Comptia

(220-1102)

CompTIA A+ Certification Exam

Total: **668 Questions**

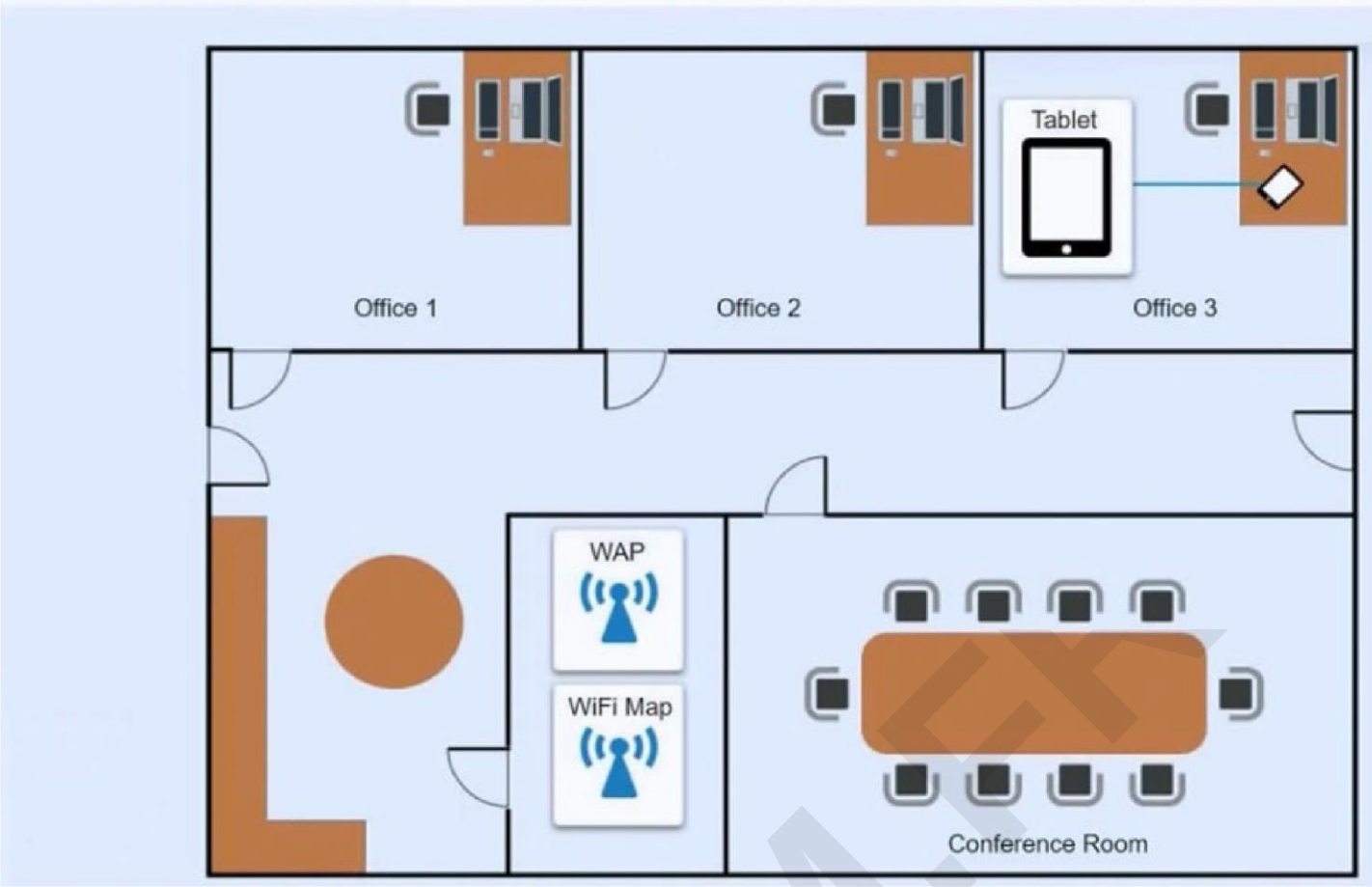
Link:

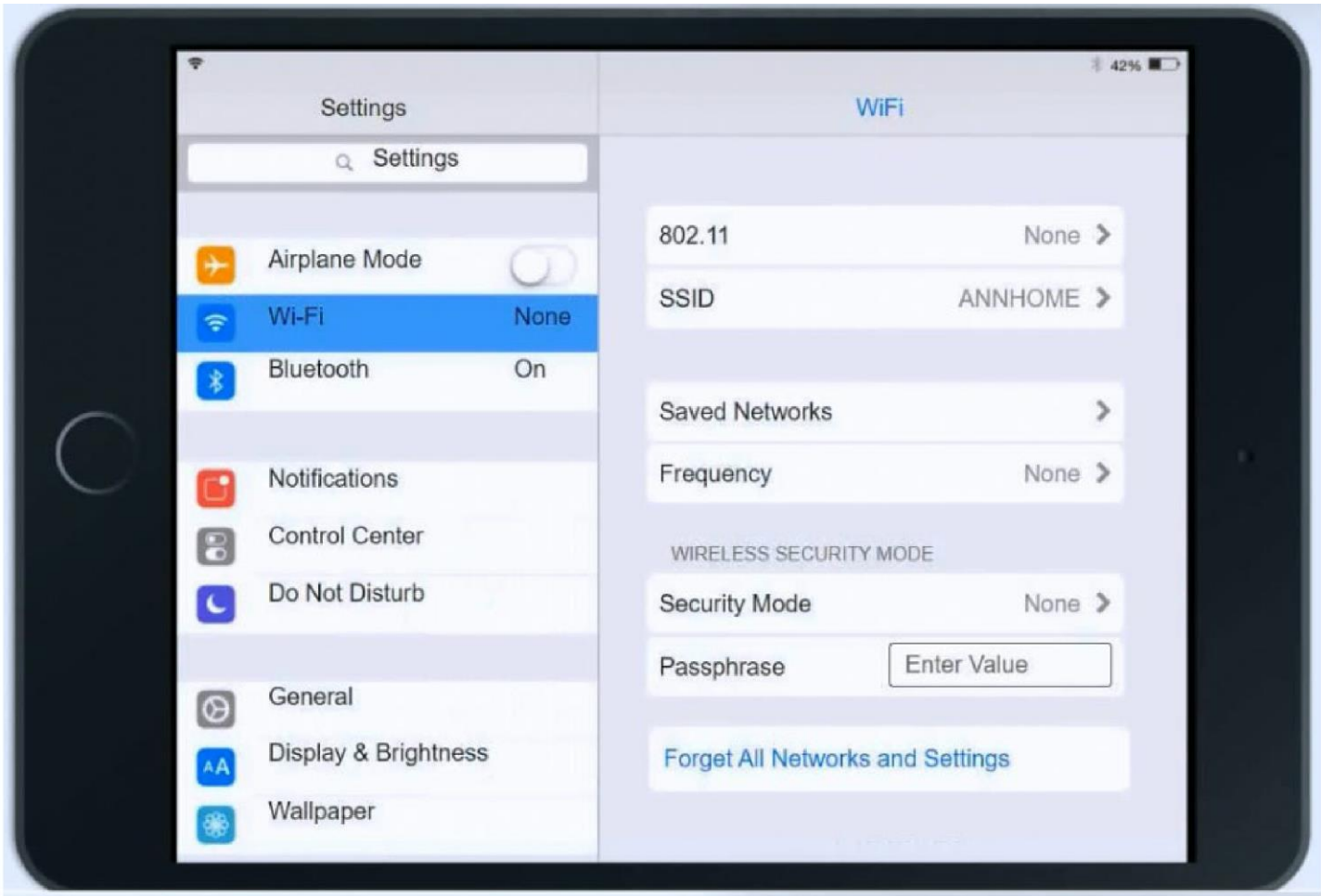
Question: 1

SIMULATION -
Ann, a CEO, has purchased a new consumer-class tablet for personal use, but she is unable to connect to the wireless network. Other users have reported that their personal devices are connecting without issues. She has asked you to assist with getting the device online without adjusting her home WiFi configuration.

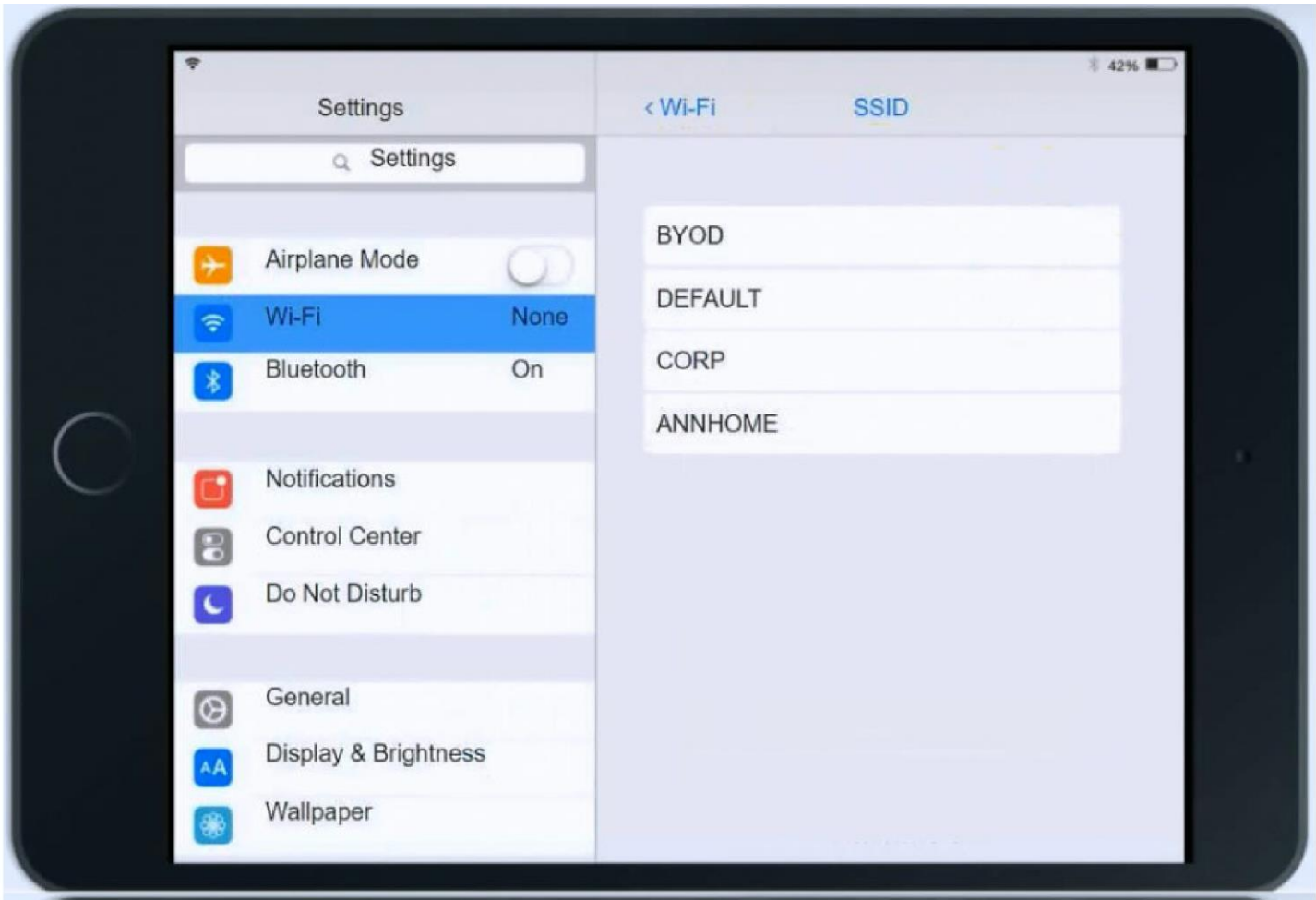
INSTRUCTIONS -
Review the network diagrams and device configurations to determine the cause of the problem and resolve any discovered issues.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Mobile Device Configuration

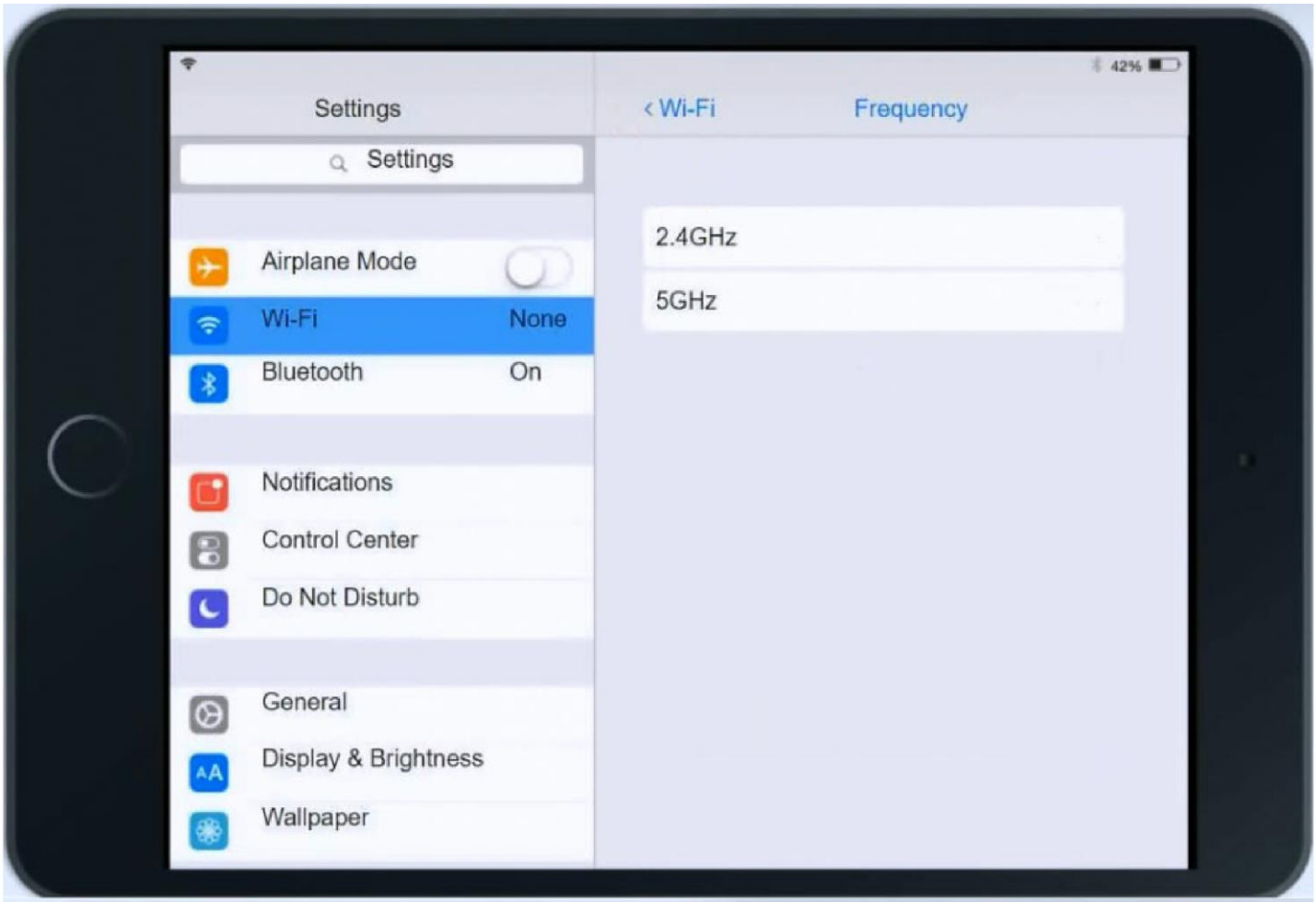



Settings
WiFi
Settings
Airplane Mode
Wi-Fi None
Bluetooth On
Notifications
Control Center
Do Not Disturb
General
Display & Brightness
Wallpaper
802.11 None
SSID ANNHOME
Saved Networks
Frequency None
WIRELESS SECURITY MODE
Security Mode None
Passphrase Enter Value
Forget All Networks and Settings

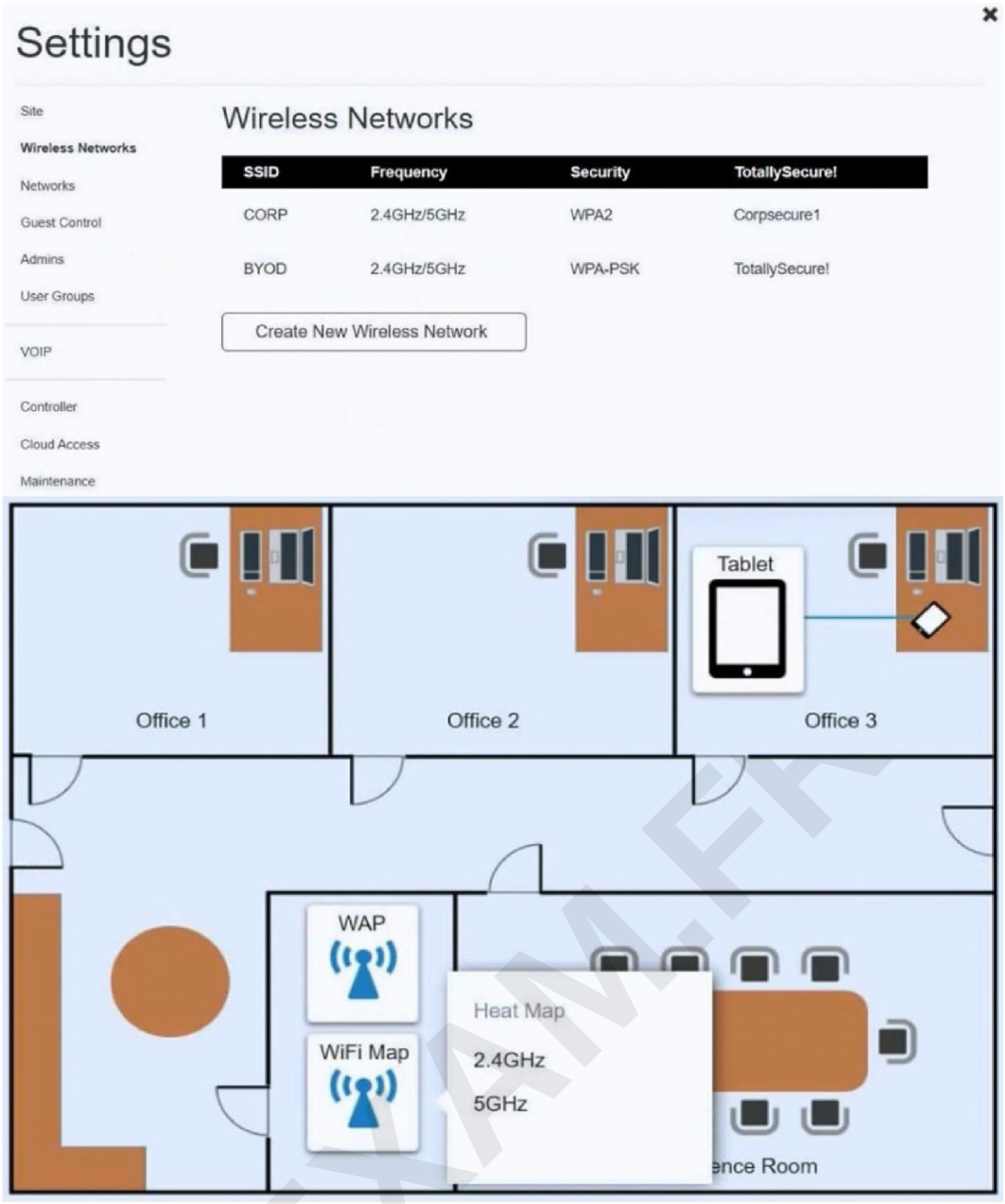

Settings
Wi-Fi 802.11
Settings
Airplane Mode
Wi-Fi None
Bluetooth On
Notifications
Control Center
Do Not Disturb
General
Display & Brightness
Wallpaper
b/g
a
ac


42%
Settings
Wi-Fi
SSID
Settings
Airplane Mode
Wi-Fi
None
Bluetooth
On
Notifications
Control Center
Do Not Disturb
General
Display & Brightness
Wallpaper
BYOD
DEFAULT
CORP
ANNHOME


42%
Settings
Wi-Fi
Saved Networks
Settings
Airplane Mode
Wi-Fi
None
Bluetooth
On
Notifications
Control Center
Do Not Disturb
General
Display & Brightness
Wallpaper
ANNHOME
COFFEESHOPPE
PAMSHOUSE


42%
Settings
Settings
Airplane Mode
Wi-Fi None
Bluetooth On
Notifications
Control Center
Do Not Disturb
General
Display & Brightness
Wallpaper
‹ Wi-Fi
Frequency
2.4GHz
5GHz


42%
Settings
Settings
Airplane Mode
Wi-Fi None
Bluetooth On
Notifications
Control Center
Do Not Disturb
General
Display & Brightness
Wallpaper
‹ Wi-Fi
Security Mode
OPEN
WEP
WPA
WPA2



Answer:

See explanation below.

Explanation:
Click on 802.11 and Select ac -

Click on SSID and select BYOD -
Click on Frequency and select 5GHz
At Wireless Security Mode, Click on Security Mode

Select the WPA and the password should be set to TotallySecure!

Question: 2

A help desk team lead contacts a systems administrator because the technicians are unable to log in to a Linux server that is used to access tools. When the administrator tries to use remote desktop to log in to the server, the administrator sees the GUI is crashing. Which of the following methods can the administrator use to troubleshoot the server effectively?

A. SFTP
B. SSH
C. VNC
D. MSRA

Answer: B

Explanation:

The correct answer is **B. SSH**. Here's why:

The problem states the GUI is crashing and technicians can't log in. This indicates a potential issue with the graphical environment or resource constraints affecting it. In such scenarios, a command-line interface (CLI) becomes invaluable.

SSH (Secure Shell) provides a secure and encrypted command-line access to the server. It operates independently of the GUI. This allows the administrator to bypass the failing graphical interface and directly interact with the server's operating system to diagnose and fix the issue. They can check system logs, resource utilization (CPU, memory), running processes, and network connectivity using command-line tools.

SFTP (Secure File Transfer Protocol) is mainly for secure file transfer, not direct server administration or troubleshooting in a scenario where login is failing due to GUI issues.

VNC (Virtual Network Computing), like remote desktop, relies on the GUI. If the GUI is crashing, VNC will likely be unusable or unreliable.

MSRA (Microsoft Remote Assistance) is a Microsoft-specific remote support tool, which is unlikely to be directly applicable to a Linux server. It also relies on a GUI which is failing in this scenario.

SSH is the most effective initial approach because it offers a stable and reliable way to access the server's underlying system when the GUI is malfunctioning.

For further research:

SSH: https://www.ssh.com/ssh/
Troubleshooting Linux servers: https://www.digitalocean.com/community/tutorials/how-to-troubleshoot-common-linux-server-issues

Question: 3

A company wants to remove information from past users' hard drives in order to reuse the hard drives. Which of the following is the MOST secure method?

A. Reinstalling Windows
B. Performing a quick format
C. Using disk-wiping software
D. Deleting all files from command-line interface:

Answer: C

Explanation:

Here's a detailed justification for why using disk-wiping software (Option C) is the most secure method for removing information from hard drives before reuse, compared to the other options.

Reinstalling Windows (Option A) might seem like a thorough approach, but it typically only overwrites the operating system files and user profiles. Data from previous users might still be recoverable from unallocated space on the drive using specialized data recovery tools. A quick format (Option B) simply removes the file system's index, making the data invisible to the operating system. However, the underlying data remains intact and is easily recoverable using readily available tools. Deleting all files from the command-line interface (Option D) is also inadequate. It only removes the pointers to the files in the file system, leaving the data itself untouched on the disk.

Disk-wiping software, on the other hand, employs a much more rigorous process. It overwrites the entire hard drive, including all sectors, multiple times with patterns of zeros, ones, or random data. This makes it extremely difficult, if not impossible, for data recovery tools to retrieve any of the original information.

Different disk-wiping standards exist, such as DoD 5220.22-M and Gutmann, which define the number of passes and the complexity of the overwriting patterns. The more passes performed and the more complex the patterns, the more secure the data sanitization process. Choosing a reputable disk-wiping software that adheres to a recognized standard is crucial for ensuring effective data removal. This ensures the hard drive is sanitized to a level that meets security and compliance requirements, making it safe for reuse.While physically destroying the hard drive is the most secure method, disk wiping offers a practical and cost-effective alternative when reuse is desired.

Here are a few authoritative links for further research:

NIST Guidelines for Media Sanitization:https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf (This document provides comprehensive guidance on data sanitization methods.)
Disk Erasure Methods Explained:https://www.ibm.com/docs/en/storage-protect/8.1.0?topic=devices-disk-erasure-methods

Question: 4

A user is having phone issues after installing a new application that claims to optimize performance. The user downloaded the application directly from the vendor's website and is now experiencing high network utilization and is receiving repeated security warnings. Which of the following should the technician perform FIRST to mitigate the issue?

A. Reset the phone to factory settings.
B. Uninstall the fraudulent application.
C. Increase the data plan limits.
D. Disable the mobile hotspot.

Answer: B

Explanation:

The most appropriate first action is to uninstall the fraudulent application. The user's issues (high network utilization, security warnings) directly correlate with the installation of the new application. This strongly suggests the application is the root cause. Uninstalling it will likely eliminate the immediate problem if the application is indeed malicious or poorly coded. This approach addresses the problem's apparent source quickly and directly.

Resetting the phone to factory settings (Option A) is a more drastic step and should be reserved for situations where the problem persists after simpler solutions are tried. It would erase all user data and settings, causing inconvenience. Increasing data plan limits (Option C) is irrelevant as it doesn't address the underlying issue of the application's behavior. Disabling the mobile hotspot (Option D) might reduce network usage, but it doesn't fix the problem's source and might not be applicable if a hotspot is not in use.

Removing the suspected application provides the quickest path to restoring normal phone functionality and security. If the issues stop after removal, it confirms the application was the cause. Further investigation can then be done on the vendor and application if necessary.

For more information about mobile security threats and application security:

OWASP Mobile Security Project: https://owasp.org/www-project-mobile-security/ NIST Guidelines on Managing the Security Risks of Mobile Devices: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-124r1.pdf

Question: 5

A change advisory board just approved a change request. Which of the following is the MOST likely next step in the change process?

A. End user acceptance
B. Perform risk analysis
C. Communicate to stakeholders
D. Sandbox testing

Answer: A

Explanation:

The most likely next step after a change advisory board (CAB) approves a change request is **End user acceptance (A)**.

Here's why: The change management process typically follows a sequential flow. After the CAB's approval, the change needs to be validated to ensure it meets the intended requirements and user needs before being fully implemented into the production environment. End-user acceptance testing (UAT) serves this critical purpose. It involves actual users testing the changed system or service in a controlled environment to confirm its functionality and usability.

While risk analysis (B) is a crucial step, it ideally occurs before CAB approval to inform the decision-making process. Sandbox testing (D) is part of the implementation and testing phase and should be performed before user acceptance to identify and address any technical issues before users interact with the change.

Communication to stakeholders (C) is an ongoing process throughout the change lifecycle, but it isn't necessarily the immediately following step. The stakeholders need to know what to communicate; thus, end-user acceptance needs to happen first. If the change fails to meet user expectations during UAT, further modifications may be required, potentially leading to another iteration before full implementation.

Successful UAT signifies that the change is ready for deployment. If UAT reveals issues, the change is reverted or modified and re-submitted for further review, testing, and UAT. After successful UAT, the change is considered ready for wider implementation and deployment.

Therefore, End user acceptance is a pivotal step after CAB approval in guaranteeing that the change delivers the expected value and meets the needs of the user community.

Reference:

ITIL 4 Foundation Study Guide (For understanding ITIL change management practices)

Question: 6

A user calls the help desk to report that none of the files on a PC will open. The user also indicates a program on the desktop is requesting payment in exchange for file access. A technician verifies the user's PC is infected with ransomware. Which of the following should the technician do FIRST?

A. Scan and remove the malware.
B. Schedule automated malware scans.
C. Quarantine the system.
D. Disable System Restore.

Answer: C

Explanation:

The correct first step when dealing with a ransomware infection is to **C. Quarantine the system.**

Immediately isolating the infected system prevents the ransomware from spreading to other devices on the network. Ransomware is designed to encrypt files and potentially propagate laterally, so containment is paramount. Scanning and removing malware (option A) is important, but not the initial action. Quarantine takes precedence to stop further damage. Scheduling automated malware scans (option B) is a good preventative measure for the future, but does not address the immediate threat. Disabling System Restore (option D) is a valid consideration later in the remediation process (as ransomware can sometimes infect restore points), but it's not the top priority in the first moments of detection. Prioritizing quarantine minimizes the blast radius and allows for safe investigation and remediation. Post-quarantine, the technician can then focus on analysis, removal, and potentially restoration of files (if backups are available). Without prompt isolation, the ransomware can encrypt more data and spread to other systems.

Further reading:

SANS Institute: https://www.sans.org/ (Search for "ransomware incident response")
NIST Computer Security Resource Center: https://csrc.nist.gov/ (Search for "ransomware")
CISA (Cybersecurity and Infrastructure Security Agency): https://www.cisa.gov/ (Search for "ransomware guide")

Question: 7

A company is issuing smartphone to employees and needs to ensure data is secure if the devices are lost or stolen. Which of the following provides the BEST solution?

A. Anti-malware
B. Remote wipe
C. Locator applications
D. Screen lock

Answer: B

Explanation:

The best solution for securing data on company-issued smartphones in case of loss or theft is remote wipe. Here's why:

While anti-malware (A) is important for general security, it doesn't address data protection after a device is lost or stolen. Locator applications (C) can help find the device, but finding it doesn't guarantee data security.
Screen locks (D) provide a basic layer of security, but can be bypassed, especially with sophisticated tools.

Remote wipe (B) allows the company to remotely erase all data from the device, preventing unauthorized access to sensitive information. This ensures that even if the device falls into the wrong hands, confidential company data, including emails, documents, and credentials, will be irretrievably deleted. This option is particularly effective as a last resort.

Mobile Device Management (MDM) solutions often include remote wipe functionality. Implementing an MDM system alongside a remote wipe policy allows administrators to centrally manage and secure all company-owned devices. This provides comprehensive control over the device and its data. Furthermore, a well-defined remote wipe procedure should be part of the company's overall data security and incident response plan. This allows the company to quickly react and protect data following the loss or theft of any corporate device.

Here are some links for further research:

NIST Guidelines on Mobile Device Security:
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-124r1.pdf
Microsoft Intune Remote Wipe:https://learn.microsoft.com/en-us/mem/intune/remote-actions/devices-wipe

Question: 8

A user reports seeing random, seemingly non-malicious advertisement notifications in the Windows 10 Action Center. The notifications indicate the advertisements are coming from a web browser. Which of the following is the BEST solution for a technician to implement?

A. Disable the browser from sending notifications to the Action Center.
B. Run a full antivirus scan on the computer.
C. Disable all Action Center notifications.
D. Move specific site notifications from Allowed to Block.

Answer: D

Explanation:

The best solution to stop advertisement notifications from a web browser in the Windows 10 Action Center is to move specific site notifications from Allowed to Block. Here's why:

Targeted Solution: This approach directly addresses the source of the problem. Instead of broadly disabling all notifications or running a scan that might not address the root cause, it focuses on the websites sending unwanted ads.

Preserves Functionality: Disabling the browser from sending notifications (Option A) would stop all notifications, including potentially useful ones. Moving specific sites to the Block list allows wanted notifications to come through while only blocking unwanted ads. Option C (disable all Action Center notifications) completely removes the benefit of the Action Center.

Virus Scan Inappropriate: While a full antivirus scan (Option B) is a good general troubleshooting step, the user reported the ads as "seemingly non-malicious." This suggests the issue is not malware, but rather unwanted permission to send notifications.

Notification Settings: Modern browsers allow granular control over website notifications. Users can grant or deny permission for websites to send notifications. The Action Center then displays these notifications based on the permissions set in the browser.

User Control: Moving sites from Allowed to Block gives the user the power to manage which sites are permitted to send notifications. This is empowering and addresses the underlying problem without overly restricting functionality.

Action Center Functionality: The Action Center is a useful feature for receiving important updates and alerts. Completely disabling it would diminish the user's experience.

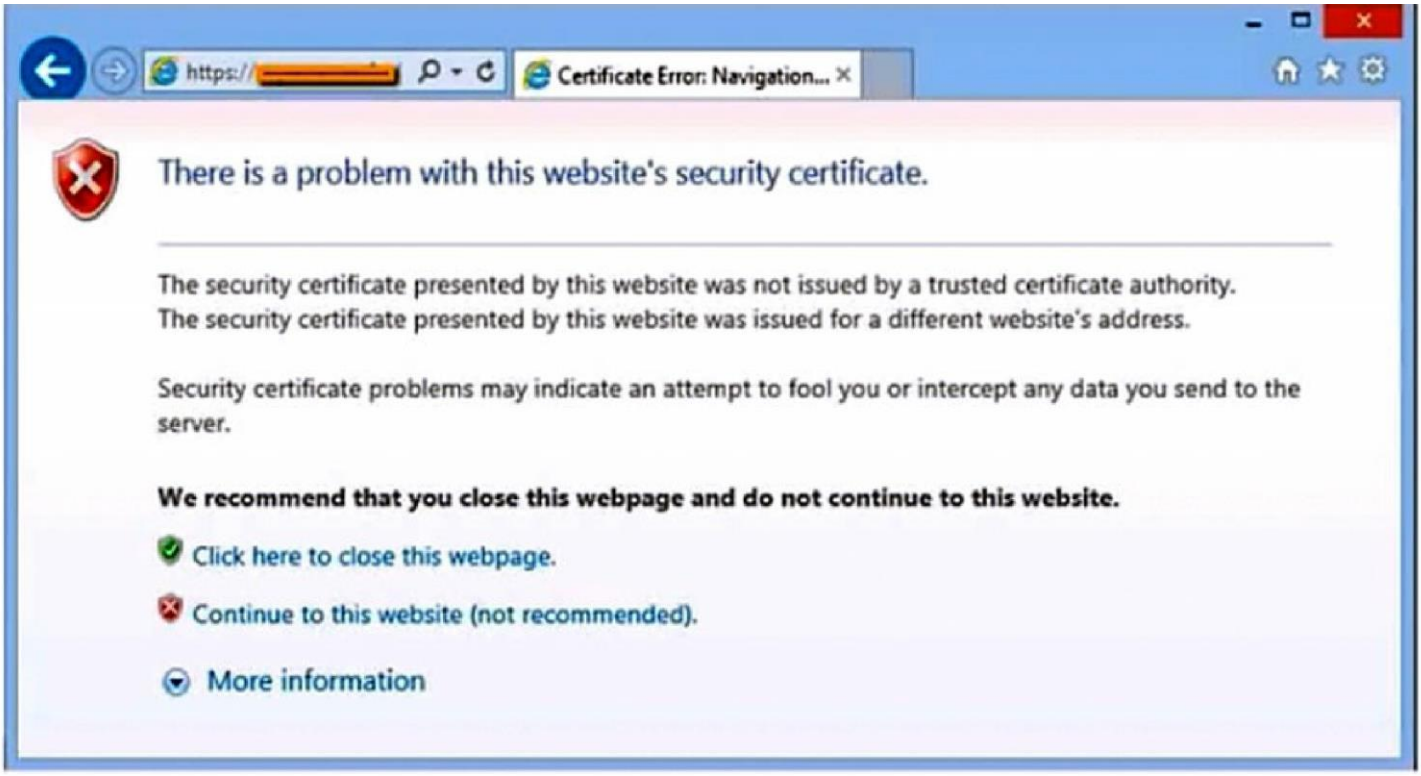
Therefore, by moving specific site notifications from Allowed to Block, the technician can effectively eliminate the unwanted ads while preserving the functionality of the Action Center and the user's ability to receive important notifications from other sources.

Relevant Documentation:

Manage website notifications in Microsoft Edge:https://support.microsoft.com/en-us/microsoft-edge/manage-website-notifications-in-microsoft-edge-0c555998-c7d2-4796-94fa-5cf592f14212 **Change your notification settings in Windows:**https://support.microsoft.com/en-us/windows/change-notification-settings-in-windows-896522a7-1394-4225-bc97-54db62a901c9

Question: 9

After clicking on a link in an email, a Chief Financial Officer (CFO) received the following error:



The CFO then reported the incident to a technician. The link is purportedly to the organization's bank. Which of the following should the technician perform FIRST?

A. Update the browser's CRLs.
B. File a trouble ticket with the bank.
C. Contact the ISP to report the CFO's concern.
D. Instruct the CFO to exit the browser.

Answer: D

Explanation:

The first step the technician should take is to instruct the CFO to exit the browser immediately. Option D is the correct answer.

The error message suggests that the link the CFO clicked on may have led to a malicious website or a phishing attempt. In such cases, it is important to immediately close the browser to prevent any potential harm to the computer or the organization's network.

After the browser is closed, the technician can proceed with further investigation and steps to address the issue, such as updating the browser's Certificate Revocation Lists (CRLs) (Option A) to ensure that the browser can detect and block certificates that have been revoked by the certificate authority. However, this step should only be taken after the immediate threat has been mitigated.

Question: 10

A help desk technician is troubleshooting a workstation in a SOHO environment that is running above normal system baselines. The technician discovers an unknown executable with a random string name running on the system. The technician terminates the process, and the system returns to normal operation. The technician thinks the issue was an infected file, but the antivirus is not detecting a threat. The technician is concerned other machines may be infected with this unknown virus. Which of the following is the MOST effective way to check other machines on the network for this unknown threat?

A. Run a startup script that removes files by name.
B. Provide a sample to the antivirus vendor.

C. Manually check each machine.

D. Monitor outbound network traffic.

Answer: C

Explanation:

The most effective immediate course of action is to manually check each machine. Here's why:

Unidentified Threat: The antivirus didn't detect the threat, meaning it's a new or highly customized malware. Automated scripts (option A) or monitoring outbound traffic (option D) are unlikely to be immediately effective because the specific indicators of compromise (IOCs) are unknown.

Proactive Identification: Manually checking allows for a direct visual inspection of processes and installed programs, enabling the technician to identify the rogue executable by its name or behavior.

Containment: Rapid identification and manual removal of the threat from all affected machines can prevent further spread within the SOHO network.

Sample Submission: While providing a sample to the antivirus vendor (option B) is a crucial step, it doesn't address the immediate need to remove the existing infection. The vendor will need time to analyze the sample and create a signature update, and meanwhile, the threat remains active.

Time Sensitivity: In a SOHO environment with potentially limited security resources, a quick and targeted manual check is more practical and efficient than relying solely on signature updates or broad network monitoring.

Therefore, option C (Manually check each machine) offers the most immediate and direct approach to identifying and containing the unknown threat on other machines. Once the threat is contained, then the antivirus vendor should be notified and the network should be monitored.

Supporting Links:

While there isn't one specific link to directly support this, the following resources discuss malware incident response and the importance of identifying and containing threats:

SANS Institute - Incident Handling Step-by-Step:https://www.sans.org/reading-room/whitepapers/incident/incident-handling-step-step-33901
NIST - Computer Security Incident Handling Guide:https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

These links emphasize the importance of identification, containment, and eradication steps in a security incident, which aligns with the manual check approach for an unknown threat.

Question: 11

A laptop user is visually impaired and requires a different cursor color. Which of the following OS utilities is used to change the color of the cursor?

A. Keyboard

B. Touch pad

C. Ease of Access Center

D. Display settings

Answer: C

Explanation:

The correct answer is C, Ease of Access Center (now known as Accessibility settings in modern Windows versions). This is because the Ease of Access Center is specifically designed within the operating system to provide tools and configurations that enhance usability for individuals with various disabilities, including visual impairments. Changing the cursor color is a common requirement for visually impaired users, as it improves cursor visibility against different backgrounds.

Options A (Keyboard), B (Touchpad), and D (Display settings) offer configuration options, but they do not primarily focus on accessibility for impaired users. The Keyboard settings deal with keyboard functionality, the Touchpad settings configure touchpad behavior, and the Display settings primarily address resolution, screen orientation, and multiple monitor configurations.

The Ease of Access Center groups all accessibility-related settings in one place, making it easy for users to find and customize settings like screen narrators, magnifiers, high contrast themes, and importantly, pointer/cursor size and color. Display settings might allow for basic changes to size, but the Ease of Access Center is the dedicated area for accessibility. The focus on centralization of all these tools is crucial for discoverability and ease of use for those who need them. Modern operating systems such as Windows 10/11 have evolved this into dedicated Accessibility settings, improving the organization and feature set. The term Ease of Access Center is somewhat outdated now, with the relevant settings being directly in the Settings app under Accessibility.Therefore, the Ease of Access Center (or Accessibility settings) is the correct answer due to its specific function in providing accessibility options, including the ability to change the cursor color for visually impaired users.

Further Research:

Microsoft Accessibility:https://www.microsoft.com/en-us/accessibility
Windows 10 Accessibility Features:https://support.microsoft.com/en-us/windows/windows-accessibility-features-02248003-d307-d361-d510-1256034737a8

Question: 12

A manager reports that staff members often forget the passwords to their mobile devices and applications. Which of the following should the systems administrator do to reduce the number of help desk tickets submitted?

A. Enable multifactor authentication.
B. Increase the failed log-in threshold.
C. Remove complex password requirements.
D. Implement a single sign-on with biometrics.

Answer: D

Explanation:

The best solution to reduce password-related help desk tickets is to implement a single sign-on (SSO) system with biometrics (D). Here's why:

SSO allows users to authenticate once and then gain access to multiple applications and devices, reducing the need to remember numerous passwords. https://www.okta.com/what-is/single-sign-on/

Coupling SSO with biometrics, such as fingerprint or facial recognition, provides a secure and user-friendly authentication method. Biometrics are harder to forget than passwords, inherently addressing the problem of users forgetting their credentials. https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-

framework

Option A, enabling multifactor authentication (MFA), adds security but doesn't address password amnesia. MFA can even increase password fatigue if not implemented carefully alongside a password management solution.

Option B, increasing the failed log-in threshold, is a poor security practice and makes devices vulnerable to brute-force attacks. It doesn't solve the underlying issue of forgotten passwords.

Option C, removing complex password requirements, also weakens security. While simpler passwords might be easier to remember, they are more susceptible to compromise. It's a trade-off that increases risk. SSO with biometrics offers a secure yet user-friendly alternative that minimizes password-related issues without sacrificing security. This streamlines access and significantly reduces password-related help desk requests. Cloud-based SSO solutions are common and offer scalability and ease of management.

Question: 13

A technician suspects a rootkit has been installed and needs to be removed. Which of the following would BEST resolve the issue?

A. Application updates
B. Anti-malware software
C. OS reinstallation
D. File restore

Answer: C

Explanation:

The best way to resolve a rootkit infection is typically an OS reinstallation. Rootkits are designed to deeply embed themselves within the operating system, often modifying core system files and processes. This makes them incredibly difficult to detect and remove using standard anti-malware software.

While anti-malware software (option B) can sometimes detect and remove rootkits, it is not always reliable. Rootkits often employ techniques to evade detection, making them persistent even after running security scans. Application updates (option A) are irrelevant to rootkit removal. File restore (option D) wouldn't address the underlying infection, as the restored files would likely be reinfected.

A clean OS reinstallation ensures that all potentially infected files and system components are replaced with clean, uninfected versions. This effectively eliminates the rootkit's presence and restores the system to a trusted state. It is the most reliable method to eliminate a rootkit infection, offering a clean slate. Other methods may leave remnants of the rootkit, allowing it to potentially re-emerge. A full reinstall is the most comprehensive solution.

Authoritative Links:

SANS Institute on Rootkits: https://www.sans.org/reading-room/whitepapers/malicious/rootkits-overview-33524
Microsoft on Rootkits: https://learn.microsoft.com/en-us/windows/security/threat-protection/intelligence/rootkits

Question: 14

A technician is setting up a SOHO wireless router. The router is about ten years old. The customer would like the most secure wireless network possible. Which of the following should the technician configure?

A. WPA2 with TKIP
B. WPA2 with AES
C. WPA3 with AES-256
D. WPA3 with AES-128

Answer: B

Explanation:

Here's a detailed justification for why option B, "WPA2 with AES," is the best choice for securing a ten-year-old SOHO wireless router, and why the other options are less suitable:

The customer's primary requirement is the most secure wireless network possible, given the router's age. Wireless security protocols have evolved over time, with newer standards offering stronger protection against attacks.

WPA2 with AES (Advanced Encryption Standard): WPA2 is a significant improvement over its predecessor, WEP, and offers a reasonable level of security when paired with AES. AES is a robust encryption algorithm that is widely considered secure and resistant to many common wireless attacks. Many older devices support WPA2/AES, making it a likely option for a ten-year-old router.

WPA2 with TKIP (Temporal Key Integrity Protocol): TKIP was designed as a stopgap measure to improve WEP security without requiring hardware upgrades. It has known vulnerabilities and is considered less secure than AES. Although WPA2 is used, the weakness of TKIP undermines overall security.

WPA3 with AES-256 or AES-128: WPA3 is the latest wireless security standard and offers the best protection against modern attacks. However, given the router's age (ten years old), it is highly unlikely to support WPA3. WPA3 requires newer hardware and firmware capabilities that older devices typically lack. Even if the router had an AES chip, the firmware would not be designed to use the protocol.

Therefore, selecting WPA2 with AES provides a balance between security and compatibility for a ten-year-old router. It offers a significantly stronger encryption method than WPA/TKIP and is more likely to be supported by the router's hardware and firmware than WPA3.

Authoritative Links:

Wi-Fi Alliance - WPA3: https://www.wi-fi.org/discover-wi-fi/security
National Institute of Standards and Technology (NIST) - AES: https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines/archived-standards

Question: 15

A technician is troubleshooting an issue involving programs on a Windows 10 machine that are loading on startup but causing excessive boot times. Which of the following should the technician do to selectively prevent programs from loading?

A. Right-click the Windows button, then select Run... entering shell:startup and clicking OK, and then move items one by one to the Recycle Bin.
B. Remark out entries listed HKEY_LOCAL_MACHINE>SOFTWARE>Microsoft>Windows>CurrentVersion>Run.
C. Manually disable all startup tasks currently listed as enabled and reboot, checking for issue resolution at startup.
D. Open the Startup tab and methodically disable items currently listed as enabled and reboot, checking for issue resolution at each startup.

Answer: D

Explanation:

The correct answer is D, which involves using the Startup tab within Task Manager to disable startup programs.

Here's why: Windows Task Manager provides a user-friendly interface for managing startup programs. The Startup tab (introduced in Windows 8 and present in Windows 10) specifically lists programs configured to launch at startup. This feature simplifies the process of disabling these programs without requiring advanced technical knowledge. By disabling startup programs methodically, a technician can isolate the problematic application causing slow boot times. Disabling items one by one and rebooting allows for precise identification, preventing the complete removal of useful startup applications. After disabling a program and rebooting, one can then check for any increase in boot speed, further confirming that the specific program was indeed the issue.

Option A, while partially correct in identifying the Startup folder, suggests deleting items. This is a more drastic approach than necessary during troubleshooting. Disabling a program temporarily is safer. Option B requires directly editing the registry, which can be risky and cause system instability if done incorrectly, especially with little experience. Editing the registry must only be done after backup and a clear understanding of consequences. Option C suggests disabling all startup tasks initially, which is less efficient for pinpointing the root cause of the issue. It lacks a methodical approach, and may disable several necessary applications along the way. Disabling them incrementally and checking helps isolate the individual program causing the problem.

Therefore, using the Startup tab offers the most controlled, safest, and effective method for selectively preventing programs from loading at startup.Authoritative Links:

Microsoft Support - Change which apps run automatically at startup in Windows:
https://support.microsoft.com/en-us/windows/change-which-apps-run-automatically-at-startup-in-windows-4b52d310-84be-a381-9505-e5aefe62475e
How to Geek - How to Manage Startup Programs in Windows 8 or 10:
https://www.howtogeek.com/74523/how-to-disable-startup-programs-in-windows/

Question: 16

A call center technician receives a call from a user asking how to update Windows. Which of the following describes what the technician should do?

A. Have the user consider using an iPad if the user is unable to complete updates.
B. Have the user text the user's password to the technician.
C. Ask the user to click in the Search field, type Check for Updates, and then press the Enter key.
D. Advise the user to wait for an upcoming, automatic patch.

Answer: C

Explanation:

The correct answer is C because it provides a clear, concise, and secure method for the user to initiate the Windows Update process themselves. It empowers the user to take control of the situation and learn how to perform updates in the future. This approach is in line with good IT support practices. Asking the user to search for "Check for Updates" directly guides them to the Windows Update settings page, where they can review available updates and start the installation process.

Option A is not helpful and suggests switching to a different device instead of solving the problem. It does not

address the core issue of updating Windows and is essentially an irrelevant suggestion.

Option B is a severe security violation. Sharing passwords via text message is incredibly risky and exposes the user's account to potential compromise. Technicians should never request passwords in this manner. This violates fundamental security best practices.

Option D is not ideal. While Windows Update is often automatic, relying solely on automatic updates can delay the installation of critical security patches. Actively checking for updates allows the user to promptly apply the latest fixes and protect their system against vulnerabilities. Furthermore, an immediate problem will not be immediately fixed. The user called for assistance, so the ideal solution would be direct and offer the best fix as soon as possible.

Therefore, guiding the user to the Windows Update settings using the search function is the safest and most efficient way to address their request.

Further Reading:

Microsoft Windows Update:https://support.microsoft.com/en-us/windows/windows-update-faq-8244922d-b71c-4695-8941-355e972fc6b5

Question: 17

When a user calls in to report an issue, a technician submits a ticket on the user's behalf. Which of the following practices should the technician use to make sure the ticket is associated with the correct user?

A. Have the user provide a callback phone number to be added to the ticket.
B. Assign the ticket to the department's power user.
C. Register the ticket with a unique user identifier.
D. Provide the user with a unique ticket number that can be referenced on subsequent calls.

Answer: C

Explanation:

The correct answer is C, registering the ticket with a unique user identifier. This practice ensures the ticket is accurately associated with the correct user in the system. Unique user identifiers, such as employee IDs, usernames, or email addresses, provide a definitive link between the reported issue and the individual experiencing it.

Options A, B, and D, while potentially useful, do not guarantee accurate user association. A callback phone number (A) doesn't always confirm the user's identity, especially if the number is shared or incorrect.

Assigning the ticket to a department's power user (B) only redirects the ticket for initial assessment and doesn't inherently link it to the original reporting user. Providing a unique ticket number (D) is crucial for tracking purposes but relies on the user remembering and correctly referencing it in future communications; it doesn't actively confirm the ticket's initial association with the right individual.

Using a unique user identifier eliminates ambiguity. It allows technicians to accurately track the issues reported by specific users, enabling them to effectively monitor trends, personalize support, and maintain a clear history of the user's interactions. This is especially important in larger organizations with many employees.

A well-defined user identification system is a cornerstone of efficient IT support. It streamlines the ticketing process, promotes accurate data analysis, and enhances user satisfaction by ensuring that their concerns are properly documented and addressed. For further reading on IT support best practices, refer to resources from ITIL (Information Technology Infrastructure Library) or CompTIA.

Question: 18

Which of the following is the MOST important environmental concern inside a data center?

A. Battery disposal
B. Electrostatic discharge mats
C. Toner disposal
D. Humidity levels

Answer: D

Explanation:

The most important environmental concern inside a data center is humidity levels (D). While battery disposal (A) and toner disposal (C) are environmentally responsible practices, they are not as critically impactful on the continuous and reliable operation of the data center itself. Electrostatic discharge mats (B) are a safety measure to protect equipment, not a direct environmental concern.

Humidity levels, on the other hand, directly affect the performance and lifespan of sensitive electronic equipment. High humidity can lead to condensation, which can cause short circuits, corrosion, and equipment failure. Conversely, low humidity can increase the risk of electrostatic discharge, which can also damage components. Data centers are packed with servers, networking gear, and storage devices that generate significant heat. Maintaining optimal humidity levels is crucial for efficient cooling and heat dissipation.

Inadequate humidity control can result in overheating, system instability, and ultimately, downtime. Proper humidity management is a key factor in ensuring the availability, reliability, and longevity of data center infrastructure. Neglecting humidity control can lead to costly repairs, data loss, and reputational damage. Cloud providers and organizations relying on data centers understand the importance of precisely controlled environments for optimal performance and business continuity. Data centers utilize sophisticated HVAC systems, humidifiers, and dehumidifiers to maintain humidity within the ideal range, typically between 40% and 60%. Failure to do so compromises the integrity of the entire data center ecosystem.

For further reading on data center environmental controls, you can refer to:

Uptime Institute:https://uptimeinstitute.com/
ASHRAE (American Society of Heating, Refrigerating and Air-Conditioning Engineers): (ASHRAE sets standards for data center environmental controls): https://www.ashrae.org/ (Specifically, look for ASHRAE Standard 90.4)

Question: 19

A user is unable to log in to the network. The network uses 802.1X with EAP-TLS to authenticate on the wired network. The user has been on an extended leave and has not logged in to the computer in several months. Which of the following is causing the log-in issue?

A. Expired certificate
B. OS update failure
C. Service not started
D. Application crash
E. Profile rebuild needed

Answer: A

Explanation:

The correct answer is **A. Expired certificate**. Here's why:

802.1X with EAP-TLS relies on digital certificates for authentication. In EAP-TLS (Extensible Authentication Protocol - Transport Layer Security), both the client (the user's computer) and the authentication server (typically a RADIUS server) must present valid certificates to establish a secure connection and authenticate the user. These certificates have an expiration date.

Since the user has been on leave for several months, the certificate on their computer has likely expired. Certificates are typically issued with a specific validity period (e.g., one year). Upon expiration, the client can no longer present a valid credential to the network. This results in the user being unable to authenticate and log in.

Options B, C, D, and E are less likely. While an OS update failure (B) could corrupt the certificate store, it's less directly tied to the length of the user's absence. A service not started (C) or application crash (D) might prevent network access in general but wouldn't specifically affect 802.1X authentication based on certificate validity. A profile rebuild (E) would address user profile corruption issues, but doesn't directly relate to certificate-based authentication.

Expired certificates are a common issue in certificate-based authentication systems. A well-managed Public Key Infrastructure (PKI) incorporates certificate lifecycle management processes, including automated certificate renewal, to prevent such outages.

Here are some authoritative links for further research:

802.1X:https://en.wikipedia.org/wiki/IEEE_802.1X
EAP-TLS:https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol
Certificate expiration:https://www.entrust.com/resources/glossary/certificate-expiration

Question: 20

A technician needs to format a USB drive to transfer 20GB of data from a Linux computer to a Windows computer. Which of the following filesystems will the technician MOST likely use?

A. FAT32
B. ext4
C. NTFS
D. exFAT

Answer: D

Explanation:

Here's a detailed justification for why exFAT (D) is the most likely filesystem choice for transferring a 20GB file between Linux and Windows computers via USB drive:

FAT32 (A) has a maximum file size limit of 4GB. Since the technician needs to transfer a 20GB file, FAT32 is immediately ruled out. While FAT32 is highly compatible, its file size limitation makes it unsuitable for larger files.

ext4 (B) is a journaling filesystem commonly used in Linux systems. While Linux can read and write to ext4, Windows typically requires third-party drivers to access ext4 formatted drives. This introduces an extra step and potential complexity for the technician. The key here is effortless transfer and compatibility out of the box.

NTFS (C) is the primary filesystem used by Windows. While Windows can read and write to NTFS, Linux can read NTFS relatively easily, but writing often involves additional steps or potential performance issues. While generally supported on both, exFAT is designed for flash drives and has less overhead.

exFAT (D), or Extended File Allocation Table, is designed specifically for flash drives and other external storage devices. It supports files larger than 4GB and is natively supported by both Windows and Linux. This means that the technician can format the USB drive with exFAT, transfer the 20GB file from the Linux computer, and then plug the drive into the Windows computer without needing to install any additional drivers or software.

Therefore, exFAT provides the best balance of large file size support and cross-platform compatibility for this specific task, making it the most suitable choice. The aim is to ensure a seamless, out-of-the-box experience on both operating systems. exFAT is designed to be a lightweight file system optimized for flash memory, which is exactly what a USB drive utilizes. The other filesystems are either restricted by file size, or better suited to hard drives and main system drives.

https://learn.microsoft.com/en-us/windows-server/storage/file-server/exfat-file-systemhttps://www.kernel.org/doc/html/latest/filesystems/exfat.html

Question: 21

Following the latest Windows update, PDF files are opening in Microsoft Edge instead of Adobe Reader. Which of the following utilities should be used to ensure all PDF files open in Adobe Reader?

A. Network and Sharing Center
B. Programs and Features
C. Default Apps
D. Add or Remove Programs

Answer: C

Explanation:

The correct answer is C, Default Apps. Here's why:

The scenario describes a situation where file associations have been altered, specifically for PDF files. After a Windows update, Microsoft Edge has taken over as the default application for opening PDFs, overriding the user's previous preference for Adobe Reader.

To rectify this, you need to specify that Adobe Reader should be the default application for handling PDF files. The **Default Apps** utility in Windows provides a centralized location to manage these file associations. You can access it through the Settings app.

A. **Network and Sharing Center** focuses on network configurations, such as setting up network connections, troubleshooting network issues, and managing shared resources on a local network. It has no bearing on file associations.

B and D. **Programs and Features** (also known as Add or Remove Programs) are used to uninstall, repair, or change existing software installations. While you could uninstall both Adobe Reader and Microsoft Edge and reinstall Adobe Reader, this is an unnecessarily drastic and time-consuming approach. It doesn't directly allow you to set a default app without extra steps.

Default Apps allows users to choose default applications for various file types, protocols, and application categories. By navigating to the PDF file extension within the Default Apps settings, you can easily select Adobe Reader as the default application. Once set, all PDF files should open with Adobe Reader instead of

Microsoft Edge. This is the most direct and efficient method to resolve the described issue.

For further reading:

Microsoft's documentation on changing default apps in Windows: https://support.microsoft.com/en-us/windows/change-default-apps-in-windows-10-e556d64c-82d8-4216-cd89-3f4677544595

Question: 22

A technician needs to exclude an application folder from being cataloged by a Windows 10 search. Which of the following utilities should be used?

A. Privacy
B. Indexing Options
C. System
D. Device Manager

Answer: B

Explanation:

The correct answer is **B. Indexing Options**. Here's why:

The Windows Search Indexer catalogs files and their contents to provide rapid search results. To prevent an application folder from being included in the search index, the "Indexing Options" utility is the direct tool to modify these settings. This utility allows users to specify which locations should be indexed. By excluding a folder from the indexed locations, its files and subfolders will no longer be included in search results generated by the Windows Search service, unless the search explicitly targets the folder.

Option A, "Privacy," primarily controls privacy settings related to location, camera, microphone, and other personal data, but doesn't directly manage the Search Index. Option C, "System," provides general information about the computer's hardware and operating system but lacks specific indexing configuration. Option D, "Device Manager," is used to manage hardware devices connected to the computer and has nothing to do with search indexing.

Therefore, "Indexing Options" is the most suitable utility for excluding an application folder from Windows 10 search. Modifying indexing settings improves search performance and prevents irrelevant files from appearing in search results.

For further information, refer to the official Microsoft documentation on indexing options:

Change Windows Search indexing options

Question: 23

As part of a CYOD policy, a systems administrator needs to configure each user's Windows device to require a password when resuming from a period of sleep or inactivity. Which of the following paths will lead the administrator to the correct settings?

A. Use Settings to access Screensaver settings.
B. Use Settings to access Screen Timeout settings.
C. Use Settings to access General.
D. Use Settings to access Display.

Answer: A

Explanation:

The correct answer is A: Use Settings to access Screensaver settings.

Here's a detailed justification:

The requirement is to configure Windows devices to prompt for a password after resuming from sleep or inactivity. This setting is intrinsically linked to the screensaver functionality within Windows. While other settings influence power management and display behavior, the screensaver settings specifically include the option to require a password upon resuming.

Navigating to the Screensaver settings allows a systems administrator to configure the timeout period after which the screensaver activates. Crucially, within the screensaver settings, there is a checkbox or similar control labeled something like "On resume, display logon screen" or "Require password on wakeup." Enabling this option ensures that users must authenticate (enter their password) before regaining access to their device after it has been in a sleep or inactive state long enough for the screensaver to have activated.

Options B, C, and D are less direct or incorrect:

B. Screen Timeout settings: These settings generally control when the display turns off, which is related to power management but doesn't directly force a password on resume.

C. General: The "General" section in Windows Settings typically contains broad, overarching settings and not specific security options like password-protected resume.

D. Display: While display settings control aspects like resolution and brightness, they don't handle password requirements after inactivity.

Therefore, the most direct and relevant path to configure this specific CYOD policy requirement is through the Screensaver settings. This method leverages a built-in Windows security feature specifically designed to control access to the device after a period of inactivity.

Authoritative Links for further research:

Microsoft Support: How to Lock your Windows 10 PC: https://support.microsoft.com/en-us/windows/lock-your-windows-10-pc-d6a3a201-29cb-051d-9b5c-c2d8a522415a (while not directly about screensaver settings, it addresses related locking and password functionality).

How to Geek: How to Require a Password When Your Computer Wakes Up: https://www.howtogeek.com/131089/how-to-require-a-password-when-your-computer-wakes-up/ (Demonstrates how to configure the setting through screensaver).

Question: 24

A technician is working with a company to determine the best way to transfer sensitive personal information between offices when conducting business. The company currently uses USB drives and is resistant to change. The company's compliance officer states that all media at rest must be encrypted. Which of the following would be the BEST way to secure the current workflow?

A. Deploy a secondary hard drive with encryption on the appropriate workstation.
B. Configure a hardened SFTP portal for file transfers between file servers.
C. Require files to be individually password protected with unique passwords.
D. Enable BitLocker To Go with a password that meets corporate requirements.

Answer: D

Explanation:

The best way to secure the current workflow, given the company's resistance to change and the compliance requirement for encrypting data at rest on removable media, is to enable BitLocker To Go with a strong password.

Here's why:

BitLocker To Go directly addresses the specific requirement of encrypting data at rest on USB drives. It's built into Windows and allows for full-disk encryption of removable storage devices like USB drives. Encryption ensures that even if a USB drive is lost or stolen, the data on it is unreadable without the correct password. Requiring a password that meets corporate standards adds a layer of security, reducing the risk of brute-force attacks. The other options are less effective or practical in this scenario. Deploying a secondary hard drive doesn't solve the portable media problem. An SFTP portal is a good idea but it is not something the company is looking for.

Individual password protection of files (Option C) is cumbersome and difficult to manage, especially with multiple users and files. Users are likely to create easy-to-remember passwords that can be easily cracked or forget the passwords altogether leading to data loss.

BitLocker To Go provides a centralized, managed approach to securing USB drives, aligning with the company's existing workflow while meeting compliance requirements.

For more information:

Microsoft's BitLocker Overview:https://learn.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview
Using BitLocker To Go:https://learn.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-to-go-faq

Question: 25

The command cat comptia.txt was issued on a Linux terminal. Which of the following results should be expected?

A. The contents of the text comptia.txt will be replaced with a new blank document.
B. The contents of the text comptia.txt would be displayed.
C. The contents of the text comptia.txt would be categorized in alphabetical order.
D. The contents of the text comptia.txt would be copied to another comptia.txt file.

Answer: B

Explanation:

The command cat in Linux is short for "concatenate." Its primary function is to read and display the contents of a file to the standard output, which is usually the terminal screen. Therefore, when the command cat comptia.txt is executed, the operating system will locate the file named "comptia.txt" in the current directory (or a directory specified in the path if the file is not in the current directory). The cat command then reads the entire contents of this file and displays them on the terminal. It does not modify the file in any way, meaning it doesn't replace it with a blank document, reorder its contents, or create a copy. It solely acts as a display utility. Option A is incorrect because cat by itself doesn't overwrite files; that requires redirection operators.
Option C is incorrect; sorting requires other utilities like sort. Option D is also incorrect; copying requires commands like cp.

For further learning, refer to these resources:

GNU Coreutils cat documentation:https://www.gnu.org/software/coreutils/manual/html_node/cat-

invocation.html

cat command on Linux man page: You can access this directly in a Linux terminal by typing man cat.

Question: 26

An incident handler needs to preserve evidence for possible litigation. Which of the following will the incident handler MOST likely do to preserve the evidence?

A. Encrypt the files.
B. Clone any impacted hard drives.
C. Contact the cyber insurance company.
D. Inform law enforcement.

Answer: B

Explanation:

The correct answer is **B. Clone any impacted hard drives.** This is because cloning creates an exact, bit-by-bit copy of the hard drive's contents, preserving the original state of the evidence. This is critical for forensic analysis as it allows investigators to examine the data without altering the original source, adhering to the principle of non-repudiation.

Here's why the other options are less suitable for evidence preservation:

A. Encrypt the files: While encryption protects confidentiality, it doesn't directly preserve the original state of the evidence. Furthermore, encrypting files after an incident can alter metadata and potentially complicate the forensic process. Encryption is primarily a security measure, not an evidence preservation technique. **C. Contact the cyber insurance company:** This is important for managing the financial aspects of the incident, but it does not directly contribute to evidence preservation. The insurance company might recommend specific forensic experts, but the initial responsibility for securing the evidence lies with the incident handler.

D. Inform law enforcement: While informing law enforcement is crucial, it doesn't directly preserve the evidence itself. Law enforcement will likely require preserved evidence to conduct their investigation. Cloning the drives enables law enforcement to properly investigate.

Cloning the drives helps maintain the chain of custody, a critical component for legal admissibility. This process documents who has handled the evidence, when they handled it, and what changes (if any) were made to it. A clear chain of custody ensures the integrity of the evidence.

In summary, cloning the impacted hard drives ensures that a forensically sound copy of the data is available for analysis while preserving the integrity of the original evidence. It's the most direct and effective action for evidence preservation in anticipation of potential litigation.Relevant link:

NIST Guidelines on Digital Evidence: (While there is no single URL) Search on the NIST website (nist.gov) for publications related to "digital evidence" and "computer forensics" for comprehensive guidance. Also search for "NIST 800-86" (Guide to Integrating Forensic Techniques into Incident Response)

Question: 27

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

A. Full

B. Differential

C. Off-site

D. Grandfather-father-son

Answer: B

Explanation:

The best backup method to mitigate ransomware attacks, considering limited storage and regularly modified files, is a Differential backup. Here's why:

Mitigating Ransomware: Ransomware often targets recent changes. By backing up these changes regularly, a Differential backup allows for restoring the system to a point before the ransomware infection, minimizing data loss.

Storage Efficiency: Differential backups only back up files that have changed since the last full backup. This means each differential backup contains accumulated changes since the full backup. Although they grow in size until the next full backup, they are generally smaller than full backups, addressing the storage concern.

Faster Restore Compared to Incremental: While Incremental backups (not listed) are even smaller, Differential backups are faster to restore. Only the last full backup and the latest differential backup are needed for a full recovery.

Full Backups (A) are inefficient: Full backups consume excessive storage and take longer, particularly when only a few files change regularly. While they offer complete protection, they are impractical given the constraints.

Off-site Backups (C) are a strategy, not a method: Off-site backups are crucial for disaster recovery, protecting data from physical events, including on-site ransomware infections. However, they don't specify how the data is backed up. They complement backup methods like Differential.

Grandfather-Father-Son (GFS) (D) is a rotation scheme: GFS is a backup rotation scheme, not a specific backup method. GFS can use Full, Differential, or Incremental backups as its underlying methods. It manages backup retention and frequency but doesn't inherently address ransomware mitigation or storage concerns on its own.

Therefore, a Differential backup, combined with off-site storage and a good retention policy (potentially incorporating a GFS-like scheme), provides a good balance between protection against ransomware, efficient storage use, and relatively quick restore times.

Authoritative Links:

US-CERT (CISA) on Ransomware:https://www.cisa.gov/ransomware (General guidance on ransomware prevention and recovery.)
NIST (National Institute of Standards and Technology) on Backup and Recovery: Search the NIST Computer Security Resource Center (csrc.nist.gov) for documents on backup and recovery best practices. This will provide detailed guidelines.

Question: 28

A technician is troubleshooting a customer's PC and receives a phone call. The technician does not take the call and sets the phone to silent. Which of the following BEST describes the technician's actions?

A. Avoid distractions

B. Deal appropriately with customer's confidential material

C. Adhere to user privacy policy
D. Set and meet timelines

Answer: A

Explanation:

The best description of the technician's actions is **A. Avoid distractions**.

Here's why: The scenario explicitly states the technician is troubleshooting a customer's PC and receives a call. Ignoring the call and silencing the phone directly addresses the potential for interruption and loss of focus on the task at hand. Troubleshooting requires concentration and systematic analysis. A phone call, especially if it's unrelated to the current task, introduces a significant distraction that can lead to errors, overlooked details, and increased troubleshooting time. By minimizing interruptions, the technician can efficiently and effectively resolve the customer's PC issue.

While B, C, and D touch upon important aspects of IT support, they aren't the primary reason for silencing the phone in this context. Dealing with confidential information (B) is about data security; user privacy (C) relates to data handling and compliance; and setting timelines (D) is about project management. While these are crucial in the broader picture of IT support, the direct and immediate impact of ignoring the call is to reduce distractions to better focus on the task at hand.

For further information on IT support best practices and time management, you can refer to resources like the CompTIA A+ certification materials themselves or articles on IT service management.

Question: 29

A technician needs to transfer a large number of files over an unreliable connection. The technician should be able to resume the process if the connection is interrupted. Which of the following tools can be used?

A. sfc
B. chkdsk
C. git clone
D. robocopy

Answer: D

Explanation:

The correct answer is D, robocopy (Robust File Copy). Robocopy is a command-line directory replication command for Microsoft Windows. Its key feature, and the reason it's optimal for this scenario, is its ability to resume interrupted transfers. This makes it ideal for unreliable connections where disruptions are likely.

Unlike simple copy commands, robocopy maintains state during the transfer. If the connection drops, robocopy can pick up where it left off, avoiding the need to restart the entire process from the beginning. This is crucial when transferring a large number of files, as restarting would be time-consuming and inefficient.

Option A, sfc (System File Checker), is a utility in Windows that allows users to scan for and restore corrupted Windows system files. It's not related to file transfer. Option B, chkdsk (Check Disk), is a utility used to verify the file system integrity of a volume and fix logical file system errors. It is also unrelated to file transfer. Option C, git clone, is used for creating a local copy of a Git repository. While it supports resuming downloads in some cases, it is designed for version control repositories, not general-purpose file transfer, and less suited for simply transferring a "large number of files" that are not part of a Git repository. Robocopy offers features specifically tailored for robust file transfer, such as restartable copies, error handling, and the ability to skip files already successfully transferred. These features significantly improve reliability and efficiency when

dealing with unstable network connections. Therefore, robocopy is the most appropriate tool for this task.

Further research:

Microsoft Robocopy documentation: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/robocopy
Robocopy tutorial: https://www.digitalcitizen.life/robocopy-command-line-windows/

Question: 30

A company installed a new backup and recovery system. Which of the following types of backups should be completed FIRST?

A. Full
B. Non-parity
C. Differential
D. Incremental

Answer: A

Explanation:

The correct answer is A. Full. Here's why:

When a new backup and recovery system is implemented, a full backup should always be the first type of backup performed. A full backup copies all data selected for backup, regardless of whether it has changed since the last backup. This serves as the baseline for all subsequent backups and ensures a complete and restorable copy of the data.

Differential and incremental backups, while efficient for daily or weekly backups after the initial full backup, rely on the existence of a previous full backup. They only back up changes made since the last full (differential) or last backup (incremental). Without a full backup to begin with, these backups would have no reference point, making restoration impossible.

Non-parity backups are not a standard backup type and relate more to RAID configurations. Parity is a method of data redundancy, which isn't directly related to the type of initial backup performed.

Performing a full backup first establishes a clean and complete starting point, enabling successful and reliable subsequent backups and restores using any backup strategy (differential or incremental). It guarantees that you have all your data securely stored at the beginning of the new backup process. In essence, it's the foundation of the entire backup strategy within the new system. Without it, other backup strategies are useless.

For more information on backup types, you can refer to resources like:

Acronis:https://www.acronis.com/en-us/resource-center/resource/backup-types/
Veritas:https://www.veritas.com/content/support/content/whitepaper_5984_1 (consider searching "Veritas backup types explained" if the direct link fails)

Question: 31

A user's smartphone data usage is well above average. The user suspects an installed application is transmitting data in the background. The user would like to be alerted when an application attempts to communicate with the internet. Which of the following BEST addresses the user's concern?

A. Operating system updates
B. Remote wipe
C. Antivirus
D. Firewall

Answer: D

Explanation:

The correct answer is **D. Firewall**. Here's why:

A firewall's primary function is to monitor and control network traffic based on predetermined security rules. In the context of a smartphone, a firewall app can track which applications are attempting to access the internet. It can then alert the user or block the application based on the user's preferences. This directly addresses the user's concern of being alerted when an application attempts to communicate with the internet, enabling them to identify the culprit behind the excessive data usage.

Let's analyze why the other options are less suitable:

A. Operating system updates: While important for security and stability, OS updates don't provide real-time monitoring of individual application network activity. They might indirectly improve security by patching vulnerabilities, but they don't offer alerts about application-specific internet access.

B. Remote wipe: Remote wipe is a security feature to erase data from a lost or stolen device. It's a drastic measure and doesn't help in identifying or controlling which applications are using excessive data.

C. Antivirus: Antivirus software primarily focuses on detecting and removing malicious software (malware) like viruses and Trojans. While some antivirus apps might have network monitoring features, their primary focus isn't on alerting users about all application network activity. Their alerts are typically related to detected threats.

Therefore, a firewall is the most appropriate solution for the user's specific need of being alerted about applications attempting to connect to the internet and thus helping identify the cause of high data usage.It allows proactive monitoring and control over network traffic on an application level, providing the necessary visibility and control.

For further reading on mobile firewalls and network security on mobile devices, consider exploring:

Android Firewall Apps: A simple web search for "android firewall apps" or "iOS firewall apps" will provide links to app store listings and reviews of available options.
Mobile Security Best Practices: NIST (National Institute of Standards and Technology) often publishes guidelines on mobile security: https://www.nist.gov/
SANS Institute Resources: SANS Institute provides training and resources on cybersecurity, including mobile security: https://www.sans.org/

Question: 32

A technician has been tasked with installing a workstation that will be used for point-of-sale transactions. The point-of-sale system will process credit cards and loyalty cards. Which of the following encryption technologies should be used to secure the workstation in case of theft?

A. Data-in-transit encryption
B. File encryption
C. USB drive encryption
D. Disk encryption

Answer: D

Explanation:

The most appropriate encryption technology for securing a point-of-sale (POS) workstation against theft is disk encryption. Disk encryption, also known as full disk encryption (FDE), protects all data on the hard drive or solid-state drive by converting it into an unreadable format. If the workstation is stolen, unauthorized users would not be able to access the operating system, applications, or, most importantly, the sensitive credit card and loyalty card data processed by the POS system. Data-in-transit encryption secures data while it's being transmitted across a network (e.g., using HTTPS for web transactions), but it does not protect data stored on the device itself. File encryption protects specific files, but it's not as comprehensive as disk encryption because it requires individual file management and might leave system files vulnerable. USB drive encryption is specific to USB drives and not the entire workstation. Given that the workstation contains sensitive customer data locally, full disk encryption provides the necessary layer of security in the event of physical theft. Encryption prevents the data from being read, even if the drive is removed and connected to another system. Standards like AES (Advanced Encryption Standard) are commonly used for this purpose. BitLocker (Windows) and FileVault (macOS) are built-in disk encryption tools.

Relevant links:

NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices:
https://csrc.nist.gov/publications/detail/sp/800-111/final
PCI Security Standards Council - Protecting Stored Cardholder Data:
https://www.pcisecuritystandards.org/pdfs/protecting_stored_cardholder_data.pdf

Question: 33

A user contacted the help desk to report pop-ups on a company workstation, indicating the computer has been infected with 137 viruses and payment is needed to remove them. The user thought the company-provided antivirus software would prevent this issue. The help desk ticket states that the user only receives these messages when first opening the web browser. Which of the following steps would MOST likely resolve the issue? (Choose two.)

A. Scan the computer with the company-provided antivirus software.
B. Install a new hard drive and clone the user's drive to it.
C. Deploy an ad-blocking extension to the browser.
D. Uninstall the company-provided antivirus software.
E. Click the link in the messages to pay for virus removal.
F. Perform a reset on the user's web browser.

Answer: AF

Explanation:

The correct answer is **AF**. Here's why:

A. Scan the computer with the company-provided antivirus software: This is a crucial first step. While the user is getting the pop-ups only in the browser, it's still important to rule out actual malware infections on the system. The antivirus software can identify and remove any potentially harmful files or programs that might be causing the problem or have been inadvertently downloaded.

F. Perform a reset on the user's web browser: The problem is isolated to when the browser is first opened, suggesting that the issue is likely browser-related, such as a malicious extension, corrupted settings, or an altered homepage. Resetting the browser will revert it to its default state, removing any unwanted extensions,

toolbars, and changing homepage settings.

Why other options are incorrect:

B. Install a new hard drive and clone the user's drive to it: This is an extreme solution that is not warranted given the symptoms. It's costly, time-consuming, and doesn't directly address the browser-specific issue. **C. Deploy an ad-blocking extension to the browser:** While ad blockers can help prevent some unwanted pop-ups in general, it's unlikely to solve the core issue of the user receiving specific messages about virus infections when opening the browser.

D. Uninstall the company-provided antivirus software: This is the opposite of what should be done. Antivirus software is a critical security component and removing it would make the system more vulnerable.

E. Click the link in the messages to pay for virus removal: This is extremely dangerous and could lead to further malware installation, identity theft, or financial loss. It's a common tactic used by scammers.

In summary: The most appropriate steps involve first scanning the computer with the antivirus software to rule out more serious infections, and then resetting the browser to remove any settings or extensions that are causing the pop-up messages. This approach directly addresses the user's symptoms while ensuring the system remains protected.

Authoritative Links for further research:

Malware Scams:https://www.consumer.ftc.gov/articles/0346-tech-support-scams
Browser Reset: (check with specific browser version)

Google Chrome: https://support.google.com/chrome/answer/3296214?hl=en
Mozilla Firefox: https://support.mozilla.org/en-US/kb/refresh-firefox-reset-add-ons-and-settings Microsoft Edge: https://support.microsoft.com/en-us/microsoft-edge/reset-microsoft-edge-if-it-s-not-working-properly-0efdb7da-2c41-49e8-a531-5b863f42b50a

Question: 34

A technician is installing new software on a macOS computer. Which of the following file types will the technician MOST likely use?

A. .deb
B. .vbs
C. .exe
D. .app

Answer: D

Explanation:

The correct answer is **D. .app**.

Here's why:

.app (Application Bundle): This is the standard file extension for executable applications on macOS. macOS applications are typically packaged as application bundles, which are directories containing the application's executable code, resources (images, sounds, etc.), and metadata. When you double-click a .app file, macOS knows to launch the application.

.deb (Debian Package): This file format is used for installing software on Debian-based Linux distributions like Ubuntu. It's not compatible with macOS.

.vbs (VBScript File): This is a scripting language developed by Microsoft, primarily used on Windows systems for automation tasks. It is not a native format for macOS applications.

.exe (Executable File): This is the standard file extension for executable programs on Windows operating systems. macOS cannot directly execute .exe files without using compatibility layers like Wine or virtualization software like Parallels Desktop or VMware Fusion.

macOS uses a different application architecture and file format than Windows or Linux. Consequently, software designed for those operating systems won't run natively on macOS. The .app bundle is designed specifically for macOS and allows the operating system to manage and execute the application correctly. macOS also utilizes the Mac App Store, which provides applications in the .app format and ensures a level of security and vetting. When a technician installs software on macOS, they will typically use a .app file downloaded directly from the developer or through the Mac App Store.

Authoritative Links:

Apple Developer Documentation: Search for ".app bundle" on the Apple Developer website (developer.apple.com) to find detailed information about the structure and requirements of macOS application bundles.
Wikipedia: Search for "Application bundle" on Wikipedia to get a general overview of the concept.

Question: 35

A technician is investigating an employee's smartphone that has the following symptoms:☞ The device is hot, even when it is not in use.
☞ Applications crash, especially when others are launched.
☞ Certain applications, such as GPS, are in portrait mode when they should be in landscape mode.
Which of the following can the technician do to MOST likely resolve these issues with minimal impact? (Choose two.)

A. Turn on autorotation.
B. Activate airplane mode.
C. Close unnecessary applications.
D. Perform a factory reset.
E. Update the device's operating system.
F. Reinstall the applications that have crashed.

Answer: DE

Explanation:

The correct answer is **D. Perform a factory reset** and **E. Update the device's operating system.**

Here's a detailed justification:

The symptoms described (overheating, crashing apps, and orientation issues) point towards a potential software problem within the smartphone. The device is likely experiencing resource contention and software conflicts.

E. Update the device's operating system: Updating the OS is a crucial first step in troubleshooting. Updates often include bug fixes, performance improvements, and compatibility updates that address issues like app crashes and orientation problems. An outdated OS can have vulnerabilities and inefficiencies that lead to overheating and app instability. By updating, you potentially resolve underlying software bugs or incompatibilities causing the listed issues. This is a relatively non-destructive process, making it a good initial step.
Android UpdatesiOS Updates

D. Perform a factory reset: A factory reset returns the smartphone to its original factory state, effectively wiping all user data and settings. This is a more drastic measure, but it can resolve deep-seated software issues that simpler troubleshooting steps cannot fix. The overheating and crashing may be due to corrupted system files, conflicting applications, or malware. A factory reset eliminates these possibilities by providing a clean slate. Ensure data is backed up prior to executing this step. Performing this step before reinstalling all applications prevents the reintroduction of potential issues.

Why other options are less ideal:

A. Turn on autorotation: While the orientation problem is a symptom, autorotation being off doesn't explain the overheating or crashing applications. This only directly addresses the orientation problem.

B. Activate airplane mode: Airplane mode only turns off wireless communication, which might temporarily reduce heat, but it doesn't address the root cause of the problems. It's more of a workaround than a solution. **C. Close unnecessary applications:** While closing apps can reduce resource usage, it is a temporary solution. The issue described may point to one or a few rogue application. But in cases of overheating and crashing, it's unlikely to solve the underlying problem, especially if the phone is hot even when not actively used.

F. Reinstall the applications that have crashed: While it could help, without addressing potential deeper operating system problems, you might just be reinstalling apps that will continue to crash. Reinstalling one application does not solve overheating.

Therefore, updating the OS and performing a factory reset are the most effective solutions with minimal impact that address a variety of possible causes.

Question: 36

A customer reported that a home PC with Windows 10 installed in the default configuration is having issues loading applications after a reboot occurred in the middle of the night. Which of the following is the FIRST step in troubleshooting?

A. Install alternate open-source software in place of the applications with issues.
B. Run both CPU and memory tests to ensure that all hardware functionality is normal.
C. Check for any installed patches and roll them back one at a time until the issue is resolved.
D. Reformat the hard drive, and then reinstall the newest Windows 10 release and all applications.

Answer: C

Explanation:

The provided answer (C) is incorrect. The FIRST step in troubleshooting application loading issues after an unexpected reboot in Windows 10 should be to gather information and perform basic checks, not immediately resort to potentially disruptive solutions like rolling back patches.

Here's why option B, "Run both CPU and memory tests to ensure that all hardware functionality is normal," is the MOST appropriate FIRST step:

1. **Hardware Suspect:** An unexpected reboot suggests potential hardware instability. This could stem from faulty RAM, an overheating CPU, or power supply issues. Addressing potential hardware causes early saves time and prevents chasing software problems arising from underlying hardware failures.
2. **Data Integrity:** RAM issues, specifically, can corrupt data during operation. It is important to eliminate this possibility as bad RAM can lead to corrupt operating system files.
3. **System Stability:** Before attempting software-based troubleshooting, verifying hardware stability is crucial for a reliable testing environment. Troubleshooting software issues on unstable hardware can lead to misleading results and wasted effort.
4. **Least Invasive:** Running CPU and memory tests is relatively non-invasive. It doesn't alter the system

configuration or data. It isolates the issue to a hardware or not.

Here's why the other options are less suitable as the FIRST step:

A. Install alternate open-source software...: Replacing applications is a workaround, not a diagnosis. It doesn't address the root cause of the problem.

C. Check for any installed patches and roll them back...: Rolling back patches without any evidence linking them to the issue is a time-consuming and potentially destabilizing approach. It's more appropriate if initial hardware checks are normal and the problem coincides with a recent patch.

D. Reformat the hard drive...: This is an extreme measure and should only be considered as a last resort after exhausting all other troubleshooting steps. Reformatting erases all data and applications.

Therefore, option B is the MOST suitable initial troubleshooting step as it addresses a potential hardware failure, is relatively non-invasive, and provides valuable insight into the system's overall stability.

Resource:

Microsoft Support - Troubleshoot blue screen errors:https://support.microsoft.com/en-us/windows/troubleshoot-blue-screen-errors-5c62226a-68b9-5299-72a9-93d0c37c05c7 (While focused on blue screens, it emphasizes hardware checks after unexpected reboots.)

Question: 37

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

A.Geofence
B.Alarm system
C.Badge reader
D.Motion sensor

Answer: C

Explanation:

The correct answer is **C. Badge reader**. Here's why:

Physical security is crucial for data centers, protecting sensitive hardware and data from unauthorized access and potential threats. Badge readers are a fundamental component of physical access control systems. They use identification badges, often containing RFID or magnetic stripe technology, to verify an individual's identity and access privileges before granting entry to a secured area like a data center.

A badge reader system ensures that only authorized personnel, such as data center employees, technicians, and approved vendors, can gain access. This helps prevent unauthorized individuals from physically compromising the data center's infrastructure, stealing data, or causing damage. Badge readers can be integrated with access control software to manage user permissions, track entry/exit times, and generate audit trails. If an unauthorized badge is presented, the system can deny access and trigger an alarm. This granular level of control is essential for maintaining a secure environment.

Let's consider why the other options are less suitable:

A. Geofence: A geofence creates a virtual perimeter around a geographic area. While useful for tracking assets or monitoring activity within a defined zone, it doesn't directly control physical access to a building or room. A geofence might alert security personnel to activity near the data center, but it won't prevent someone from physically entering.

B. Alarm system: An alarm system detects intrusions or other security breaches. While it's a vital part of a comprehensive security strategy, it's reactive rather than proactive in controlling access. An alarm system is triggered after a breach has occurred, whereas a badge reader prevents the breach in the first place.

D. Motion sensor: Motion sensors detect movement within a specific area. Like an alarm system, they primarily serve as a detection mechanism. While useful for alerting security to unauthorized activity within the data center (after someone has gained access), they don't prevent unauthorized entry. A motion sensor's value increases when integrated with an alarm system.

In summary, while geofences, alarm systems, and motion sensors contribute to overall security, only a badge reader actively controls and verifies physical access, making it the most direct and effective method for securing a data center. It provides an active, permission-based security layer that directly addresses the physical entry point.

Authoritative Links:

NIST (National Institute of Standards and Technology) - Physical Security Recommendations for Data Centers: Search on NIST website: "Data Center Physical Security Recommendations" Note: NIST is a government agency and its website is the most authoritative source, however, finding the direct PDF might require searching the NIST website.

PCI Security Standards Council - Information Security:https://www.pcisecuritystandards.org/ (While focused on payment card security, it contains useful guidelines on physical access control applicable to data centers).

Question: 38

The Chief Executive Officer at a bank recently saw a news report about a high-profile cybercrime where a remote-access tool that the bank uses for support was also used in this crime. The report stated that attackers were able to brute force passwords to access systems. Which of the following would BEST limit the bank's risk? (Choose two.)

A. Enable multifactor authentication for each support account.
B. Limit remote access to destinations inside the corporate network.
C. Block all support accounts from logging in from foreign countries.
D. Configure a replacement remote-access tool for support cases.
E. Purchase a password manager for remote-access tool users.
F. Enforce account lockouts after five bad password attempts.

Answer: AF

Explanation:

The correct answers are A and F. Here's why:

A. **Enable multifactor authentication for each support account:** Multifactor authentication (MFA) adds an extra layer of security beyond just a password. Even if an attacker brute-forces a password, they would still need a second factor (like a code from a mobile app, biometric scan, or hardware token) to gain access. This significantly reduces the risk of unauthorized access, mitigating the vulnerability highlighted in the news report. This is a crucial aspect of zero-trust security and identity and access management (IAM).

F. **Enforce account lockouts after five bad password attempts:** Implementing account lockout policies prevents brute-force attacks. After a set number of failed login attempts, the account is temporarily locked, making it much harder for attackers to repeatedly guess passwords. This significantly slows down and often deters brute-force attacks.

Here's why the other options are less effective or incomplete:

B. **Limit remote access to destinations inside the corporate network:** While limiting access is a good security practice (least privilege principle), it doesn't directly address the brute-force attack vulnerability. The attacker could still gain access to internal systems within the allowed destinations.

C. **Block all support accounts from logging in from foreign countries:** While limiting access based on geographical location can be a useful security measure, it's not a comprehensive solution against brute-force attacks. Attackers could potentially use VPNs or other methods to bypass this restriction, and legitimate support staff might need to access systems while traveling internationally.

D. **Configure a replacement remote-access tool for support cases:** Replacing the tool might seem like a solution, but it doesn't address the underlying vulnerability (weak passwords and lack of MFA). The new tool could be susceptible to the same attacks if security best practices aren't implemented.

E. **Purchase a password manager for remote-access tool users:** While a password manager can improve password strength and security, it doesn't prevent brute-force attacks if users choose weak master passwords or the password manager itself is compromised. It's a good supplementary measure but not a primary defense.

In summary, MFA (A) and account lockouts (F) are the most effective measures to directly address the risk of brute-force attacks on remote-access tools.

Authoritative Links:

NIST Guidelines on MFA:https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf **OWASP on Brute Force Attacks:**https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A7-Cross-Site_Scripting_(XSS) (Although focused on XSS, OWASP provides general security principles applicable to all vulnerabilities)

Question: 39

A user reports a computer is running slow. Which of the following tools will help a technician identify the issue?

A. Disk Cleanup
B. Group Policy Editor
C. Disk Management
D. Resource Monitor

Answer: D

Explanation:

The correct answer is D, Resource Monitor, because it provides a real-time overview of how system resources are being utilized. A slow computer usually indicates a resource bottleneck, such as high CPU usage, memory constraints, disk I/O saturation, or network congestion. Resource Monitor allows a technician to pinpoint exactly which processes are consuming the most resources in each of these categories, providing concrete data for troubleshooting.

Option A, Disk Cleanup, helps free up disk space by removing temporary files and other unnecessary data. While low disk space can contribute to slow performance, Disk Cleanup doesn't actively monitor resource usage to identify the root cause of the slowdown in real time. It’s a preventative measure more than a diagnostic tool for this specific scenario.

Option B, Group Policy Editor, manages system settings and policies for users and computers in a domain

environment. It doesn't provide real-time performance monitoring capabilities and is unrelated to diagnosing general slowness. It is typically used for centralized configuration management, not performance troubleshooting.

Option C, Disk Management, primarily manages disk partitions and volumes. While it can help identify disk-related issues like fragmented volumes or full partitions, it doesn't provide the detailed, real-time performance insights offered by Resource Monitor to diagnose general slowdowns. You wouldn't use Disk Management to determine if a specific application is using excessive memory.

Therefore, Resource Monitor is the most effective tool in this scenario because it presents a dynamic, real-time view of resource consumption, enabling a technician to quickly identify the component or process causing the performance bottleneck.

Further Resources:

Microsoft's documentation on Resource Monitor: https://learn.microsoft.com/en-us/windows-server/administration/performance-monitor/using-resource-monitor
How to use Resource Monitor to troubleshoot PC performance: https://www.digitalcitizen.life/resource-monitor-windows/

Question: 40

Upon downloading a new ISO, an administrator is presented with the following string:
59d15a16ce90c8ee97fa7c211b7673a8
Which of the following BEST describes the purpose of this string?

A. XSS verification
B. AES-256 verification
C. Hash verification
D. Digital signature verification

Answer: C

Explanation:

The correct answer is C, Hash verification. Here's why:

The string "59d15a16ce90c8ee97fa7c211b7673a8" strongly resembles a cryptographic hash value. Hashes are used to verify the integrity of files, like downloaded ISO images.

A hash function takes an input (in this case, the ISO file) and produces a fixed-size string of characters. The key characteristic of a cryptographic hash is that even a tiny change in the input file will result in a drastically different hash value. This makes them ideal for detecting file corruption or tampering.

When you download an ISO, the provider often publishes the expected hash value (e.g., MD5, SHA-1, SHA-256, SHA-512). After downloading, you can use a hashing tool to calculate the hash of the downloaded file. If the calculated hash matches the published hash, it confirms that the file was downloaded without errors or alterations.

XSS (Cross-Site Scripting) verification (A) involves preventing malicious scripts from being injected into websites. AES-256 verification (B) confirms the successful decryption or encryption of data using the AES-256 algorithm, which doesn't directly apply to file integrity checking post-download. Digital signature verification (D) involves using public key cryptography to verify the authenticity and integrity of a file, often including verifying the publisher. While digital signatures provide stronger assurance than simple hash verification, the given string format points more directly towards a hash. Digital signatures typically involve

more complex structures.

Thus, the provided string is overwhelmingly indicative of a hash used for file integrity verification, making option C the most appropriate answer.

Further reading:

Hash Functions:https://en.wikipedia.org/wiki/Cryptographic_hash_function **File Integrity Monitoring:**https://www.varonis.com/blog/file-integrity-monitoring

Question: 41

A user's mobile phone has become sluggish. A systems administrator discovered several malicious applications on the device and reset the phone. The administrator installed MDM software. Which of the following should the administrator do to help secure the device against this threat in the future? (Choose two.)

A. Prevent a device root.
B. Disable biometric authentication.
C. Require a PIN on the unlock screen.
D. Enable developer mode.
E. Block a third-party application installation.
F. Prevent GPS spoofing.

Answer: AE

Explanation:

The correct answer is AE. Here's a detailed justification:

A. **Prevent a device root:** Rooting an Android device (or jailbreaking an iOS device) removes the manufacturer's security restrictions, granting users privileged control over the operating system. This allows the installation of unofficial software and modification of system settings. While this can offer advanced customization, it significantly increases the risk of malware infection. Malicious applications can exploit the unlocked system, gaining unrestricted access to data and device functions, which is exactly what caused the original problem. MDM software can be configured to detect and block rooted devices from accessing corporate resources, mitigating the risk.

E. **Block a third-party application installation:** Allowing users to install applications from untrusted sources (outside of official app stores like Google Play or Apple App Store) significantly increases the risk of installing malware. These third-party app stores or sideloaded apps often lack the rigorous security checks implemented by official stores. Malicious actors distribute malware disguised as legitimate applications through these channels. MDM software can enforce policies that restrict application installation to trusted sources, drastically reducing the chances of users installing malicious apps inadvertently. This addresses the original issue where malicious applications were the root cause of the phone's sluggishness.

Let's look at why the other options are less suitable:

B. Disable biometric authentication: Disabling biometric authentication weakens the security of the device by relying solely on PINs or passwords, but it doesn't directly prevent malware installation.

C. Require a PIN on the unlock screen: While requiring a PIN is a good security practice for general device security, it doesn't prevent the installation of malicious applications. It only secures the device after it has been compromised.

D. Enable developer mode: Enabling developer mode is for software development and debugging and opens up the device to security vulnerabilities if not properly managed. It would increase the risk of compromise.

F. Prevent GPS spoofing: Preventing GPS spoofing protects location data but isn't directly related to

preventing malware installation or the sluggishness caused by malicious applications.

Therefore, preventing device rooting and blocking third-party application installations are the most effective measures to secure the device against the type of threat described in the scenario. These measures directly address the root cause of the problem: the installation and execution of malicious applications due to weakened security controls.

Supporting Links:

Android Security Overview (Google):https://source.android.com/security
Mobile Device Management (MDM):https://www.gartner.com/en/information-technology/glossary/mobile-device-management-mdm

Question: 42

A technician is unable to join a Windows 10 laptop to a domain. Which of the following is the MOST likely reason?

A. The domain's processor compatibility is not met.
B. The laptop has Windows 10 Home installed.
C. The laptop does not have an onboard Ethernet adapter.
D. The laptop does not have all current Windows updates installed.

Answer: B

Explanation:

The correct answer is B: The laptop has Windows 10 Home installed.

Windows 10 Home edition lacks the functionality to join a domain. Domain joining is a feature primarily available in Windows 10 Pro, Enterprise, and Education editions. Domain joining allows a computer to become part of a centrally managed network, typically found in business or organizational environments. Domain controllers, the heart of Active Directory domains, manage user accounts, security policies, and access to network resources.

Windows 10 Home is designed for personal use and is typically deployed in standalone environments where centralized management is not required. It lacks the necessary components and capabilities to authenticate against a domain controller and enforce domain policies. Therefore, a laptop running Windows 10 Home will be unable to be joined to a domain network.

Options A, C, and D are less likely to be the primary reason. Processor compatibility (A) might cause installation problems, but it typically wouldn't prevent a domain join if the OS itself supports it. The absence of an Ethernet adapter (C) could hinder network connectivity but would not inherently prevent a domain join if Wi-Fi is available and configured correctly. Missing Windows updates (D) might cause issues but are generally not the direct cause of failure to join a domain; they are more likely to affect security and software
compatibility after joining.

Therefore, the key differentiator is the operating system edition itself. Windows 10 Home simply does not have the built-in features to join a domain, making it the most likely reason a technician is unable to join the laptop to the domain.

Further research:

Microsoft Documentation on Windows 10 Editions: https://www.microsoft.com/en-us/windows/business/compare-windows-10-plans
Difference between Windows 10 Home and Pro: https://support.microsoft.com/en-us/windows/which-version-

of-windows-operating-system-am-i-running-6283a825-401b-ed3a-8512-16c4ca82a3c6

Question: 43

Which of the following OS types provides a lightweight option for workstations that need an easy-to-use, browser-based interface?

A. FreeBSD
B. Chrome OS
C. macOS
D. Windows

Answer: B

Explanation:

The correct answer is B, Chrome OS. Chrome OS is specifically designed to be a lightweight operating system that primarily relies on web applications and cloud storage. Its core functionality is centered around the Chrome web browser, offering a streamlined and user-friendly experience. This makes it an excellent option for workstations needing easy access to web-based tools and applications without the overhead of a full-fledged desktop OS.

FreeBSD, macOS, and Windows, on the other hand, are all more comprehensive operating systems. While they can certainly be used with web browsers and cloud services, they are not inherently designed with a "lightweight" or browser-centric philosophy in mind. They consume more resources and offer a broader range of features, including native application support, hardware drivers, and system administration tools that a simple web-based workstation might not require. They can be more complex to manage and maintain.

Chrome OS updates are generally seamless and occur in the background. The security model is also tightly integrated with Google's services, providing robust protection against web-based threats. It's a good choice for educational settings, call centers, or any environment where users primarily need access to web applications.

For further information on Chrome OS, its features, and its suitability for various use cases, you can refer to the following resources:

Chrome OS official website:https://chromeenterprise.google/os/
Wikipedia - ChromeOShttps://en.wikipedia.org/wiki/ChromeOS

Question: 44

A user has requested help setting up the fingerprint reader on a Windows 10 laptop. The laptop is equipped with a fingerprint reader and is joined to a domain.
Group Policy enables Windows Hello on all computers in the environment. Which of the following options describes how to set up Windows Hello Fingerprint for the user?

A. Navigate to the Control Panel utility, select the Security and Maintenance submenu, select Change Security and Maintenance settings, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete.

B. Navigate to the Windows 10 Settings menu, select the Accounts submenu, select Sign-in options, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete.

C. Navigate to the Windows 10 Settings menu, select the Update & Security submenu, select Windows Security, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete.

D. Navigate to the Control Panel utility, select the Administrative Tools submenu, select the user account in the list, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete.

Answer: B

Explanation:

The correct answer is B. Here's why:

Windows Hello Fingerprint setup is found within the Windows 10 Settings app under the Accounts section, specifically within Sign-in options. This is the centralized location for managing user authentication methods, including fingerprint, PIN, and facial recognition.

Option A is incorrect because the Control Panel does not directly provide access to the Windows Hello settings. While the Control Panel contains security-related settings, Windows Hello is primarily managed through the Settings app. Also, the path described in the option does not exist.

Option C is incorrect because the Update & Security section of the Settings app focuses on system updates, security features like Windows Defender, and recovery options, but not on user sign-in methods like Windows Hello. Windows Security provides access to features like Virus & threat protection, but not Windows Hello setup.

Option D is incorrect because the Control Panel's Administrative Tools section contains system-level utilities and services, and it does not directly manage individual user account settings for Windows Hello. Further, Windows Hello is not configured per-user through administrative tools, but via the user's personal settings.

The process of setting up Windows Hello Fingerprint involves navigating to the correct settings page and then following the on-screen prompts to register a fingerprint by repeatedly placing it on the reader. This registration process allows the system to capture multiple angles of the fingerprint for more reliable authentication. Group Policy enabling Windows Hello means that the feature is available for the user to configure; it doesn't automate the fingerprint enrollment process.

Authoritative links for further research:

Microsoft Support: https://support.microsoft.com/en-us/windows/learn-about-windows-hello-and-set-it-up-ea5b31cf-d046-39a3-9961-6140269f51f3
Microsoft Docs: https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-identity-verification

Question: 45

An architecture firm is considering upgrading its computer-aided design (CAD) software to the newest version that forces storage of backups of all CAD files on the software's cloud server. Which of the following is MOST likely to be of concern to the IT manager?

A. All updated software must be tested with all system types and accessories.
B. Extra technician hours must be budgeted during installation of updates.
C. Network utilization will be significantly increased due to the size of CAD files.
D. Large update and installation files will overload the local hard drives.

Answer: C

Explanation:

The correct answer is C: Network utilization will be significantly increased due to the size of CAD files. Here's

why:

CAD files are notorious for being large due to the complex 3D models and detailed drawings they contain.

Forcing backups to a cloud server means transferring these large files over the network regularly. This increased traffic will put a significant strain on the organization's bandwidth. Increased network utilization can lead to slower internet speeds for all users, network congestion, and potential bottlenecks, impacting productivity across the firm, not just for CAD users.

Options A, B, and D are less directly related to the core problem of cloud-based CAD backup. While A is a good practice, it's a general concern for all software updates, not specifically this scenario. B is also generally true for software updates but less critical than the imminent network impact. Option D, although pertinent for local storage, is less directly applicable to the scenario as the primary action is data transfer to a remote server.

The shift to cloud backups of large CAD files creates a direct and immediate burden on the network infrastructure. The IT manager will likely need to investigate network bandwidth, implement traffic shaping, or potentially upgrade the network connection to accommodate the increased data transfer volume.

Consider these resources for more information on the challenges of cloud storage and network bandwidth:

Network Bandwidth Considerations for Cloud Storage:
https://www.vmware.com/topics/glossary/content/network-bandwidth (General overview)
Cloud Storage:https://azure.microsoft.com/en-us/solutions/cloud-storage/ (Microsoft Azure Cloud Storage Documentation)

Question: 46

Someone who is fraudulently claiming to be from a reputable bank calls a company employee. Which of the following describes this incident?

A. Pretexting
B. Spoofing
C. Vishing
D. Scareware

Answer: C

Explanation:

The correct answer is **C. Vishing**. Here's why:

Vishing, or voice phishing, is a type of phishing attack conducted over the telephone. The attacker impersonates a legitimate institution, such as a bank, to deceive the victim into revealing sensitive information like account numbers, passwords, or personal details. The scenario directly describes this: someone pretending to be from a reputable bank calling an employee to likely extract information.

Let's examine why the other options are incorrect:

A. Pretexting: Pretexting is creating and using an invented scenario (the pretext) to engage a target in a manner that increases the chance the victim will divulge information or perform actions that would be unlikely in ordinary circumstances. While a vishing attack uses a pretext (claiming to be from a bank), the key element that makes it vishing is the use of voice communication. Pretexting is a broader term.

B. Spoofing: Spoofing is disguising a communication from an unknown source as being from a known, trusted source. While the caller ID might be spoofed to appear as if the call is coming from the bank, spoofing itself

doesn't describe the entire attack strategy. It's a technique that can be used in vishing.

D. Scareware: Scareware is a type of malware that tricks users into believing their computer is infected with a virus and urges them to pay for fake malware removal software. This is unrelated to the described scenario.

In summary, because the attack involves someone falsely claiming to be from a bank over the phone to solicit information, vishing is the most accurate description.

Here are some authoritative links for further research:

NIST (National Institute of Standards and Technology): The NIST Glossary of Key Information Security Terms defines vishing, phishing, and other relevant security concepts.

https://csrc.nist.gov/glossary/term/vishing
SANS Institute: SANS provides information on various security threats and attack vectors, including vishing.

https://www.sans.org/
FBI (Federal Bureau of Investigation): The FBI investigates and provides resources on internet crime, including phishing and vishing scams. https://www.fbi.gov/

Question: 47

The network was breached over the weekend. System logs indicate that a single user's account was successfully breached after 500 attempts with a dictionary attack. Which of the following would BEST mitigate this threat?

A.Encryption at rest
B.Account lockout
C.Automatic screen lock
D.Antivirus

Answer: B

Explanation:

The best mitigation strategy for a successful dictionary attack leading to a user account breach is **B. Account lockout**. Here's why:

A dictionary attack relies on systematically trying common passwords against a user account. The system logs clearly indicate this happened with 500 failed attempts before success. An account lockout policy automatically disables an account after a specified number of incorrect login attempts within a defined timeframe. This would have prevented the attacker from continuing after, for example, 3-5 failed attempts, significantly hindering the attack's success.

Encryption at rest (A) protects data when it's stored, not during the login process. Automatic screen lock (C) protects an unattended, logged-in workstation, but doesn't prevent initial unauthorized login attempts. Antivirus (D) protects against malware, but is not specifically designed to prevent brute-force attacks on user accounts. While it might detect malicious software installed after a breach, it won't inherently block the initial attack.

Account lockout is a proactive measure specifically designed to counter brute-force and dictionary attacks. It introduces a delay or complete halt to the attacker's attempts, making such attacks computationally infeasible and significantly reducing the risk of a successful breach. This defense mechanism is a
fundamental security best practice for authentication and authorization. Implementing a strong password policy alongside account lockout further strengthens the security posture.

For more information:

NIST Guidelines for Digital Identity Management:https://pages.nist.gov/800-63-3/sp800-63b.html (While primarily about digital identity, it includes password policy and lockout guidelines)
OWASP Authentication Cheat Sheet:
https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html (Discusses authentication best practices including lockout)

Question: 48

A user reports a PC is running slowly. The technician suspects it has a badly fragmented hard drive. Which of the following tools should the technician use?

A. resmon.exe
B. msconfig.exe
C. dfrgui.exe
D. msinfo32.exe

Answer: C

Explanation:

The correct answer is **C. dfrgui.exe**.

The user reports a slow PC potentially caused by a fragmented hard drive. Disk fragmentation occurs when files are scattered across the hard drive instead of being stored contiguously. This leads to the read/write head having to move around more to access all parts of a file, slowing down performance. To resolve this, the technician needs a defragmentation tool.

dfrgui.exe is the command-line executable for the Disk Defragmenter utility in Windows. This is the tool specifically designed to analyze and defragment hard drives, consolidating fragmented files into contiguous blocks and optimizing disk performance.

The other options are incorrect:

resmon.exe (Resource Monitor) displays real-time resource usage statistics for CPU, memory, disk, and network. While helpful for identifying bottlenecks, it doesn't defragment the drive.

msconfig.exe (System Configuration) manages startup programs and services. It is useful for troubleshooting boot issues but doesn't address disk fragmentation.

msinfo32.exe (System Information) provides detailed information about the computer's hardware and software configuration. It is helpful for diagnosing system issues but doesn't perform disk defragmentation.

Therefore, only dfrgui.exe directly addresses the suspected problem of a fragmented hard drive, making it the appropriate tool to use.

Authoritative link: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/defrag

Question: 49

A company has just refreshed several desktop PCs. The hard drives contain PII. Which of the following is the BEST method to dispose of the drives?

A. Drilling
B. Degaussing

C. Low-level formatting
D. Erasing/wiping

Answer: B

Explanation:

The best method for disposing of hard drives containing PII (Personally Identifiable Information) from refreshed desktop PCs is degaussing. While other methods exist, degaussing offers a high level of assurance that the data is unrecoverable.

Degaussing involves using a powerful magnetic field to disrupt the magnetic domains on the hard drive platter, effectively scrambling the data. This renders the drive unusable and makes data recovery extremely difficult, if not impossible, even with sophisticated forensic techniques.

Drilling the hard drive is a physical destruction method that can be effective, but it's more prone to human error and might not completely destroy all platters if not done thoroughly. There's also a small chance of data recovery from undamaged areas.

Low-level formatting is a data sanitization method, but it's less effective than degaussing for securely erasing data, especially on modern drives. Data might still be recoverable using specialized tools.

Erasing/wiping (overwriting with random data) can be a suitable method, but it takes considerable time and resources, and its effectiveness is still less certain compared to degaussing. Some data could potentially remain if sectors are damaged or inaccessible.

Given the presence of PII, the goal is to employ the most secure and reliable data sanitization method. Degaussing provides this security by physically disrupting the magnetic storage, guaranteeing that the data cannot be easily recovered. It exceeds the security offered by software-based methods like wiping and formatting, and offers more consistent assurance than physical destruction methods vulnerable to human error. Therefore, degaussing emerges as the superior choice.

Authoritative Resources:

NIST Guidelines for Media Sanitization: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
DoD 5220.22-M Data Sanitization Standard.

These resources can help to clarify the differences in data sanitization methods and their relative effectiveness.

Question: 50

Which of the following is the MOST cost-effective version of Windows 10 that allows remote access through Remote Desktop?

A. Home
B. Pro for Workstations
C. Enterprise
D. Pro

Answer: D

Explanation:

The correct answer is D, Pro. Here's why:

Windows 10 offers different editions tailored for different user needs and market segments. When considering cost-effectiveness and Remote Desktop functionality, Windows 10 Pro strikes the optimal balance.

Windows 10 Home is the most basic version and does not include Remote Desktop functionality as a host. While you can use Remote Desktop client to connect to other computers from Home, you cannot remotely connect to a Windows 10 Home machine. This restriction immediately eliminates it as a suitable option for hosting remote sessions.

Windows 10 Enterprise offers the most features, including advanced security, deployment, and management capabilities beneficial in larger organizations. However, its licensing is significantly more expensive than Pro, targeting organizations needing volume licensing and advanced features like DirectAccess and AppLocker, which aren't strictly necessary for simple remote access.

Windows 10 Pro for Workstations is an even more specialized edition than Enterprise, designed for high-end hardware and demanding workloads. While it also supports Remote Desktop, its high cost is unwarranted if the primary need is just remote access.

Windows 10 Pro, on the other hand, incorporates Remote Desktop host capabilities as a standard feature and offers a more accessible price point for small businesses and power users who require remote access without the complexities and expenses of Enterprise or Workstation editions. This makes it the most cost-effective option. Therefore, Pro delivers the Remote Desktop functionality at the lowest cost.

In summary, while other editions offer Remote Desktop capabilities, Windows 10 Pro provides the necessary remote access feature without the premium price tag associated with Enterprise or Workstation versions, making it the most cost-effective choice.

Relevant Links:

Compare Windows 10 Editions:https://www.microsoft.com/en-us/windows/business/compare-windows-10-editions
Use Remote Desktop:https://support.microsoft.com/en-us/windows/how-to-use-remote-desktop-5fe128d3-8b21-a30a-66e6-c50a4e5a90a0

Question: 51

A user created a file on a shared drive and wants to prevent its data from being accidentally deleted by others. Which of the following applications should the technician use to assist the user with hiding the file?

A. Device Manager
B. Indexing Options
C. File Explorer
D. Administrative Tools

Answer: C

Explanation:

The correct answer is C, File Explorer. Here's why:

File Explorer, the file management system in Windows, offers options to control file visibility without resorting to more complex system configurations. The 'Hidden' attribute within File Explorer's properties (accessed by right-clicking a file and selecting 'Properties') allows a user to mark a file as hidden. While this doesn't

prevent deletion if someone deliberately chooses to show hidden files and then delete it, it effectively prevents accidental deletion by casual users who haven't enabled the viewing of hidden items.

Device Manager (A) is used for managing hardware devices connected to the computer, and is completely unrelated to file visibility or protection. Indexing Options (B) configures how Windows indexes files for faster searching; while it affects search results, it doesn't directly prevent accidental deletion. Administrative Tools (D) is a collection of advanced tools for system administration, containing utilities like services management and event viewer; it's also not relevant to a simple file hiding scenario for preventing accidental deletion.

The 'Hidden' attribute is a basic yet effective measure for preventing accidental data loss in shared environments. It leverages user behavior rather than robust security mechanisms. This is a common practice in environments where files need to be shared, but accidental modification or deletion should be minimized.

Further research:

Microsoft File Explorer documentation: https://support.microsoft.com/en-us/windows/file-explorer-in-windows-10-839635e8-aaf1-4dd9-851c-e65fae5e5264
About file attributes: https://www.computerhope.com/jargon/a/attrib.htm

Question: 52

A user is configuring a new SOHO Wi-Fi router for the first time. Which of the following settings should the user change FIRST?

A. Encryption
B. Wi-Fi channel
C. Default passwords
D. Service set identifier

Answer: C

Explanation:

The correct answer is **C. Default passwords**.

Changing the default password of a new SOHO Wi-Fi router is the most crucial initial step for security reasons. Routers ship with well-known default passwords. Leaving these unchanged makes the router and the entire network vulnerable to unauthorized access. Attackers frequently use automated tools that attempt to log in using these default credentials. Once inside the router's configuration, they can change settings, redirect traffic, steal data, or use the network for malicious purposes. This is a basic security hygiene principle known as password management. Changing the password immediately minimizes this risk considerably. While other settings like encryption and SSID are important, they are not as immediately critical as preventing unauthorized access at the administrative level. Think of it like securing the front door before deciding which furniture to buy. After securing the admin access with a strong password, you can move on to configuring encryption, SSID, and Wi-Fi channel to further optimize security and performance.

Authoritative Links:

NIST Guidelines for Password Management:https://www.nist.gov/ (Search for "password management") **FCC on Home Network Security:**https://www.fcc.gov/ (Search for "home network security")

Question: 53

A technician has spent hours trying to resolve a computer issue for the company's Chief Executive Officer (CEO).

The CEO needs the device returned as soon as possible. Which of the following step should the technician take NEXT?

A. Continue researching the issue.
B. Repeat the iterative processes.
C. Inform the CEO the repair will take a couple of weeks.
D. Escalate the ticket.

Answer: D

Explanation:

The correct answer is **D. Escalate the ticket.**

Here's why: Given the CEO's urgency and the technician's prolonged troubleshooting without resolution, escalating the ticket is the most appropriate next step. Continuing to research or repeat processes without a breakthrough suggests the issue may be beyond the technician's current expertise or available resources.
Informing the CEO of a long delay without exploring alternative solutions is unacceptable, especially for a high-priority user.

Escalating the ticket involves transferring the issue to a higher-level support team, a subject matter expert, or a more experienced technician who can offer a fresh perspective or specialized knowledge. This ensures that the problem receives the attention and resources it requires for a timely resolution, minimizing disruption to the CEO's work. This also aligns with service level agreements (SLAs) that often define response and resolution times based on user roles or impact. Proper escalation is a key element of effective incident management, helping organizations to promptly resolve IT issues and restore service. It might also involve engaging vendor support if hardware or software is suspected to be faulty. Prioritizing the CEO's request through escalation maintains good customer service and minimizes potential business impact caused by the unresolved technical issue. Delaying escalation could lead to further frustration and negatively impact productivity.

Question: 54

Which of the following must be maintained throughout the forensic evidence life cycle when dealing with a piece of evidence?

A. Acceptable use
B. Chain of custody
C. Security policy
D. Information management

Answer: B

Explanation:

The correct answer is B, Chain of Custody.

Chain of custody is a meticulously documented chronological record outlining the seizure, custody, control, transfer, analysis, and disposition of evidence, whether physical or digital. It is absolutely crucial in forensic investigations because it ensures the integrity and admissibility of evidence in a court of law. Without a complete and unbroken chain of custody, the evidence can be challenged, deemed unreliable, and potentially excluded from consideration.

Maintaining the chain of custody involves recording everyone who handled the evidence, the dates and times

of each transfer, the purpose of the transfer, and the security measures taken to protect the evidence. Any gap or break in the chain of custody can cast doubt on the authenticity and integrity of the evidence, potentially undermining the entire investigation. Digital evidence, due to its volatile nature and ease of manipulation, requires even stricter adherence to chain of custody principles. Hash values are often calculated and documented at each stage to verify that the data has not been altered.

Acceptable use policies (AUPs) outline the rules and regulations for using an organization's resources, but are not directly related to evidence handling. Security policies govern an organization's overall security posture but don't specifically address forensic evidence handling. Information management concerns the organization and control of data assets, which is broader than the specific requirements of maintaining evidence integrity.

Only chain of custody comprehensively tracks and validates the history of evidence, preserving its legal standing.

For further research, consult resources from the National Institute of Standards and Technology (NIST): https://www.nist.gov/ and search for "digital forensics" and "chain of custody." You can also look into SANS Institute resources: https://www.sans.org/.

Question: 55

A technician is configuring a SOHO device. Company policy dictates that static IP addresses cannot be used. The company wants the server to maintain the same
IP address at all times. Which of the following should the technician use?

A. DHCP reservation
B. Port forwarding
C. DNS A record
D. NAT

Answer: A

Explanation:

The correct answer is A, DHCP reservation. Here's why:

The requirement is for the server to have the same IP address consistently without using static IP configuration. DHCP reservation (also called DHCP static lease) is the perfect solution for this. It allows the DHCP server to dynamically assign IP addresses to devices but reserves a specific IP address for a particular device based on its MAC address.

Here's a breakdown of why the other options are incorrect:

B. Port forwarding: Port forwarding redirects network traffic from one IP address and port number combination to another. It doesn't ensure a device always gets the same IP address. It is used to allow external access to internal servers.

C. DNS A record: A DNS A record maps a domain name to an IP address. While it's crucial for resolving domain names to IP addresses, it doesn't control IP address assignment.

D. NAT (Network Address Translation): NAT translates private IP addresses to public IP addresses and vice-versa. NAT is primarily about allowing multiple devices on a private network to share a single public IP address and not about providing a consistent IP for a single device on the internal network.

DHCP reservation enables centralized IP address management, reducing administrative overhead and preventing IP address conflicts. It combines the benefits of dynamic IP assignment with the predictability of static IP addresses. The DHCP server automatically assigns the reserved IP address whenever the server requests an IP address, thus satisfying the requirement.In summary, DHCP reservation enables assigning a

specific IP address to a device dynamically based on its MAC address ensuring the device maintains the same IP address at all times without using static IP configuration.

For further reading:

DHCP Reservation:

https://www.ibm.com/docs/en/ztpf/2021?topic=configuration-dhcp-static-lease-support
https://kb.netgear.com/27438/How-to-assign-a-static-IP-address-using-DHCP-Reservation

Question: 56

Security software was accidentally uninstalled from all servers in the environment. After requesting the same version of the software be reinstalled, the security analyst learns that a change request will need to be filled out.
Which of the following is the BEST reason to follow the change management process in this scenario?

A. Owners can be notified a change is being made and can monitor it for performance impact.
B. A risk assessment can be performed to determine if the software is needed.
C. End users can be aware of the scope of the change.
D. A rollback plan can be implemented in case the software breaks an application.

Answer: A

Explanation:

The best reason to follow the change management process even when security software was accidentally uninstalled and needs reinstallation is that it ensures owners are notified of the change and can monitor for performance impact (A). Change management provides a structured framework to handle changes in an IT environment, even seemingly straightforward reinstalls. While option D, implementing a rollback plan, is a valid consideration within change management, it's not the best primary reason in this specific scenario.
Here's why:

1. **Notification and Oversight:** Change management mandates notifying stakeholders (owners) about the proposed change. This is crucial because security software impacts system performance and resource utilization. Owners need to be aware so they can observe and address potential performance bottlenecks or conflicts arising from the reinstallation.
2. **Performance Impact Monitoring:** Installing any software, even a reinstall, can affect system stability. The change management process allows for scheduled monitoring during and after the reinstallation. This proactive approach helps identify and resolve performance issues promptly, ensuring minimal disruption to business operations.
3. **Ensuring Compatibility:** Although reinstalling the same version should be compatible, the change management process ensures this is verified. Compatibility issues might have been the underlying cause of the original uninstall, and a check is warranted.
4. **Documentation and Audit Trail:** The change management process documents the change, its rationale, and the steps taken. This creates an audit trail that is essential for compliance, security audits, and future troubleshooting.
5. **Reduced Unplanned Outages:** While a rollback plan (D) is helpful, it's a reactive measure. Change management aims to prevent problems in the first place through careful planning and monitoring, thus reducing unplanned outages.
6. **Communication is key**: Change management is crucial for keeping everyone informed during the transition process, allowing users to understand the situation and reduce interruptions.

While risk assessment (B) and end-user awareness (C) are beneficial elements of change management, the critical immediate concern after security software removal is ensuring the reinstallation doesn't negatively

impact system performance and that stakeholders are aware of the change. Therefore, notifying owners and monitoring the impact (A) is the paramount reason to adhere to the change management process in this instance.

Relevant links:

ITIL Change Management: https://www.bmc.com/blogs/change-management-process/
NIST Guidelines on Change Management: https://csrc.nist.gov/glossary/term/change-management

Question: 57

Once weekly, a user needs Linux to run a specific open-source application that is not available for the currently installed Windows platform. The user has limited bandwidth throughout the day. Which of the following solutions would be the MOST efficient, allowing for parallel execution of the Linux application and Windows applications?

A. Install and run Linux and the required application in a PaaS cloud environment.

B. Install and run Linux and the required application as a virtual machine installed under the Windows OS.

C. Use a swappable drive bay for the boot drive and install each OS with applications on its own drive. Swap the drives as needed.

D. Set up a dual boot system by selecting the option to install Linux alongside Windows.

Answer: B

Explanation:

The best solution for running a Linux application alongside Windows, given the constraints of weekly use and limited bandwidth, is to install Linux and the application as a virtual machine (VM) within Windows. This approach offers several advantages over the other options. A VM allows for parallel execution of both operating systems and their respective applications. The user can run the Windows applications they use daily and then seamlessly launch the Linux VM when needed, without rebooting or physically swapping hardware.

Using a PaaS cloud environment (option A) isn't ideal for this specific scenario because of the limited bandwidth constraint. While PaaS is excellent for application development and deployment, it requires consistent internet connectivity to function. Since the Linux application is only needed weekly, maintaining constant connectivity for it through a PaaS solution is inefficient and costly. Furthermore, uploading the application and potentially dealing with data transfer to the cloud every week consumes unnecessary bandwidth.

A swappable drive bay (option C) and a dual-boot system (option D) are less efficient solutions for several reasons. Swapping drives is cumbersome and time-consuming. Dual-booting requires restarting the computer to switch between operating systems, disrupting workflow and preventing simultaneous operation of Windows and the Linux application. Both options require the user to fully commit to one OS at a time, negating the ability to run applications from both platforms concurrently, which contradicts the requirement for "parallel execution."

Virtualization, on the other hand, provides isolation and resource management. Hypervisors, like VMware Workstation, VirtualBox, or Hyper-V, allow Windows to allocate a specific amount of resources (CPU, RAM, storage) to the Linux VM. This ensures the Linux application can run without significantly impacting the performance of the Windows system, and vice versa. The bandwidth requirements for this method are minimized to the initial download of the Linux distribution ISO and potentially small updates.

Here are some authoritative links about virtualization:

VMware:https://www.vmware.com/topics/virtualization.html
Microsoft Hyper-V:https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/about/

Oracle VirtualBox:https://www.virtualbox.org/

In summary, running Linux and the application as a VM offers the best balance between efficiency, convenience, and minimal bandwidth usage for the user's weekly Linux application needs.

Question: 58

A user connects a laptop that is running Windows 10 to a docking station with external monitors when working at a desk. The user would like to close the laptop when it is docked, but the user reports it goes to sleep when it is closed. Which of the following is the BEST solution to prevent the laptop from going to sleep when it is closed and on the docking station?

A. Within the Power Options of the Control Panel utility, click the Change Plan Settings button for the enabled power plan and select Put the Computer to Sleep under the Plugged In category to Never.

B. Within the Power Options of the Control Panel utility, click the Change Plan Settings button for the enabled power plan and select Put the Computer to Sleep under the On Battery category to Never.

C. Within the Power Options of the Control Panel utility, select the option Choose When to Turn Off the Display and select Turn Off the Display under the Plugged In category to Never.

D. Within the Power Options of the Control Panel utility, select the option Choose What Closing the Lid Does and select When I Close the Lid under the Plugged In category to Do Nothing.

Answer: D

Explanation:

The correct answer is D because it directly addresses the action of closing the laptop lid. The user wants the laptop to remain active while closed and docked.

Option A, while related to power settings, focuses on sleep behavior based on inactivity and not directly on lid closure. Setting "Put the Computer to Sleep" to "Never" under the Plugged In category might prevent sleep in some cases, but it doesn't specifically prevent sleep when the lid is closed. This is an indirect solution at best.

Option B is incorrect because it deals with battery settings. The laptop is docked and plugged in; therefore, the battery settings won't be relevant when the device is connected to external power.

Option C targets turning off the display. While this could be a related issue, the problem is not with the display turning off, but with the laptop going to sleep. Changing the display turn-off setting will not prevent the system from sleeping when the lid is closed.

Option D directly controls what happens when the lid is closed. By navigating to "Choose What Closing the Lid Does" and setting "When I Close the Lid" under the "Plugged In" category to "Do Nothing," the operating system will ignore the lid closure event. This is the most direct and correct approach to solving the user's problem. The laptop will stay active, using the external monitors, even with the lid closed.

https://support.microsoft.com/en-us/windows/how-to-adjust-power-and-sleep-settings-in-windows-9090a43a-19eb-f5e7-6749-d756b8c90f08https://www.dummies.com/article/technology/computers/operating-systems/windows/how-to-change-lid-closing-behavior-in-windows-10-143761/

Question: 59

A user attempts to open some files, but a message appears stating that the files are encrypted. The user was able to access these files before without receiving this message, and no changes have been made within the company. Which of the following has infected the computer?

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

Answer: C

Explanation:

The correct answer is **C. Ransomware**.

Ransomware is a type of malicious software that encrypts a victim's files, rendering them inaccessible until a ransom is paid to the attacker. The message indicating that files are encrypted, coupled with the fact that the user previously accessed them without issue and no company-wide changes occurred, strongly suggests a ransomware infection. Cryptominers (A) use system resources to mine cryptocurrency, which may slow down the computer but wouldn't directly encrypt files. Phishing (B) is a social engineering technique used to trick users into revealing sensitive information, but it doesn't inherently encrypt files. A keylogger (D) records keystrokes, potentially capturing passwords and other data, but does not encrypt files.

Therefore, the symptom of encrypted files only accessible if you pay, which is the presented evidence, points unequivocally to Ransomware. Ransomware attacks often occur rapidly and without obvious user interaction, potentially explaining why the user is unaware of any actions that led to the encryption. They frequently spread via email attachments, malicious websites, or vulnerabilities in software. The urgent message about encryption is often combined with instructions on how to pay the ransom (usually in cryptocurrency).

Further research on ransomware, its prevention, and remediation can be found on cybersecurity vendor websites such as CrowdStrike or Palo Alto Networks, and authoritative sources like the Cybersecurity & Infrastructure Security Agency (CISA) website: https://www.cisa.gov/ and the National Institute of Standards and Technology (NIST): https://www.nist.gov/. Specifically for Ransomware information, please consider this link: https://www.cisa.gov/ransomware.

Question: 60

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? (Choose 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

Answer: AB

Explanation:

The best safety procedures to protect internal computer components when replacing a processor are utilizing an ESD strap and disconnecting the computer from the power source.

A. Utilizing an ESD (Electrostatic Discharge) strap is crucial because static electricity can severely damage sensitive electronic components, including the processor, motherboard, and RAM. An ESD strap, properly

connected to ground, safely dissipates any static charge from the technician's body, preventing it from discharging into the computer components. This is essential for preventing latent or immediate damage to the electronics. [Authoritative Link: See CompTIA A+ certification resources on ESD prevention for electronics.]

B. Disconnecting the computer from the power source is critical to eliminate the risk of electrical shock to the technician and to prevent short circuits that can damage the components. Even when turned off, a computer connected to a power outlet can still carry a charge. Disconnecting it ensures that no current is flowing through the system during the processor replacement, guaranteeing safety and preventing damage.
[Authoritative Link: Hardware Repair Guide's section on safety precautions.]

C. While placing the PSU in an antistatic bag might be useful for storing a PSU, it doesn't address the immediate safety concerns during processor replacement.D. Ensuring proper ventilation and E. Removing dust from ventilation fans are important for the computer's operation and longevity, but are not directly related to protecting the components during the processor replacement process itself. They are preventive maintenance tasks.F. While grounding the equipment is a general electrical safety principle, using an ESD strap provides a more direct and effective method for preventing electrostatic discharge from the technician to the internal components.

Therefore, using an ESD strap to prevent static discharge and disconnecting the power source to prevent electrical hazards are the most appropriate safety measures in this scenario.

Question: 61

A user wants to set up speech recognition on a PC. In which of the following Windows Settings tools can the user enable this option?

A. Language
B. System
C. Personalization
D. Ease of Access

Answer: D

Explanation:

The correct answer is D. Ease of Access.

The Ease of Access settings in Windows are specifically designed to make the computer easier to use for people with disabilities. Speech recognition falls under this category, as it provides an alternative input method for users who may have difficulty using a keyboard or mouse. Within Ease of Access, there is a dedicated section for Speech, where users can enable and configure speech recognition settings.

Options A (Language), B (System), and C (Personalization) are not the correct settings to enable Speech Recognition. The Language settings primarily focus on language packs, keyboard layouts, and regional formats. The System settings contain hardware and system configuration options unrelated to accessibility.
The Personalization settings deal with the visual aspects of Windows, such as themes, backgrounds, and colors. Therefore, selecting Speech Recognition will not be found in these settings.

The Ease of Access (now called Accessibility in newer Windows versions) tools are built into the Windows operating system to provide a more inclusive computing experience. Speech recognition is a key feature within these tools, helping users with limited mobility or other impairments interact with their computers more effectively. Microsoft specifically designates speech recognition tools under accessibility settings.

Further research on this topic can be found in the official Microsoft documentation:

Microsoft Accessibility Support:https://support.microsoft.com/en-us/windows/accessibility-support-for-windows-982e4c7b-6798-35c3-6947-a864d44a63a2
Use voice typing to talk instead of type on your PC:https://support.microsoft.com/en-us/windows/use-voice-typing-to-talk-instead-of-type-on-your-pc-fec94565-c4bd-3629-9ffe-db1a58038305

Question: 62

A user reports that antivirus software indicates a computer is infected with viruses. The user thinks this happened while browsing the internet. The technician does not recognize the interface with which the antivirus message is presented. Which of the following is the NEXT step the technician should take?

A. Shut down the infected computer and swap it with another computer.
B. Investigate what the interface is and what triggered it to pop up.
C. Proceed with initiating a full scan and removal of the viruses using the presented interface.
D. Call the phone number displayed in the interface of the antivirus removal tool.

Answer: B

Explanation:

The correct next step is to investigate the unfamiliar interface and what triggered it. Here's why:

The user reports an antivirus message with an interface the technician doesn't recognize. This strongly suggests a fake antivirus program, also known as scareware or a rogue security program. These programs mimic legitimate antivirus software to trick users into paying for unnecessary or even harmful "services".

Clicking on prompts within this interface could lead to the installation of malware, theft of personal information, or other malicious activities.

Option A (Shut down the infected computer and swap it with another computer) is premature. While isolating a potentially infected system is a good security practice, it's essential to understand the nature of the threat first. Swapping the computer without investigation prevents learning about the infection vector and protecting other systems.

Option C (Proceed with initiating a full scan and removal of the viruses using the presented interface) is highly risky. Interacting with a fake antivirus program is exactly what its creators want. It can lead to further infection and compromise the system.

Option D (Call the phone number displayed in the interface of the antivirus removal tool) is also very dangerous. These phone numbers often connect to scammers who will try to extort money or gain remote access to the computer.

Investigating the interface helps determine if it's genuine antivirus software or a fake. The technician should look for the program's executable file location, examine the program's processes in Task Manager, and search online for the program's name to check its legitimacy. It will also uncover the installation method and trigger. Understanding the source helps to plan the appropriate remediation steps, which might involve using a legitimate antivirus scanner, specialized malware removal tools, or even reinstalling the operating system in severe cases. It also enables implementing preventative measures.

In short, due diligence and information gathering are crucial before taking any action on a suspected malware infection. Jumping to conclusions without investigation can worsen the situation.

Further reading:

Rogue security software:https://en.wikipedia.org/wiki/Rogue_security_software
Scareware:https://us.norton.com/internetsecurity-malware-what-is-scareware.html

Question: 63

A technician found that an employee is mining cryptocurrency on a work desktop. The company has decided that this action violates its guidelines. Which of the following should be updated to reflect this new requirement?

A. MDM
B. EULA
C. IRP
D. AUP

Answer: D

Explanation:

The correct answer is D. AUP (Acceptable Use Policy). An AUP outlines what users are and are not allowed to do with company resources, including computers and network access. Mining cryptocurrency on a company desktop violates acceptable use because it consumes resources (processing power, electricity, bandwidth) that are intended for business purposes. It also introduces security risks, such as malware and unauthorized network activity. The company's decision to prohibit cryptocurrency mining necessitates updating the AUP to explicitly state this prohibition.

Let's examine why the other options are less suitable. MDM (Mobile Device Management) primarily concerns the management and security of mobile devices, not desktop computers. A EULA (End-User License Agreement) governs the use of specific software, not general computer usage guidelines. An IRP (Incident Response Plan) details the procedures for handling security incidents after they occur. While a cryptocurrency mining incident might trigger the IRP, the policy prohibiting it in the first place belongs in the AUP. Updating the AUP proactively prevents future incidents.

Therefore, the most appropriate response is to update the AUP to reflect the company's stance against cryptocurrency mining on its devices and network. This ensures employees are aware of the new restriction.

Further Reading:

SANS Institute on Acceptable Use Policies: https://www.sans.org/information-security-policy/
NIST Cybersecurity Framework: https://www.nist.gov/cyberframework (While not directly AUP-focused, it outlines overall cybersecurity policy management.)

Question: 64

An organization is centralizing support functions and requires the ability to support a remote user's desktop. Which of the following technologies will allow a technician to see the issue along with the user?

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

Answer: B

Explanation:

The correct answer is **B. VNC (Virtual Network Computing)** because it allows a technician to directly see and interact with the remote user's desktop graphically. RDP (Remote Desktop Protocol) also provides graphical

access, but it usually creates a separate session for the technician, disconnecting the user or providing a separate, potentially non-identical view of the desktop. VNC, on the other hand, typically mirrors the existing user's session, allowing both the user and the technician to see the same screen simultaneously, facilitating effective collaboration and troubleshooting.

SSH (Secure Shell) is a command-line interface, providing secure remote access to a server or device, but it doesn't offer a visual representation of the user's desktop. It's suitable for tasks like system administration and file transfer, not for visually assisting a user with desktop problems. A VPN (Virtual Private Network) creates a secure, encrypted tunnel for network traffic, enabling secure access to the organization's network from a remote location. While a VPN is crucial for secure remote access, it doesn't, on its own, provide screen sharing or remote desktop capabilities needed to view the user's desktop issue. VNC's ability to share the exact same screen with a user is crucial when centralizing support functions requiring visual assistance and real-time collaboration, making it the most appropriate choice for addressing the stated requirements. It allows the technician to guide the user through the issue while both can see the same screen.

For further information:

VNC:https://www.realvnc.com/en/
RDP:https://learn.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients/remote-desktop-clients
SSH:https://www.ssh.com/ssh/
VPN:https://www.cloudflare.com/learning/security/glossary/what-is-vpn/

Question: 65

Which of the following provide the BEST way to secure physical access to a data center server room? (Choose two.)

A. Biometric lock
B. Badge reader
C. USB token
D. Video surveillance
E. Locking rack
F. Access control vestibule

Answer: AB

Explanation:

The best methods for securing physical access to a data center server room focus on controlling and monitoring who enters the space. A biometric lock (A) provides a strong layer of security by verifying an individual's identity using unique biological traits, such as fingerprints or iris scans. This prevents
unauthorized access even if someone obtains a physical key or password, as the individual's biometrics are required for entry. Badge readers (B) are another effective method, using access cards or fobs to grant entry. These systems can be integrated with access control software, allowing administrators to track who enters and exits the server room, and to quickly revoke access if necessary. They also provide an audit trail for security investigations.

While video surveillance (D) can provide valuable evidence in the event of a security breach, it doesn't actively prevent unauthorized access. It's more of a reactive measure. Locking racks (E) secure the servers within the room, but do not control entry into the room itself. USB tokens (C) are typically used for logical access control to systems, not physical access to a facility. An access control vestibule (F) is a good security measure and a valid option but a combination of Biometric lock and a badge reader offers a layered and more immediately verifiable solution. The combination of biometric authentication and badge readers creates a multi-factor

authentication approach, significantly reducing the risk of unauthorized physical access.

Therefore, biometric locks and badge readers offer the most direct and effective means of physically securing a data center server room by controlling who is permitted entry in the first place.

Relevant resources for further information include:

NIST Guidelines on Electronic Authentication:https://csrc.nist.gov/publications/detail/sp/800-63/3/final
Data Center Security Best Practices: (Search for reputable IT security firms and publications like SANS Institute or OWASP for detailed guides)

Question: 66

Which of the following Wi-Fi protocols is the MOST secure?

A. WPA3
B. WPA-AES
C. WEP
D. WPA-TKIP

Answer: A

Explanation:

The correct answer is A, WPA3. Here's why:

WPA3 (Wi-Fi Protected Access 3) is the most secure Wi-Fi protocol among the options listed because it incorporates several advanced security features that address vulnerabilities present in its predecessors. Specifically, WPA3 uses Simultaneous Authentication of Equals (SAE), also known as Dragonfly handshake, which provides a more robust defense against password cracking attempts compared to the pre-shared key (PSK) method used in WPA2. SAE makes it much harder for attackers to guess passwords, even weak ones, through offline dictionary attacks.

Furthermore, WPA3 offers enhanced data encryption using Galois/Counter Mode Protocol (GCMP-256) for improved confidentiality and integrity of wireless communications. This represents a significant upgrade from WPA2, which typically uses AES-CCMP. WPA3 also includes a feature called Wi-Fi Enhanced Open, which provides opportunistic wireless encryption (OWE) for open Wi-Fi networks, protecting data in transit even when a password is not required.

WPA-AES (using AES encryption with WPA2) is more secure than WEP and WPA-TKIP, but it's less secure than WPA3. WEP (Wired Equivalent Privacy) is an outdated and highly vulnerable protocol that should never be used. WPA-TKIP (Temporal Key Integrity Protocol) is also considered insecure and has been superseded by more modern protocols. It has known vulnerabilities and is susceptible to attacks.

In summary, WPA3's advanced features, including SAE authentication, stronger encryption with GCMP-256, and opportunistic wireless encryption, provide the best level of security for Wi-Fi networks, making it the most secure option among the choices.

Authoritative Links for Further Research:

Wi-Fi Alliance on WPA3:https://www.wi-fi.org/discover-wi-fi/security
WPA3 - Wikipedia:https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access#WPA3

Question: 67

A department has the following technical requirements for a new application:

Quad Core processor -
250GB of hard drive space
6GB of RAM

Touch screens -
The company plans to upgrade from a 32-bit Windows OS to a 64-bit OS. Which of the following will the company be able to fully take advantage of after the upgrade?

A. CPU
B. Hard drive
C. RAM
D. Touch screen

Answer: C

Explanation:

The correct answer is RAM. Here's why:

A 32-bit operating system has inherent limitations on the amount of RAM it can address. This is due to the way memory addresses are handled. A 32-bit system uses 32 bits to represent a memory address, which limits the addressable memory space to 2^32 bytes, or 4GB. In practice, even less than 4GB is usable due to hardware reservations.

Upgrading to a 64-bit operating system expands the addressable memory space significantly. A 64-bit system uses 64 bits to represent a memory address, allowing it to theoretically address up to 2^64 bytes of RAM, a massive amount far exceeding current hardware capabilities. This means the system can utilize RAM far beyond the 4GB limit imposed by 32-bit systems.

In the scenario, the requirement of 6GB of RAM cannot be fully met by a 32-bit OS. Only after the upgrade to a 64-bit OS will the application be able to fully utilize the required 6GB of RAM.

The CPU's core count (Quad Core) functions independently of the OS architecture (32-bit or 64-bit). Both 32-bit and 64-bit operating systems can support multi-core processors. The hard drive's storage capacity (250GB) is also not directly affected by the OS architecture; both can support hard drives of that size. Touchscreen functionality is primarily determined by hardware drivers and OS compatibility, not the OS's bitness (32-bit or 64-bit). The OS must have appropriate drivers for the specific touchscreen. However, the ability to use the full 6 GB of RAM is directly and dramatically affected by the shift to a 64-bit operating system.

Further resources:

Microsoft - Memory Limits for Windows and Windows Server:https://docs.microsoft.com/en-us/windows/win32/memory/memory-limits-for-windows-releases (Although focusing on Windows, the concept of memory limits and 32-bit vs 64-bit OS applies broadly.)

GeeksforGeeks - Difference between 32 bit and 64 bit Operating System:
https://www.geeksforgeeks.org/difference-between-32-bit-and-64-bit-operating-system/

Question: 68

A user is unable to log in to the domain with a desktop PC, but a laptop PC is working properly on the same

network. A technician logs in to the desktop PC with a local account but is unable to browse to the secure intranet site to get troubleshooting tools. Which of the following is the MOST likely cause of the issue?

A. Time drift
B. Dual in-line memory module failure
C. Application crash
D. Filesystem errors

Answer: A

Explanation:

Here's a detailed justification for why time drift is the most likely cause in this scenario:

The scenario presents two key symptoms: domain login failure on the desktop PC and inability to access a secure intranet site even when logged in locally. The fact that a laptop on the same network works fine suggests a problem specific to the desktop PC and not the network infrastructure itself.

Time drift, where the system time on the desktop significantly deviates from the domain controller's time, explains both symptoms. Domain authentication protocols, like Kerberos, are extremely time-sensitive. If the desktop's clock is too far off from the domain controller's clock, authentication will fail. Kerberos, in particular, uses timestamps for security and to prevent replay attacks. A significant time difference makes the authentication tokens appear invalid.

Secondly, secure intranet sites often rely on SSL/TLS certificates for secure communication. These certificates have validity periods. If the desktop's time is drastically wrong (either ahead or behind), the browser might incorrectly interpret the certificate as expired or not yet valid, preventing access to the secure site even with a local account.

While other issues could potentially contribute, time drift is the most direct and common cause that would simultaneously lead to domain login failure and secure site access problems. It's much more likely than a memory module failure selectively affecting network authentication and certificate validation (B), a general application crash preventing only intranet access (C), or file system errors preventing network and secure site access (D). Moreover, A+ certification emphasizes troubleshooting common user problems, and time synchronization issues are a frequent occurrence in networked environments. NTP (Network Time Protocol) servers are crucial for keeping systems in sync.

Authoritative links:

Microsoft on Kerberos and Time Skew:https://support.microsoft.com/en-us/topic/how-kerberos-version-5-authentication-works-9565b931-ddaf-40a8-a268-6c32f96a9762
NIST on NTP:https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-framework/online-learning/time-synchronization

Question: 69

A user reports that a workstation is operating sluggishly. Several other users operate on the same workstation and have reported that the workstation is operating normally. The systems administrator has validated that the workstation functions normally. Which of the following steps should the systems administrator most likely attempt NEXT?

A. Increase the paging file size.
B. Run the chkdsk command.
C. Rebuild the user's profile.
D. Add more system memory.

E. Defragment the hard drive.

Answer: C

Explanation:

The answer is C: Rebuild the user's profile.

Here's a detailed justification:

The problem is isolated to a single user experiencing sluggish performance on a workstation that otherwise functions normally for other users and the administrator. This strongly suggests a user-specific issue rather than a system-wide hardware or software problem.

Options like increasing the paging file size (A), running chkdsk (B), adding more system memory (D), or defragmenting the hard drive (E) address system-level performance bottlenecks. These actions would likely impact all users, which isn't the case here. While those steps could potentially improve overall performance, they are not the most likely next step given the specific symptoms. These actions are also more disruptive to all users of the workstation.

A corrupted or bloated user profile can cause sluggish performance, specifically for that user. The profile contains user-specific settings, temporary files, cached data, and application configurations. Corruption within these files can lead to slow application loading times, errors, and general sluggishness. Rebuilding the profile essentially creates a fresh start for the user's configuration, potentially resolving issues caused by the corrupted data. Before rebuilding, backing up the existing profile is crucial to prevent data loss. If the rebuild fixes the problem, then the issue was profile related. If the rebuild does not fix the problem, you know it is something else.

Therefore, rebuilding the user's profile is the most targeted and logical first step to address a user-specific performance issue on a shared workstation that otherwise functions normally.

Further Reading:

Microsoft Documentation on User Profiles: https://learn.microsoft.com/en-us/windows-server/identity/user-profiles/user-profiles-overview
Troubleshooting Slow Performance on Windows: (Although not specifically about user profiles, it offers general performance troubleshooting steps): https://support.microsoft.com/en-us/windows/tips-to-improve-pc-performance-in-windows-b3b0ef55-593a-fa74-2d4c-46ff662a645b

Question: 70

A technician is setting up a desktop computer in a small office. The user will need to access files on a drive shared from another desktop on the network. Which of the following configurations should the technician employ to achieve this goal?

A. Configure the network as private.
B. Enable a proxy server.
C. Grant the network administrator role to the user.
D. Create a shortcut to public documents.

Answer: A

Explanation:

The correct answer is A, configuring the network as private. Here's why:

When a network is configured as "private" (also sometimes referred to as "home" or "work" network), it enables features like network discovery and file/printer sharing. This allows the desktop computer being set up to see other devices on the local network, including the desktop sharing the files. Windows, for instance, manages network profiles (public, private, domain), with private profiles offering the necessary permissions and firewall exceptions for seamless local network interactions.

Option B, enabling a proxy server, is incorrect because a proxy server is generally used to mediate internet traffic, not local network file sharing. It doesn't directly enable file sharing capabilities within the local network.

Option C, granting the user network administrator role, is also incorrect. While administrator privileges might be needed for certain network configuration changes, granting the user such broad access solely for accessing shared files is a security risk and unnecessary. File sharing can be configured with standard user accounts and appropriate share permissions.

Option D, creating a shortcut to public documents, while seemingly relevant, wouldn't work effectively without first establishing the underlying network connectivity and file sharing configurations. The shortcut relies on the network being properly configured to access the shared drive. Simply creating a shortcut without the right network settings in place will result in an error.

Therefore, setting the network to private is the most fundamental and appropriate step to enable file sharing in a small office environment. It establishes the foundation upon which file sharing permissions and access can then be configured.

For further research:

Microsoft's documentation on network discovery and file sharing:https://support.microsoft.com/en-us/windows/file-sharing-over-a-network-in-windows-b5870c92-f66b-3766-390c-7d8e71aa73a8
Understanding Network Profiles in Windows:https://www.dummies.com/computers/operating-systems/windows-10/understanding-network-location-profiles-in-windows-10/ (This is a non-official resource, but it does a good job explaining network profiles.)

Question: 71

Which of the following is a proprietary Cisco AAA protocol?

A. TKIP
B. AES
C. RADIUS.
D. TACACS+

Answer: D

Explanation:

TACACS+ (Terminal Access Controller Access-Control System Plus) is the correct answer because it is a Cisco proprietary protocol used for AAA (Authentication, Authorization, and Accounting). AAA protocols are critical for network security and management, handling user authentication, granting appropriate access levels, and tracking user activities on the network. TACACS+ differs from RADIUS in several ways. While RADIUS combines authentication and authorization, TACACS+ separates them. This separation provides greater flexibility in controlling user access. TACACS+ uses TCP port 49, offering reliable transport, whereas RADIUS uses UDP. TACACS+ encrypts the entire packet body during communication, providing more secure transmission of data compared to RADIUS, which only encrypts the password.

TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard) are encryption protocols

primarily associated with wireless security (specifically Wi-Fi protected Access (WPA) and WPA2). While essential for secure communication, they don't serve the purpose of centralized AAA management. RADIUS (Remote Authentication Dial-In User Service) is a widely used AAA protocol, but it's an open standard, not proprietary to Cisco.

In cloud environments and enterprise networks, AAA protocols are essential for controlling access to resources, tracking usage, and maintaining security policies. Cisco often employs TACACS+ for its network devices to enforce fine-grained control over administrative access and ensure a robust security posture. The enhanced security features of TACACS+, like full packet encryption, are particularly beneficial in
environments where sensitive information is transmitted. Choosing the correct AAA protocol helps manage network access, monitor user activity, and maintain a high level of security compliance.

Relevant links:

Cisco TACACS+ overview: https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs/10594-tacacs-radius.html
RADIUS Protocol: https://datatracker.ietf.org/doc/html/rfc2865

Question: 72

A technician is asked to resize a partition on the internal storage drive of a computer running macOS. Which of the followings tools should the technician use to accomplish this task?

A.Console
B.Disk Utility
C.Time Machine
D.FileVault

Answer: B

Explanation:

The correct answer is Disk Utility. Disk Utility is the native macOS application designed for managing disks, partitions, and volumes. It offers a graphical user interface (GUI) specifically for tasks such as formatting drives, partitioning disks, repairing disk errors, creating disk images, and, importantly, resizing partitions.

Option A, Console, is primarily used for viewing system logs and debugging applications, not for disk management tasks. Option C, Time Machine, is macOS's built-in backup solution, responsible for creating and restoring system backups, but it does not directly manipulate partition sizes. Option D, FileVault, is a disk encryption program that encrypts the entire startup disk, securing its contents, but it doesn't handle partition resizing either.

Therefore, Disk Utility is the only application among the choices that provides the necessary functionality to resize partitions on a macOS system. The other options are designed for different purposes related to system management and data security, but they don't offer partition resizing capabilities.

For further details, you can refer to Apple's official documentation on Disk Utility:

https://support.apple.com/guide/disk-utility/welcome/mac

Question: 73

A desktop specialist needs to prepare a laptop running Windows 10 for a newly hired employee. Which of the

following methods should the technician use to refresh the laptop?

A. Internet-based upgrade
B. Repair installation
C. Clean install
D. USB repair
E. In-place upgrade

Answer: C

Explanation:

The correct method to prepare a laptop for a new employee and ensure it's in a clean, consistent state is a Clean Install (C). Here's why:

A clean install completely erases the existing operating system, applications, and user data. It then installs a fresh copy of Windows 10. This is the best way to ensure there are no remnants of the previous user's data, configurations, or potential malware. It minimizes security risks and ensures a standardized and predictable environment for the new employee.

Internet-based upgrade (A) and In-place upgrade (E) keep existing files and configurations, potentially carrying over problems or unwanted software. A repair installation (B) attempts to fix the existing OS without removing it, which is unsuitable when starting fresh for a new user. USB repair (D) may not wipe the hard drive entirely.

A clean install offers a pristine environment, free from bloatware or conflicting configurations, optimizing performance and reducing potential support issues down the line. This is particularly important in a corporate environment where consistency and security are paramount. This method is more involved initially but saves time and resources in the long run by preventing future issues stemming from remnants of a previous installation. Using a clean install guarantees a standard image, crucial for IT management and software deployments.

For further research, consider exploring Microsoft's documentation on clean installing Windows 10:

How to Clean Install Windows 10
Clean Install vs. Fresh Start - What's the Difference?

Question: 74

A user reports that a PC seems to be running more slowly than usual. A technician checks system resources, but disk, CPU, and memory usage seem to be fine.
The technician sees that GPU temperature is extremely high. Which of the following types of malware is MOST likely to blame?

A. Spyware
B. Cryptominer
C. Ransomware
D. Boot sector virus

Answer: B

Explanation:

The correct answer is B. Cryptominer. Here's a detailed justification:

Cryptominers are a type of malware that utilizes a computer's resources, especially the GPU, to mine cryptocurrency without the user's consent. The high GPU temperature is a key indicator. Cryptomining is a computationally intensive process that puts a heavy load on the GPU, leading to increased heat generation. When a system's CPU, disk, and memory usage seem normal but the GPU is overheating, it strongly suggests that the GPU is being heavily utilized for purposes the user is unaware of, such as cryptocurrency mining by malware.

Spyware (A) primarily focuses on collecting user data and doesn't typically push the GPU to its thermal limits.
While it may cause some slowdown, the GPU overheating is not a characteristic symptom. Ransomware (C) locks users out of their system or data and demands payment, but again, this doesn't necessarily involve sustained high GPU usage leading to overheating. A boot sector virus (D) infects the boot sector of a hard drive, which can lead to boot problems and general instability. It also wouldn't characteristically drive the GPU to extremely high temperatures.

Cryptomining malware has become increasingly prevalent, taking advantage of unsuspecting users' systems for illicit profit. Because of the processing power needed for mining, the GPU is a prime target. This constant, intensive activity leads to overheating and system slowdowns.

For further research, consider the following resources:

Malwarebytes: (https://www.malwarebytes.com/cryptojacking) Discusses cryptojacking and its impact on system resources.

Avast: (https://www.avast.com/c-cryptojacking) Explains the nature of cryptojacking and its symptoms.

Question: 75

A user is experiencing frequent malware symptoms on a Windows workstation. The user has tried several times to roll back the state, but the malware persists.
Which of the following would MOST likely resolve the issue?

A. Quarantining system files
B. Reimaging the workstation
C. Encrypting the hard drive
D. Disabling TLS 1.0 support

Answer: B

Explanation:

Reimaging the workstation (option B) is the most effective solution in this scenario because it completely overwrites the existing operating system and reinstalls a clean, known-good image. Since the user has attempted system restore with no success, the malware is likely deeply embedded within the system files, boot sector, or other critical areas that are not easily removed by antivirus software or system restore.

Quarantining system files (option A) is risky because it can lead to system instability and is unlikely to remove persistent malware. Encrypting the hard drive (option C) will not remove the malware; it will only encrypt the infected system. Disabling TLS 1.0 support (option D) is a security best practice, but it addresses vulnerabilities related to communication protocols, not malware infections.

Reimaging ensures that all traces of the malware are removed, including any rootkits or persistent infections that may be preventing system restore from working correctly. It essentially returns the workstation to a clean state before the malware infection occurred. This is the fastest and most reliable way to guarantee complete removal of deeply entrenched malware, especially when standard removal methods have failed. A

good strategy following reimaging would be to ensure the user is educated on safe browsing habits and that an effective endpoint protection solution is deployed and regularly updated.

For further research, consider these resources:

Microsoft Documentation on Recovery Options:https://support.microsoft.com/en-us/windows/recovery-options-in-windows-31ce2444-7de3-818c-d626-e5b3a3024da5
NIST Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Question: 76

A change advisory board did not approve a requested change due to the lack of alternative actions if implementation failed. Which of the following should be updated before requesting approval again?

A. Scope of change
B. Risk level
C. Rollback plan
D. End user acceptance

Answer: C

Explanation:

The correct answer is C, Rollback plan. The scenario explicitly states the change advisory board (CAB) rejected the change request because of a lack of alternative actions if the implementation failed. A rollback plan details the steps to revert a system or service to its previous state in case of a failed or problematic change. This plan outlines how to undo the implemented changes, minimizing disruption and ensuring business continuity. It's a crucial component of change management, especially in environments where changes can have significant impacts. Without a well-defined rollback plan, a failed change can lead to prolonged downtime, data loss, and user dissatisfaction. Options A (Scope of change), B (Risk level), and D (End-user acceptance) are important aspects of change management, but they don't directly address the CAB's concern about failed implementation alternatives. While reducing the scope or risk might be helpful in some cases, the immediate need is a plan to recover if things go wrong. Similarly, end-user acceptance testing comes after successful implementation, not as a fallback. The rollback plan provides the necessary safety net and contingency, making it the most pertinent update for re-submission to the CAB. A
comprehensive rollback plan typically includes steps like identifying critical dependencies, creating backups, documenting the restoration process, and assigning responsibilities.

Further reading on change management best practices:

ITIL 4 Foundation: https://www.axelos.com/certifications/itil-service-management
NIST Special Publication 800-100: Information Security Handbook: A Guide for Managers:
https://csrc.nist.gov/publications/detail/sp/800-100/rev-1/final (While focusing on security, it covers general IT management principles).

Question: 77

A technician is setting up a new laptop. The company's security policy states that users cannot install virtual machines. Which of the following should the technician implement to prevent users from enabling virtual technology on their laptops?

A. UEFI password

B. Secure boot
C. Account lockout
D. Restricted user permissions

Answer: A

Explanation:

The correct answer is **A. UEFI password**. Here's why:

A **UEFI (Unified Extensible Firmware Interface) password** restricts access to the system's firmware settings. Virtualization technology, like Intel VT-x or AMD-V, is often enabled or disabled within the UEFI/BIOS settings. Setting a strong UEFI password prevents users from entering the UEFI setup and enabling virtualization features. This aligns directly with the company's policy of preventing users from installing virtual machines.

Secure Boot (B), while a security feature, primarily focuses on ensuring that only trusted operating system loaders and UEFI drivers are executed during the boot process. It doesn't directly prevent the enabling of virtualization in the UEFI settings.

Account lockout (C) is a security measure that disables a user account after a certain number of failed login attempts. This is irrelevant to the UEFI settings or virtualization.

Restricted user permissions (D) limits what a user can do within the operating system (e.g., installing software, changing system settings). However, enabling virtualization is often a hardware-level function controlled by the UEFI and is not directly impacted by operating system user permissions. An administrator can enable virtualization in UEFI and the user with restricted permissions could still use it.

Therefore, setting a UEFI password provides a preventative measure at the hardware level, ensuring that unauthorized users cannot enable virtualization. This is the most direct and effective way to enforce the company's policy.

Further research:

UEFI:https://uefi.org/
BIOS security: Search for "BIOS security best practices" in your preferred search engine.

Question: 78

During a recent flight, an executive unexpectedly received several dog and cat pictures while trying to watch a movie via in-flight Wi-Fi on an iPhone. The executive has no records of any contacts sending pictures like these and has not seen these pictures before. To BEST resolve this issue, the executive should:

A. set AirDrop so that transfers are only accepted from known contacts.
B. completely disable all wireless systems during the flight.
C. discontinue using iMessage and only use secure communication applications.
D. only allow messages and calls from saved contacts.

Answer: A

Explanation:

The correct answer is A: set AirDrop so that transfers are only accepted from known contacts.

Here's why: The executive is receiving unwanted pictures via AirDrop. AirDrop is Apple's proprietary ad-hoc service that allows file transfers among supported iOS and macOS devices over Wi-Fi and Bluetooth. The key issue is that the AirDrop setting is likely set to "Everyone," allowing anyone within range to send files.

Changing the AirDrop setting to "Contacts Only" means that only people in the executive's contact list can send files. This is the most targeted and minimally disruptive solution.

Option B is too extreme. Completely disabling all wireless systems prevents the executive from using any network connectivity.

Option C is related to messaging security but doesn't directly address the problem of unwanted AirDrop transfers. While using secure communication apps is generally good practice, it doesn't prevent someone from sending unwanted files via AirDrop.

Option D, while providing some level of contact filtering, is not relevant to the issue of AirDrop. The executive is receiving unsolicited files, not necessarily messages or calls. AirDrop operates independently of contact-based messaging or calling features.

Therefore, configuring AirDrop to accept transfers only from known contacts directly targets the source of the problem (unsolicited AirDrop transfers) without significantly impacting the executive's ability to use other wireless functionalities.

Supporting Documentation:

Apple Support - Use AirDrop on your iPhone, iPad, or iPod touch: https://support.apple.com/en-us/HT204144 (This official Apple documentation explains how to adjust AirDrop settings and their implications for file transfer privacy.)

Question: 79

A technician receives a call from a user who is unable to open Outlook. The user states that Outlook worked fine yesterday, but the computer may have restarted sometime overnight. Which of the following is the MOST likely reason Outlook has stopped functioning?

A. Spam filter installation
B. Invalid registry settings
C. Malware infection
D. Operating system update

Answer: D

Explanation:

The most likely reason Outlook has stopped functioning after a computer restart, especially after a possible overnight operating system update, is an operating system update (D). Here's why:

Operating system updates often involve significant changes to system files, libraries, and configurations. These updates can sometimes interfere with the proper functioning of applications, especially those deeply integrated with the OS like Outlook. During an OS update, files required by Outlook might be modified, replaced, or moved, leading to compatibility issues.

Spam filter installations (A) are less likely to cause a sudden failure of Outlook after a reboot. While a new spam filter could potentially interfere with incoming or outgoing emails, it wouldn't typically prevent Outlook from opening altogether. Invalid registry settings (B) could certainly cause problems with Outlook, but the sudden onset after a system restart suggests an external trigger like an update rather than spontaneous registry corruption. Malware infection (C) is a possibility, but the fact that Outlook worked fine the previous day makes an OS update a more plausible initial suspect. Malware often has broader impacts beyond a single application failure.

An operating system update is a major system event that often involves restarting the computer. The update

process might disrupt services that Outlook relies on, or it might change settings that are necessary for Outlook to function correctly. The timing aligns perfectly with the user's report of the computer restarting overnight. Further, Windows updates are notorious for occasionally causing application issues.
Troubleshooting should start with verifying a successful OS update and checking logs for related errors.

Consider the following: Windows Update can sometimes break application compatibility; a recent update might have modified or corrupted necessary Outlook files or settings, causing the application to fail on launch. This is a common occurrence and thus, makes (D) the MOST likely reason.

Authoritative link: https://support.microsoft.com/en-us/windows

Question: 80

A bank would like to enhance building security in order to prevent vehicles from driving into the building while also maintaining easy access for customers. Which of the following BEST addresses this need?

A. Guards
B. Bollards
C. Motion sensors
D. Access control vestibule

Answer: B

Explanation:

The correct answer is B, Bollards. Here's why:

Bollards are short, sturdy posts designed to prevent vehicles from crossing a boundary. They are a physical security measure specifically intended to stop vehicular attacks or accidental vehicle incursions into pedestrian areas or buildings. This directly addresses the bank's need to prevent vehicles from driving into the building.

Guards (A) can provide security presence and observation, but they cannot physically stop a moving vehicle.
They are more focused on access control and identifying potential threats. Motion sensors (C) detect movement but don't prevent vehicles from approaching or impacting the building. They are primarily used for alarm systems. An access control vestibule (D) controls personnel access into the building, creating a secure entry point by allowing only one door to be open at a time. While valuable for personnel security, it doesn't specifically prevent vehicles from impacting the building's exterior.

Bollards offer a passive, physical barrier, effectively stopping vehicles while often allowing pedestrian access.
They can be designed aesthetically to blend into the building's architecture, maintaining a welcoming appearance for customers while providing robust security. For a bank seeking to prevent vehicle incursions while preserving easy customer access, bollards are the optimal solution because they do not require active monitoring or intervention, yet provide a concrete, physical barrier. Furthermore, modern bollard designs can be retractable, allowing for occasional vehicle access for deliveries or maintenance while maintaining security during normal operation. They are a physical deterrent explicitly designed for this threat vector.

Further Reading:

National Academies of Sciences, Engineering, and Medicine. 2020. Vehicle Barriers and Mitigation Strategies.
Washington, DC: The National Academies Press. https://doi.org/10.17226/25936 Whole
Building Design Guide (WBDG): https://www.wbdg.org/ (Search for "bollards")