click HERE to change your password.
Regards,
CompTIA IT Help Desk
Email Classification Menu
Classification
Phishing
Spam
Legitimate
Resolution
Report email to Information Security
Perform no additional actions
Unsubscribe
Open attachment


Inbox
Account Locked
Dear User, We have detected unusual activity com...
Share Your Feedback
It only takes 4 minutes of your time! In partnersh...
Employee Orientation
Dear Joe, Welcome to CompTIA! We are excited...
Security Update
We need to install an urgent patch to your Windows...
Interview
Good afternoon Joe, I just wanted to thank you for...
From: survey@researchco.net
Subject: Share Your Feedback And Get Free Wireless Headphones!
To: joe@comptia.org
Signed By: survey@researchco.net
External Email
It only takes 4 minutes of your time!
In partnership with Research & Co. we are conducting a survey regarding your cellular service. As an expert in your field, we'd love to get your feedback!
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.
Take the Survey here!
Manage Email Preferences
Email Classification Menu
Classification
Phishing
Spam
Legitimate
Resolution
Report email to Information Security
Perform no additional actions
Unsubscribe
Open attachment


Inbox
Account Locked
Dear User, We have detected unusual activity com...
Share Your Feedback
It only takes 4 minutes of your time! In partnersh...
Employee Orientation
Dear Joe, Welcome to CompTIA! We are excited...
Security Update
We need to install an urgent patch to your Windows...
Interview
Good afternoon Joe, I just wanted to thank you for...
From: Human Resources <hr@comptia.org>
Subject: Employee Orientation
To: joe@comptia.org
Employee_Reference_Guide.PDF
Dear Joe,
Welcome to CompTIA!
We are excited that you are here, and we know you will be a valuable asset to the company.
Please review the attached orientation material to get started with the onboarding experience.
Regards,
CompTIA Human Resources
Email Classification Menu
Classification
Phishing
Spam
Legitimate
Resolution
Report email to Information Security
Perform no additional actions
Unsubscribe
Open attachment





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 52
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 systemstypically 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 57
A user recently installed an application that accesses a database from a local server. When launching the application, it does not populate any information. Which of the following command-line tools is the best to troubleshoot the issue?

A. ipconfig
B. nslookup
C. netstat
D. curl

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The scenario involves an application that should retrieve data from a local database server but is failing to do so. This likely indicates a problem in communication between the application and the database server (such as a network issue, port misconfiguration, or service unavailability). The correct troubleshooting approach involves testing the network/service connectivity between the client and the database.
Let??s examine the options:
? A. ipconfig:This command displays IP configuration details for Windows systems, such as IP address, subnet mask, and default gateway. While useful for diagnosing general networkissues, it does not test service connectivity or the availability of a specific application port/service.
? B. nslookup:Used to query DNS servers to resolve domain names to IP addresses.
However, since the question references a local server (likely accessed via IP or static hostname), DNS is probably not involved. Also, it does not test application/service availability.
? C. netstat:Displays active TCP connections, listening ports, and routing tables. It
helps determine whether the local system is listening for or maintaining any network connections, but it does not initiate a connection to test availability. It??s diagnostic but not interactive for service testing.
? D. curl:This is the most appropriate tool for this scenario. curl is used to test
connectivity to services over protocols like HTTP, HTTPS, FTP, and more. If the application retrieves data via a web interface or API (common in database-driven applications), curl can be used to test if the application can successfully reach and retrieve data from the server. It provides immediate, testable feedback on whether the server and service are available and responsive.
Example usage: curlhttp://localhost:8080/api/data
This command would test whether a local server's application programming interface (API) is available and responding on port 8080.
CompTIA A+ 220-1102 Reference Points:
? Objective 2.4: Given a scenario, use appropriate tools to troubleshoot and support Windows OS issues.
? Objective 3.3: Use appropriate tools to troubleshoot and resolve issues.
? The CompTIA A+ Core 2 study guide references curl as a useful command-line utility for testing connectivity and troubleshooting application access to services.
==========

NEW QUESTION 62
An organization is experiencing an increased number of issues. A technician notices applications that are not installed by default. Users are reporting an increased number of system prompts for software licensing. Which of the following would the security team most likely do to remediate the root cause?

A. Deploy an internal PKI to filter encrypted web traffic.
B. Remove users from the local admin group.
C. Implement stronger controls to block suspicious websites.
D. Enable stricter UAC settings on Windows.

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
If unauthorized or non-standard applications are appearing on systems and users are receiving licensing prompts, it??s likely users are installing software themselves. Removing users from the local administrators group will prevent them from installing software without approval and reduce the likelihood of introducing unapproved or malicious programs.
* A. Deploying a PKI helps with secure communications but doesn??t address user software installation rights.
* C. Blocking suspicious websites is helpful but doesn??t prevent local installations.
* D. Stricter UAC may add prompts but can still be bypassed by admin users. Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast access control methods and user privilege settings.
Study Guide Section: Principle of least privilege and managing local admin rights
==========

NEW QUESTION 67
A technician needs to provide remote support for a legacy Linux-based operating system from their Windows laptop. The solution needs to allow the technician to see what the user is doing and provide the ability to interact with the user's session. Which of the following remote access technologies would support the use

case?

A. VPN
B. VNC
C. SSH
D. RDP

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The correct answer isVNC (Virtual Network Computing). VNC is a graphical desktop- sharing system that uses the Remote Frame Buffer protocol (RFB) to remotely control another computer. It is platform-independent and widely supported on Linux, which makes it ideal for providinginteractive remote support for a Linux-based operating system. It allows the technician not only to view the remote desktop session but also tocontrol it, fulfilling the need to see and interact with the user??s session.
? A. VPN(Virtual Private Network) creates a secure tunnel to a network but doesnot
provide desktop sharing or session controlby itself.
? C. SSH(Secure Shell) provides secure command-line access to Unix/Linux systems but does not offergraphical desktop interaction, which is a requirement in this case.
? D. RDP(Remote Desktop Protocol) is primarily a Microsoft protocol, and although it can be made to work on Linux, it isnot natively supported on legacy Linux systems, and thusless suitablethan VNC in this scenario.
CompTIA A+ 220-1102 Core 2 Objective Reference:
Objective 1.8 – Given a scenario, use features and tools of the operating system. Under this objective, candidates are expected to be familiar with remote access technologies, includingRDP, SSH, and VNC, and understand their appropriate uses and limitations on different platforms such as Windows and Linux.

NEW QUESTION 68
A technician is setting up a surveillance system for a customer. The customer wants access to the system's web interface on the LAN via the system??s IP address. Which of the following should the technician use to prevent external log-in attempts from the internet?

A. Port mapping
B. Subnetting
C. Static IP
D. Content filtering

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
To prevent external access, the technician should avoid exposing the surveillance system??s port to the public internet. Port mapping (also known as port forwarding) is the method used to control which internal devices and ports are accessible from the outside. By not configuring port forwarding for the device, external login attempts are effectively blocked.
* B. Subnetting organizes IP addresses but doesn't directly restrict access.
* C. A static IP ensures consistent addressing but does not secure access.
* D. Content filtering is used to restrict web content, not to block access to a web interface. Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast security measures and tools. Study Guide Section: SOHO router security — port forwarding and blocking external
access
==========

NEW QUESTION 71
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 74
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 78
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 81
A user reports some single sign-on errors to a help desk technician. Currently, the user is able tosign in to the company's application portal but cannot access a specific SaaS-based tool. Which of the following would the technician most likely suggest as a next step?

A. Reenroll the user's mobile device to be used as an MFA token
B. Use a private browsing window to avoid local session conflicts
C. Bypass single sign-on by directly authenticating to the application
D. Reset the device being used to factory defaults

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
SSO issues are often related to cached session data, cookies, or browser artifacts. The fact that the user can access the company portal but not one specific SaaS tool suggests a session or token problem. Using a private/incognito browsing window allows a clean session to be initiated, which often resolves SSO conflicts.
* A. Reenrolling MFA is not related unless access issues stem from failed multifactor authentication.
* C. Bypassing SSO may not be possible depending on the SaaS tool and company policies.
* D. Factory resetting a device is a last resort and unnecessary in this case. Reference:
CompTIA A+ 220-1102 Objective 3.3: Troubleshoot common software, application, and OS security issues.
Study Guide Section: Troubleshooting login and authentication issues, especially with SSO services.
==========

NEW QUESTION 84
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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