



# CompTIA

## Exam Questions 220-1102

CompTIA A+ Certification Exam: Core 2

## About ExamBible

### *Your Partner of IT Exam*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

#### NEW QUESTION 1

A systems administrator is monitoring an unusual amount of network traffic from a kiosk machine and needs to investigate to determine the source of the traffic. Which of the following tools can the administrator use to view which processes on the kiosk machine are connecting to the internet?

- A. Resource Monitor
- B. Performance Monitor
- C. Command Prompt
- D. System Information

**Answer:** A

#### Explanation:

Resource Monitor is a tool that shows the network activity of each process on a Windows machine, including the TCP connections and the sent and received bytes. Performance Monitor is a tool that shows the performance metrics of the system, such as CPU, memory, disk and network usage. Command Prompt is a tool that allows running commands and scripts on a Windows machine. System Information is a tool that shows the hardware and software configuration of a Windows machine. Verified References:

<https://www.comptia.org/blog/how-to-use-resource-monitor> <https://www.comptia.org/certifications/a>

#### NEW QUESTION 2

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:

Chrome OS provides a lightweight option for workstations that need an easy-to-use browser-based interface.

#### NEW QUESTION 3

Which of the following data is MOST likely to be regulated?

- A. Name in a Phone book
- B. Name on a medical diagnosis
- C. Name on a job application
- D. Name on a employer's website

**Answer:** B

#### Explanation:

A name on a medical diagnosis (B) is most likely to be regulated. This is because it falls under the category of protected health information (PHI), which is subject to regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States. These regulations aim to protect the privacy and security of individuals' health information.

#### NEW QUESTION 4

A customer installed a new web browser from an unsolicited USB drive that the customer received in the mail. The browser is not working as expected, and internet searches are redirected to another site. Which of the following should the user do next after uninstalling the browser?

- A. Delete the browser cookies and history.
- B. Reset all browser settings.
- C. Change the browser default search engine.
- D. Install a trusted browser.

**Answer:** D

#### Explanation:

The customer's web browser is likely infected by a browser hijacker, which is a type of malware that changes the browser's settings and redirects the user to malicious websites. A browser hijacker can also steal the user's personal data, display unwanted ads, and install more malware on the device. To remove a browser hijacker, the user should first uninstall the browser from the Control Panel, then scan the device with an antivirus or anti-malware program, and finally install a trusted browser from a legitimate source. Deleting the browser cookies and history, resetting the browser settings, or changing the browser default search engine may not be enough to get rid of the browser hijacker, as it may have embedded itself into the system or other browser components.

#### NEW QUESTION 5

A technician at a customer site is troubleshooting a laptop. A software update needs to be downloaded but the company's proxy is blocking traffic to the update site. Which of the following should the technician perform?

- A. Change the DNS address to 1.1.1.1
- B. Update Group Policy
- C. Add the site to the client's exceptions list
- D. Verify the software license is current.

**Answer:** C

**Explanation:**

The technician should add the update site to the client's exceptions list to bypass the proxy. This can be done through the client's web browser settings, where the proxy settings can be configured. By adding the update site to the exceptions list, the client will be able to access the site and download the software update.

**NEW QUESTION 6**

A technician is troubleshooting a Windows 10 PC that is unable to start the GUI. A new SSD and a new copy of Windows were recently installed on the PC. Which of the following is the most appropriate command to use to fix the issue?

- A. msconfig
- B. chkdsk
- C. sfc
- D. diskpart
- E. mstsc

**Answer: C**

**Explanation:**

The sfc command is a tool for scanning and repairing system files that are corrupted or missing on Windows operating systems<sup>12</sup>. System files are essential files that are required for the proper functioning of the operating system, such as the GUI, drivers, services, and applications. If system files are damaged or deleted, the operating system may fail to start or run properly, causing errors, crashes, or blue screens.

The sfc command can be used to fix the issue of the PC that is unable to start the GUI, assuming that the problem is caused by corrupted or missing system files. The sfc command can be run from the command prompt, which can be accessed by booting the PC from the installation media, choosing the repair option, and selecting the command prompt option<sup>3</sup>. The sfc command can be used with different switches, such as /scannow, /verifyonly, /scanfile, or /offbootdir, depending on the situation and the desired action<sup>4</sup>. The

most common switch is /scannow, which scans all the system files and repairs any problems that are found<sup>5</sup>. The syntax of the sfc command with the /scannow switch is: sfc /scannow

The sfc command will then scan and repair the system files, and display the results on the screen. If the sfc command is able to fix the system files, the PC should be able to start the GUI normally after rebooting. If the sfc command is unable to fix the system files, the PC may need further troubleshooting or a clean installation of Windows.

References<sup>1</sup>: CompTIA A+ Certification Exam Core 2 Objectives, page 10 <sup>2</sup>: CompTIA A+ Core 2 (220-1102) Complete Video Course, Lesson 26 Documentation

<sup>3</sup>: How to use SFC Scannow to repair Windows system files <sup>4</sup>: SFC Command (System File Checker) <sup>5</sup>: How to Repair Windows 10 using Command Prompt

**NEW QUESTION 7**

A large university wants to equip all classrooms with high-definition IP videoconferencing equipment. Which of the following would most likely be impacted in this situation?

- A. SAN
- B. LAN
- C. GPU
- D. PAN

**Answer: B**

**Explanation:**

LAN is the most likely option to be impacted in this situation. LAN stands for Local Area Network, and it is a network that connects devices within a limited area, such as a building or a campus. Installing high-definition IP videoconferencing equipment in all classrooms would require a high bandwidth and reliable LAN infrastructure to support the video and audio transmission. The LAN would also need to be configured with proper security, quality of service, and multicast protocols to ensure the optimal performance of the videoconferencing system. SAN, GPU, and PAN are not directly related to this scenario. SAN stands for Storage Area Network, and it is a network that provides access to consolidated storage devices. GPU stands for Graphics Processing Unit, and it is a hardware component that handles graphics rendering and computation. PAN stands for Personal Area Network, and it is a network that connects devices within a short range, such as Bluetooth or infrared. References:

? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 20

? CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 104

**NEW QUESTION 8**

Which of the following is used to identify potential issues with a proposed change prior to implementation?

- A. Request form
- B. Rollback plan
- C. End-user acceptance
- D. Sandbox testing

**Answer: D**

**Explanation:**

Sandbox testing is a method of identifying potential issues with a proposed change prior to implementation. It involves creating a simulated or isolated environment that mimics the real system and applying the change to it. This can help to verify that the change works as expected and does not cause any errors or conflicts. Request form, rollback plan and end-user acceptance are other components of a change management process, but they do not involve identifying issues with a change. Verified References: <https://www.comptia.org/blog/what-is-sandbox-testing> <https://www.comptia.org/certifications/a>

**NEW QUESTION 9**

A Linux technician needs a filesystem type that meets the following requirements:

- . All changes are tracked.
- . The possibility of file corruption is reduced.
- . Data recovery is easy.

Which of the following filesystem types best meets these requirements?

ext3

- B. FAT32
- C. exFAT
- D. NTFS

**Answer:** A

**Explanation:**

The ext3 file system is a Linux native file system that meets the requirements of the question. It has the following features:

? All changes are tracked. The ext3 file system uses a journaling mechanism that records all changes to the file system metadata in a special log called the journal before applying them to the actual file system. This ensures that the file system can be restored to a consistent state in case of a power failure or system crash<sup>12</sup>.

? The possibility of file corruption is reduced. The journaling feature of ext3 also reduces the possibility of file corruption, as it avoids the need for a full file system check after an unclean shutdown. The file system can be quickly replayed from the journal and any inconsistencies can be fixed<sup>12</sup>.

? Data recovery is easy. The ext3 file system supports undeletion of files using tools such as ext3grep or extundelete, which can scan the file system for deleted inodes and attempt to recover the data blocks associated with them<sup>34</sup>.

References:

1: Introduction to Linux File System [Structure and Types] - MiniTool1 2: 7 Ways to Determine the File System Type in Linux (Ext2, Ext3 or Ext4) - Tecmint3 3: How to Recover Deleted Files in Linux with ext3grep 4: How to Recover Deleted Files from ext3 Partitions

**NEW QUESTION 10**

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:**

Installing applications directly from a vendor's website can be risky, as the application may be malicious or fraudulent. Uninstalling the application can help mitigate the issue by removing the source of the problem.

**NEW QUESTION 10**

A technician is securing a new Windows 10 workstation and wants to enable a Screensaver lock. Which of the following options in the Windows settings should the technician use?

- A. Ease of Access
- B. Privacy
- C. Personalization
- D. Update and Security

**Answer:** C

**Explanation:**

The technician should use the Personalization option in the Windows settings to enable a Screensaver lock. The Personalization option allows users to customize the appearance and behavior of their desktop, such as themes, colors, backgrounds, lock screen and screensaver. The technician can enable a Screensaver lock by choosing a screensaver from the drop-down menu, setting a wait time in minutes and checking the box that says "On resume, display logon screen". This will lock the computer and require a password or PIN to log back in after the screensaver is activated. Ease of Access is an option in the Windows settings that allows users to adjust accessibility features and settings, such as narrator, magnifier, high contrast and keyboard shortcuts. Ease of Access is not related to enabling a

Screensaver lock. Privacy is an option in the Windows settings that allows users to manage privacy and security settings, such as location, camera, microphone and app permissions. Privacy is not related to enabling a Screensaver lock. Update and Security is an option in the Windows settings that allows users to check and install updates, troubleshoot problems, backup files and restore system. Update and Security is not related to enabling a Screensaver lock. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.7

**NEW QUESTION 12**

A technician is troubleshooting a mobile device that was dropped. The technician finds that the screen (ails to rotate, even though the settings are correctly applied. Which of the following pieces of hardware should the technician replace to resolve the issue?

- A. LCD
- B. Battery
- C. Accelerometer
- D. Digitizer

**Answer:** C

**Explanation:**

The piece of hardware that the technician should replace to resolve the issue of the screen failing to rotate on a mobile device that was dropped is the accelerometer. The accelerometer is a sensor that detects the orientation and movement of the mobile device by measuring the acceleration forces acting on it. The accelerometer allows the screen to rotate automatically according to the position and angle of the device. If the accelerometer is damaged or malfunctioning, the screen may not rotate properly or at all, even if the settings are correctly applied. LCD stands for Liquid Crystal Display and is a type of display that uses liquid crystals and backlight to produce images on the screen. LCD is not related to the screen rotation feature but to the quality and brightness of the display. Battery is a component that provides power to the mobile device by storing and releasing electrical energy. Battery is not related to the screen rotation feature but to the battery life and performance of the device. Digitizer is a component that converts touch inputs into digital signals that can be processed by the mobile device. Digitizer is not related to the screen rotation feature but to the touch sensitivity and accuracy of the display. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.5

#### NEW QUESTION 14

Which of the following is used as a password manager in the macOS?

- A. Terminal
- B. FileVault
- C. Privacy
- D. Keychain

**Answer:** D

#### Explanation:

Keychain is a feature of macOS that securely stores passwords, account numbers, and other confidential information for your Mac, apps, servers, and websites<sup>1</sup>. You can use the Keychain Access app on your Mac to view and manage your keychains and the items stored in them<sup>1</sup>. Keychain can also sync your passwords across your devices using iCloud Keychain<sup>1</sup>. Keychain can be used as a password manager in macOS to help you keep track of and protect your passwords. References: 1: Manage passwords using keychains on Mac (<https://support.apple.com/guide/mac-help/use-keychains-to-store-passwords-mchlf375f392/mac>)

#### NEW QUESTION 19

The courts determined that a cybercrimes case could no longer be prosecuted due to the agency's handling of evidence. Which of the following was MOST likely violated during the investigation?

- A. Open-source software
- B. EULA
- C. Chain of custody
- D. AUP

**Answer:** C

#### Explanation:

Chain of custody is a process that documents how evidence is collected, handled, stored and transferred during a cybercrime investigation. It ensures that the evidence is authentic, reliable and admissible in court. If the chain of custody is violated during an investigation, it can compromise the integrity of the evidence and lead to the case being dismissed. Open-source software, EULA (end-user license agreement) and AUP (acceptable use policy) are not related to cybercrime investigations or evidence handling. Verified References: <https://www.comptia.org/blog/what-is-chain-of-custody> <https://www.comptia.org/certifications/a>

#### NEW QUESTION 22

Which of the following would MOST likely be deployed to enhance physical security for a building? (Select TWO).

- A. Multifactor authentication
- B. Badge reader
- C. Personal identification number
- D. Firewall
- E. Motion sensor
- F. Soft token

**Answer:** BE

#### Explanation:

Badge reader and motion sensor are devices that can be deployed to enhance physical security for a building. A badge reader is a device that scans and verifies an identification card or tag that grants access to authorized personnel only. A badge reader can help prevent unauthorized entry or intrusion into a building or a restricted area. A motion sensor is a device that detects movement and triggers an alarm or an action when motion is detected. A motion sensor can help deter or alert potential intruders or trespassers in a building or an area. Multifactor authentication is a method of verifying identity using two or more factors, such as something you know, something you have or something you are. Multifactor authentication is not a device that can be deployed to enhance physical security for a building but a technique that can be used to enhance logical security for systems or services. Personal identification number is a numeric code that can be used as part of authentication or access control. Personal identification number is not a device that can be deployed to enhance physical security for a building but an example of something you know factor in multifactor authentication. Firewall is a device or software that filters network traffic based on rules and policies. Firewall is not a device that can be deployed to enhance physical security for a building but a device that can be used to enhance network security for systems or services. Soft token is an application or software that generates one-time passwords or codes for authentication purposes. Soft token is not a device that can be deployed to enhance physical security for a building but an example of something you have factor in multifactor authentication. References: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 3.3

#### NEW QUESTION 24

A company needs employees who work remotely to have secure access to the corporate intranet. Which of the following should the company implement?

- A. Password-protected Wi-Fi
- B. Port forwarding
- C. Virtual private network
- D. Perimeter network

**Answer:** C

#### Explanation:

A virtual private network (VPN) is a technology that creates a secure and encrypted connection over a public network, such as the internet. A VPN allows remote employees to access the corporate intranet as if they were physically connected to the local network<sup>3</sup>.

Password-protected Wi-Fi is a security measure for wireless networks that does not provide access to the corporate intranet. Port forwarding is a technique that allows external devices to access services on a private network through a router, but does not provide access to the corporate intranet. A perimeter network is a network segment that lies between an internal network and an external network, such as the internet, and provides an additional layer of security, but does not provide access to the corporate intranet.



#### NEW QUESTION 28

Windows updates need to be performed on a department's servers. Which of the following methods should be used to connect to the server?

- FIP
- A. MSRA  
B. RDP  
C. VPN  
D. FIP

**Answer: C**

#### Explanation:

RDP (Remote Desktop Protocol) is a protocol that allows a user to connect to and control a remote computer over a network. RDP can be used to perform Windows updates on a department's servers without physically accessing them.

Reference: CompTIA A+ Core 2 Exam Objectives, Section 5.6

#### NEW QUESTION 32

A company is looking for a solution that provides a backup for all data on the system while providing the lowest impact to the network. Which of the following backup types will the company MOST likely select?

- A. Off-site  
B. Synthetic  
C. Full  
D. Differential

**Answer: B**

#### Explanation:

A synthetic backup is a backup type that provides a backup for all data on the system while providing the lowest impact to the network. It combines a full backup with one or more incremental backups to create a single backup set, without requiring access to the original data source. Off-site is a backup location, not a backup type. Full and differential are backup types, but they have a higher impact on the network than synthetic. Verified References:

<https://www.comptia.org/blog/what-is-a-synthetic-backup> <https://www.comptia.org/certifications/a>

#### NEW QUESTION 37

A technician downloads a validated security tool and notes the vendor hash of a58e87a2. When the download is complete, the technician again validates the hash, but the value returns as 2a876a7d3. Which of the following is the MOST likely cause of the issue?

- A. Private-browsing mode  
B. Invalid certificate  
C. Modified file  
D. Browser cache

**Answer: C**

#### Explanation:

The most likely cause of the issue of having different hash values for a downloaded security tool is a modified file. A hash value is a unique and fixed-length string that is

generated from an algorithm that processes data or files. A hash value can be used to verify the integrity and authenticity of data or files by comparing it with a known or expected value. If the hash values do not match, it means that the data or file has been altered or corrupted in some way. A modified file may result from intentional or unintentional changes, such as editing, encryption, compression or malware infection. Private-browsing mode is a feature that allows users to browse the web without storing any browsing history, cookies or cache on their browser. Private-browsing mode does not affect the hash value of a downloaded file but only how the browser handles user data. Invalid certificate is an error that occurs when a website or a server does not have a valid or trusted digital certificate that proves its identity and secures its communication. Invalid certificate does not affect the hash value of a downloaded file but only how the browser verifies the website or server's credibility. Browser cache is a temporary storage that stores copies of web pages, images and other content that users have visited on their browser.

#### NEW QUESTION 39

Which of the following filesystems replaced FAT as the preferred filesystem for Microsoft Windows OS?

- A. APFS  
B. FAT32  
C. NTFS  
D. ext4

**Answer: C**

#### Explanation:

NTFS stands for New Technology File System and it is the preferred filesystem for Microsoft Windows OS since Windows NT 3.1 in 19931. NTFS replaced FAT (File Allocation Table) as the default filesystem for Windows because it offers many advantages over FAT, such as:

- ? Support for larger volumes and files (up to 16 exabytes)<sup>2</sup>
- ? Support for file compression, encryption, and permissions<sup>2</sup>
- ? Support for journaling, which records changes to the filesystem and helps recover from errors<sup>2</sup>
- ? Support for hard links, symbolic links, and mount points<sup>2</sup>
- ? Support for long filenames and Unicode characters<sup>2</sup>

FAT32 is an improved version of FAT that supports larger volumes and files (up to 32 GB and 4 GB respectively) and is compatible with older versions of Windows and other operating systems<sup>3</sup>. However, FAT32 still has many limitations and drawbacks compared

to NTFS, such as:

- ? No support for file compression, encryption, and permissions<sup>3</sup>
- ? No support for journaling, which makes it vulnerable to corruption and data loss<sup>3</sup>

? No support for hard links, symbolic links, and mount points<sup>3</sup>

? No support for long filenames and Unicode characters<sup>3</sup>

APFS (Apple File System) is the default filesystem for macOS, iOS, iPadOS, watchOS, and tvOS since 2017. APFS replaced HFS+ (Hierarchical File System Plus) as the preferred filesystem for Apple devices because it offers many advantages over HFS+, such as:

? Support for larger volumes and files (up to 8 zettabytes)<sup>4</sup>

? Support for file cloning, snapshots, and encryption<sup>4</sup>

? Support for space sharing, which allows multiple volumes to share the same storage pool<sup>4</sup>

? Support for fast directory sizing, which improves performance and efficiency<sup>4</sup> ext4 (Fourth Extended Filesystem) is the default filesystem for most Linux distributions since 2008. ext4 replaced ext3 as the preferred filesystem for Linux because it offers many advantages over ext3, such as:

? Support for larger volumes and files (up to 1 exabyte and 16 terabytes respectively)<sup>5</sup>

? Support for extents, which reduce fragmentation and improve performance<sup>5</sup>

? Support for journal checksumming, which improves reliability and reduces recovery time<sup>5</sup>

? Support for delayed allocation, which improves efficiency and reduces metadata overhead<sup>5</sup>

References:

1: NTFS - Wikipedia 2: [NTFS vs FAT32 vs exFAT: What's the Difference?] 3: [FAT32 - Wikipedia] 4: [Apple File System - Wikipedia] 5: [ext4 - Wikipedia] : NTFS vs FAT32 vs exFAT: What's the Difference? : FAT32 - Wikipedia : Apple File System - Wikipedia : ext4 - Wikipedia

### NEW QUESTION 43

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 technician should quarantine the system first<sup>1</sup> Reference:

CompTIA A+ Certification Exam: Core 2 Objectives Version 4.0. Retrieved from [https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-\(3-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-(3-0))

### NEW QUESTION 45

#### SIMULATION

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

. All phishing attempts must be reported.

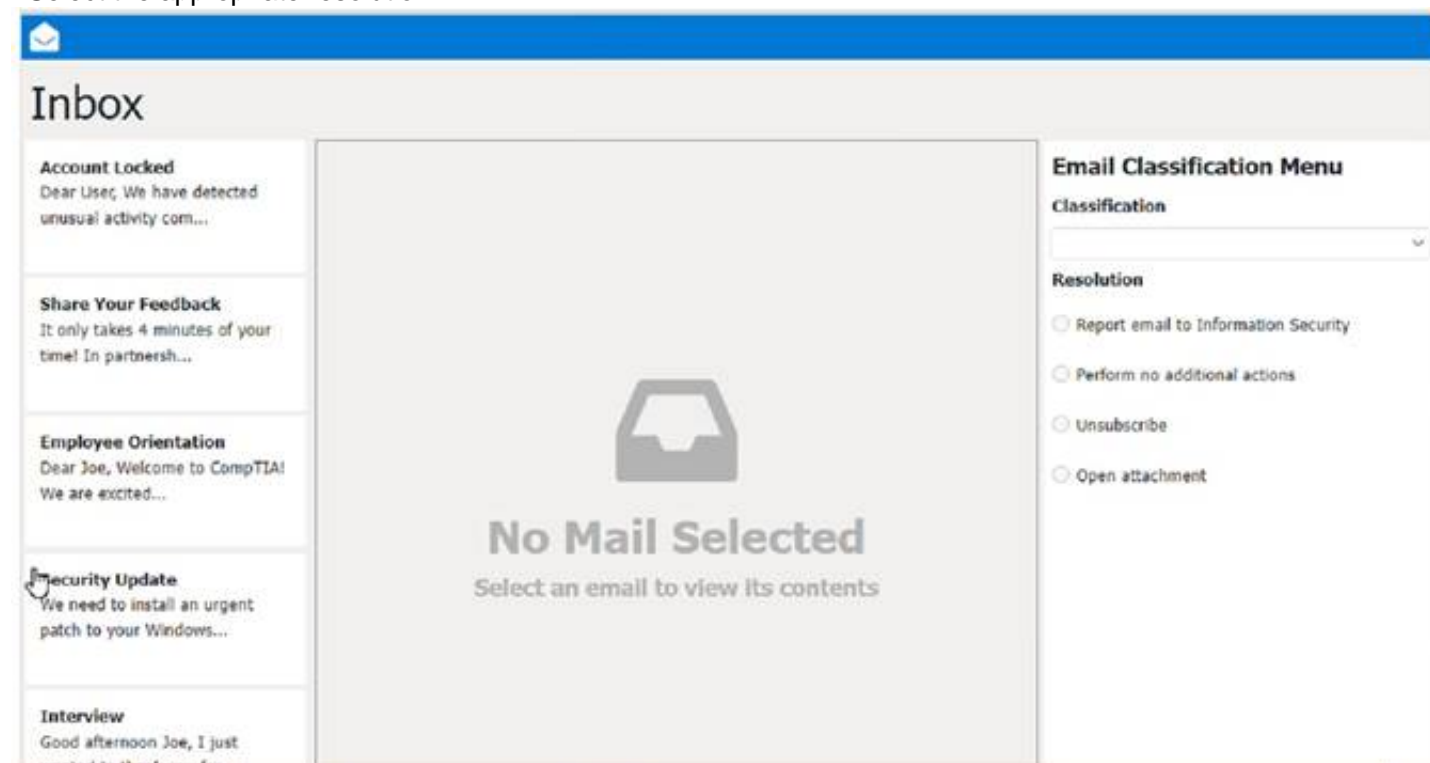
. Future spam emails to users must be prevented. INSTRUCTIONS

Review each email and perform the following within the email:

. Classify the emails

. Identify suspicious items, if applicable, in each email

. Select the appropriate resolution



**Answer:**

See the Full solution in Explanation below.

- A. Mastered
- B. Not Mastered

**Answer: A**

### Explanation:

Classification: a) Phishing

This email is a phishing attempt, as it tries to trick the user into clicking on a malicious link that could compromise their account or personal information. Some suspicious items in this email are:

? The email has a generic greeting and does not address the user by name.

? The email has spelling errors, such as "unusal" and "Locaked".

? The email uses a sense of urgency and fear to pressure the user into clicking on the link.

? The email does not match the official format or domain of the IT Help Desk at CompTIA.



? The email has two black bat icons, which are not related to CompTIA or IT support.

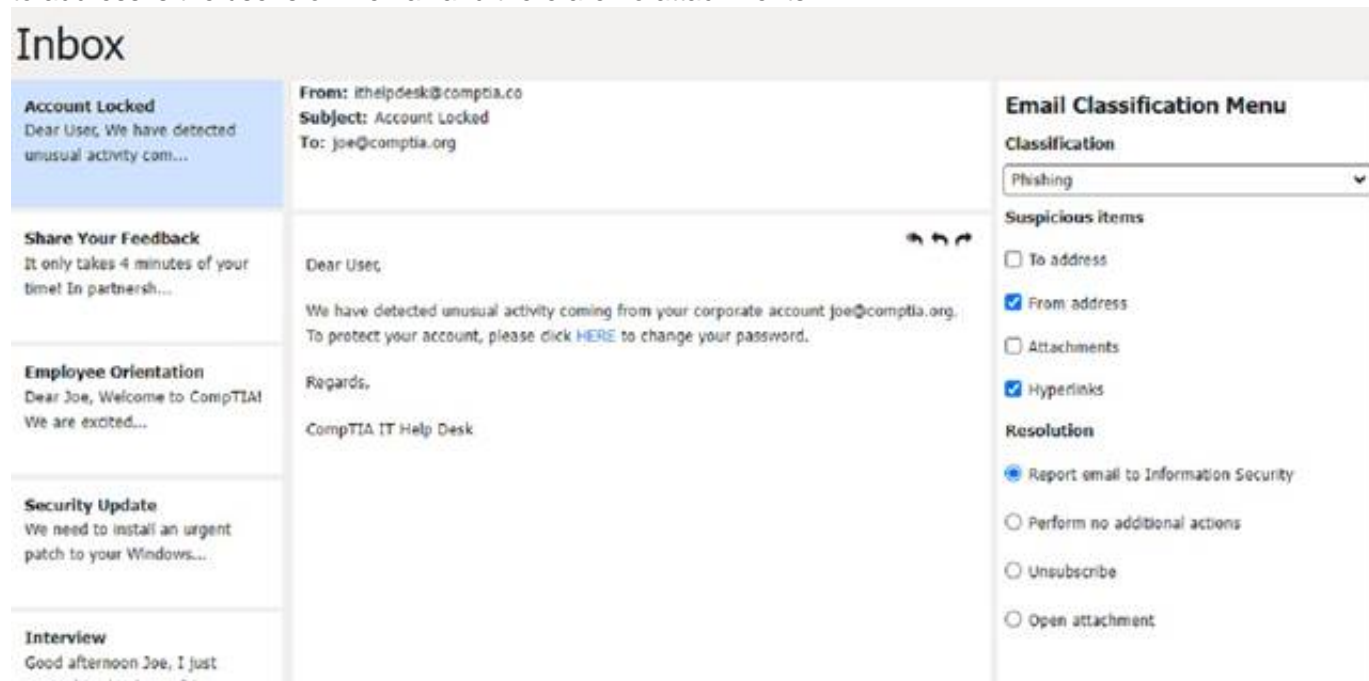
The appropriate resolution for this email is A. Report email to Information Security. The user should not click on the link, reply to the email, or provide any personal or account information. The user should forward the email to the Information Security team or use a professional email form to report the phishing attempt. The user should also delete the email from their inbox and trash folder.

The suspicious items to select are:

? b) From address

? d) Hyperlinks

These items indicate that the email is not from a legitimate source and that the link is potentially malicious. The other items are not suspicious in this case, as the to address is the user's own email and there are no attachments.



Classification: b) Spam

This email is a spam email, as it is an unsolicited and unwanted message that tries to persuade the user to participate in a survey and claim a reward. Some suspicious items in this email are:

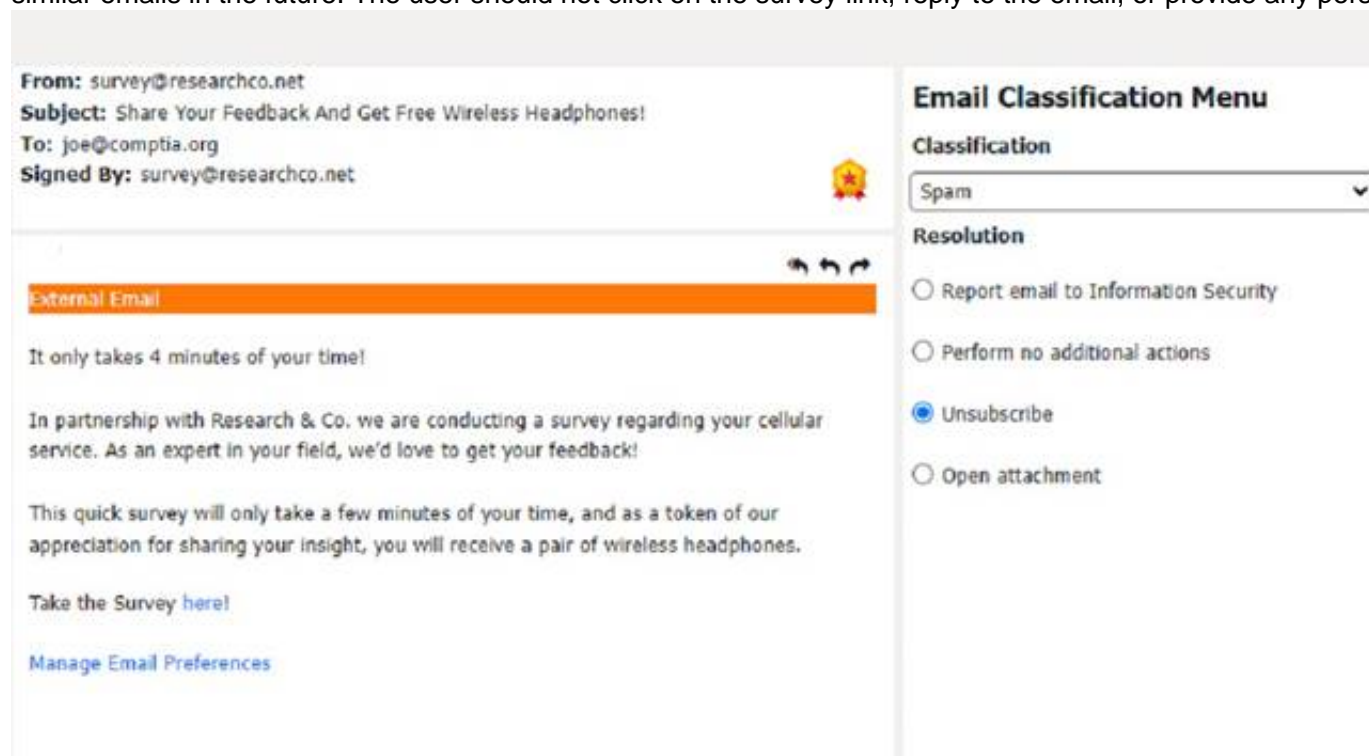
? The email offers a free wireless headphone as an incentive, which is too good to be true.

? The email does not provide any details about the survey company, such as its name, address, or contact information.

? The email contains an external survey link, which may lead to a malicious or fraudulent website.

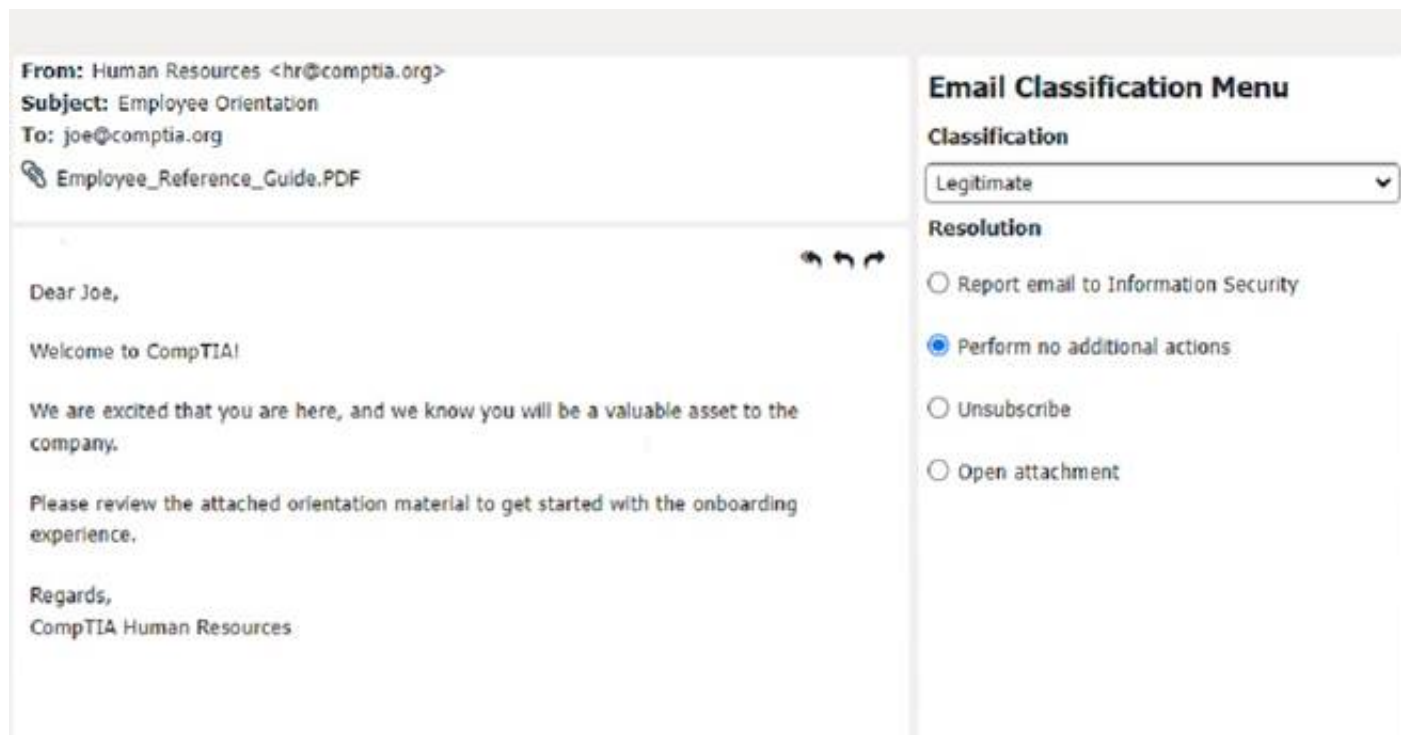
? The email does not have an unsubscribe option, which is required by law for commercial emails.

The appropriate resolution for this email is C. Unsubscribe. The user should look for an unsubscribe link or button at the bottom of the email and follow the instructions to opt out of receiving future emails from the sender. The user should also mark the email as spam or junk in their email client, which will help filter out similar emails in the future. The user should not click on the survey link, reply to the email, or provide any personal or financial information.



Classification: c) Legitimate

This email is a legitimate email, as it is from a trusted source and has a valid purpose. There are no suspicious items in this email, as the from address, the to address, the attachment, and the email body are all consistent and relevant. The appropriate resolution for this email is B. Perform no additional actions. The user can open the attachment and review the orientation material as instructed. The user does not need to report, unsubscribe, or delete this email.



A screenshot of a computer

Description automatically generated

Classification: a) Phishing

This email is a phishing attempt, as it tries to deceive the user into downloading and running a malicious attachment that could compromise their system or data.

Some suspicious items in this email are:

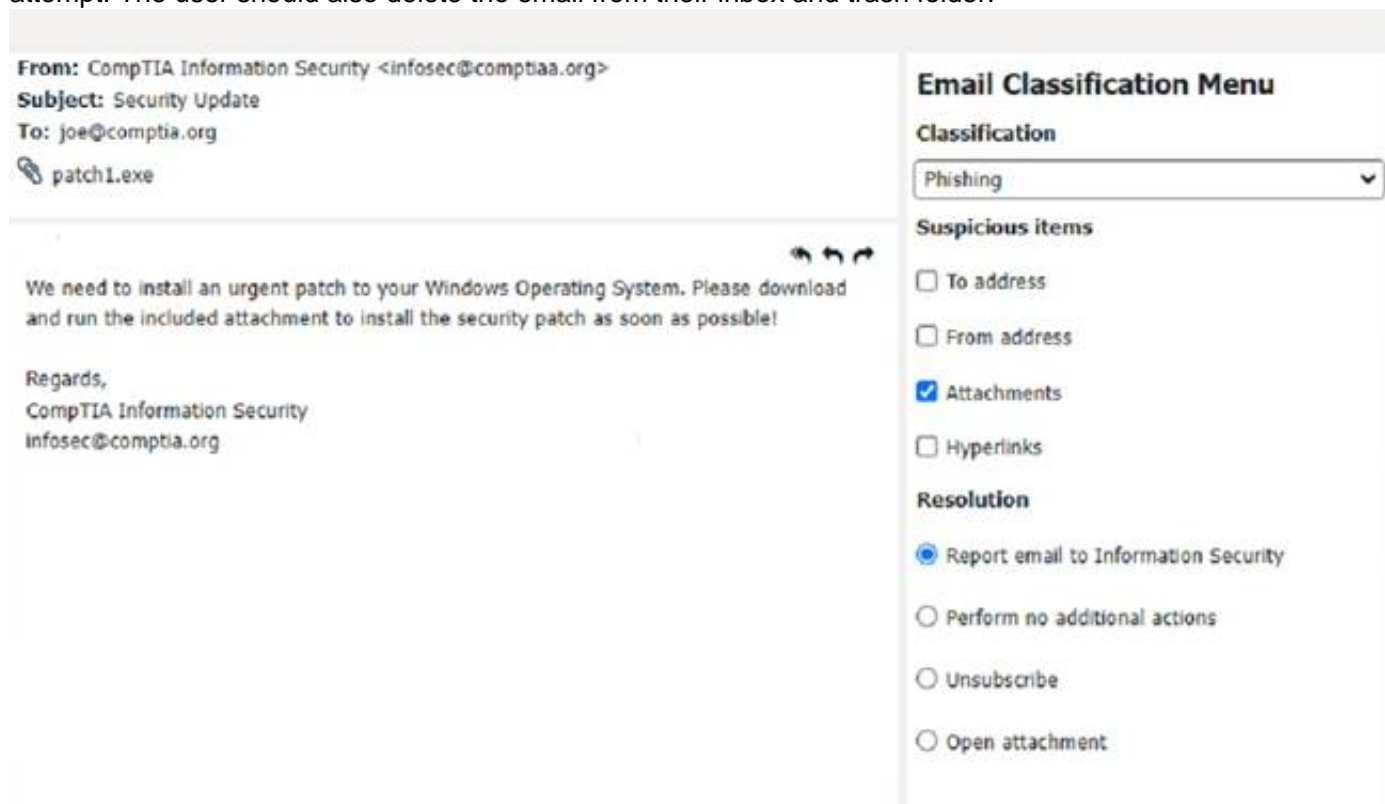
? The email has a generic greeting and does not address the user by name or username.

? The email has an urgent tone and claims that a security patch needs to be installed immediately.

? The email has an attachment named "patch1.exe", which is an executable file that could contain malware or ransomware.

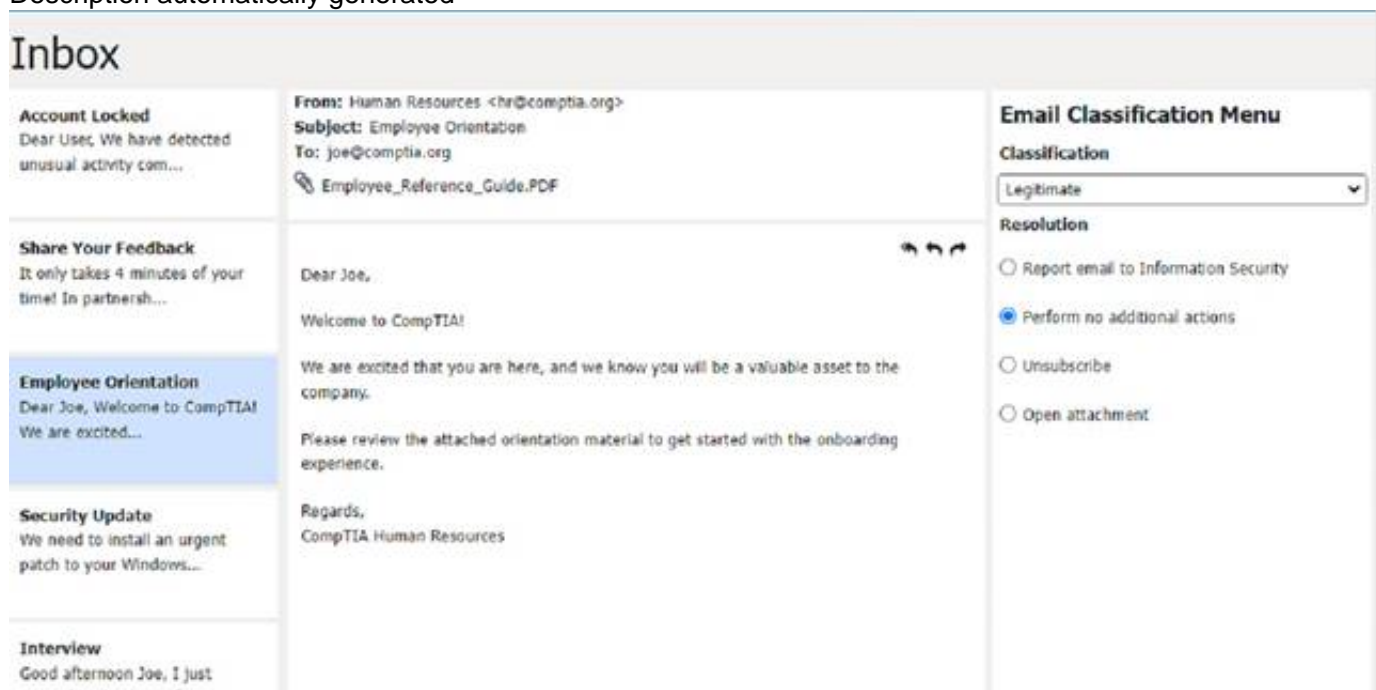
? The email does not match the official format or domain of CompTIA Information Security.

The appropriate resolution for this email is A. Report email to Information Security. The user should not open the attachment, reply to the email, or provide any personal or account information. The user should forward the email to the Information Security team or use a professional email form to report the phishing attempt. The user should also delete the email from their inbox and trash folder.



A screenshot of a computer

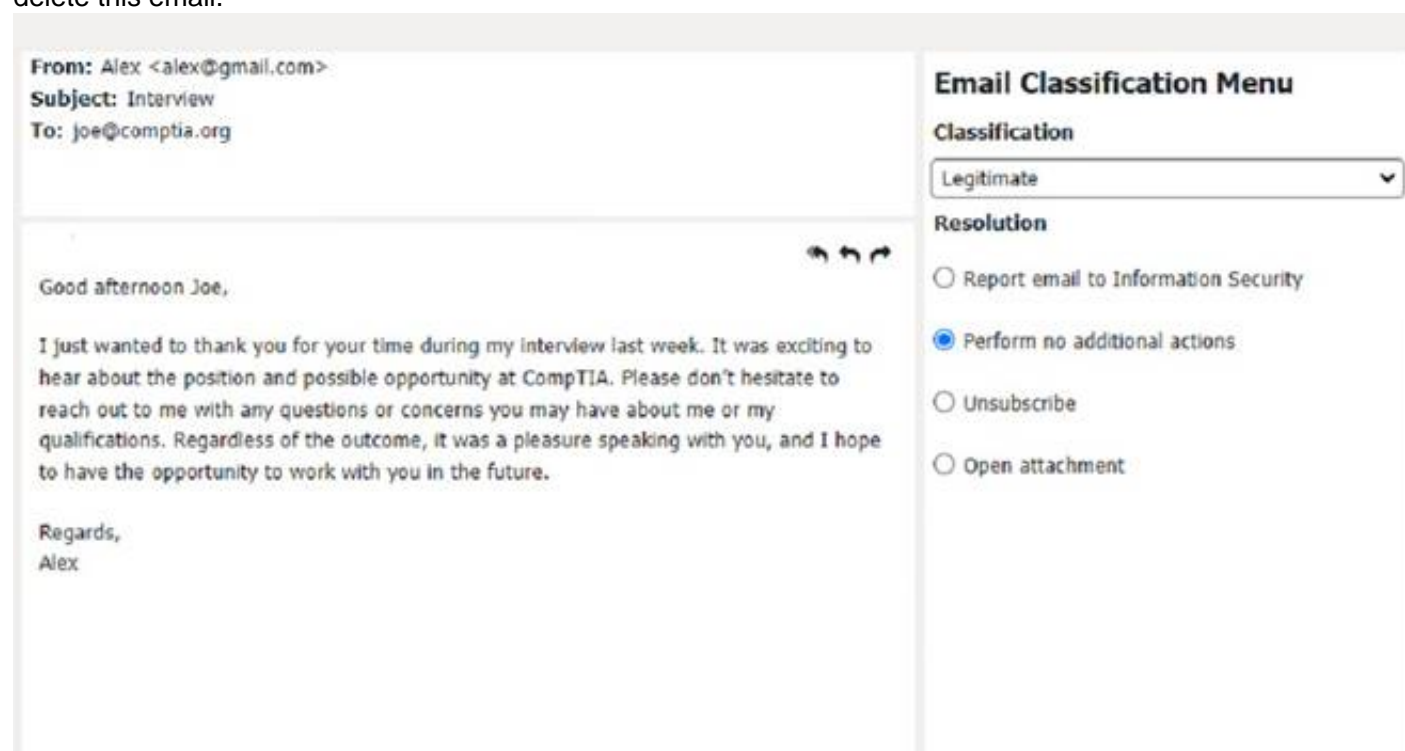
Description automatically generated



Classification: c) Legitimate

This email is a legitimate email, as it is from a trusted source and has a valid purpose. There are no suspicious items in this email, as the from address, the to address, and the email body are all consistent and relevant. The appropriate resolution for this email is B.

Perform no additional actions. The user can reply to the email and thank the sender for the interview opportunity. The user does not need to report, unsubscribe, or delete this email.



A screenshot of a computer  
Description automatically generated

#### NEW QUESTION 50

A user recently purchased a second monitor and wants to extend the Windows desktop to the new screen. Which of the following Control Panel options should a technician adjust to help the user?

- A. Color Management
- B. Troubleshooting System
- C. Device Manager
- D. Administrative Tools

**Answer: D**

#### NEW QUESTION 54

A technician has verified that a user's computer has a virus and the antivirus software is out of date. Which of the following steps should the technician take next?

- A. Quarantine the computer.
- B. Use a previous restore point.
- C. Educate the end user about viruses.
- D. Download the latest virus definitions.

**Answer: D**

#### Explanation:

The first step in removing a virus from a computer is to update the antivirus software with the latest virus definitions. Virus definitions are files that contain information about the characteristics and behavior of known viruses and malware. They help the antivirus software to identify and remove the malicious threats from the computer. Without the latest virus definitions, the antivirus software may not be able to detect or remove the virus that infected the user's computer. Therefore, the technician should download the latest virus definitions from the antivirus vendor's website or use the update feature in the antivirus program before scanning the computer for viruses.

References:

- ? How to remove malware or viruses from my Windows 10 PC, section 21
- ? How to Remove a Virus From a Computer in 2023, section 32
- ? The Official CompTIA A+ Core 2 Study Guide (220-1102), page 2193

#### NEW QUESTION 58

A user visits a game vendor's website to view the latest patch notes, but this information is not available on the page. Which of the following should the user perform before reloading the page?

- A. Synchronize the browser data.
- B. Enable private browsing mode.
- C. Mark the site as trusted.
- D. Clear the cached file.

**Answer: D**

#### Explanation:

Clearing the cached file is an action that can help resolve the issue of not seeing the latest patch notes on a game vendor's website. A cached file is a copy of a web page or file that is stored locally on the user's browser or device for faster loading and offline access. However, sometimes a cached file may become outdated or corrupted and prevent the user from seeing the most recent or accurate version of a web page or file. Clearing the cached file can force the browser to download and display the latest version from the server instead of using the old copy from the cache. Synchronizing the browser data, enabling private browsing mode, and marking the site as trusted are not actions that can help resolve this issue.



#### NEW QUESTION 60

A user in a corporate office reports the inability to connect to any network drives. No other users have reported this issue. Which of the following is the MOST likely reason the user is having this issue?

- A. Mastered
- B. Not Mastered

**Answer:** A

#### NEW QUESTION 64

Which of the following operating systems is most commonly used in embedded systems?

- A. Chrome OS
- B. macOS
- C. Windows
- D. Linux

**Answer:** D

#### Explanation:

Linux is the most commonly used operating system in embedded systems because it is open source, free, customizable, and supports a wide range of architectures and devices. Linux also offers many advantages for embedded development, such as real-time capabilities, modularity, security, scalability, and reliability. Linux can run on embedded systems with limited resources, such as memory, storage, or power, and can be tailored to the specific needs of the application. Linux also has a large and active community of developers and users who contribute to its improvement and innovation. Some examples of embedded systems that use Linux are smart TVs, routers, drones, robots, smart watches, and IoT devices

#### NEW QUESTION 66

A systems administrator is setting up a Windows computer for a new user. Corporate policy requires a least privilege environment. The user will need to access advanced features and configuration settings for several applications. Which of the following BEST describes the account access level the user will need?

- A. Power user account
- B. Standard account
- C. Guest account
- D. Administrator account

**Answer:** B

#### Explanation:

The account access level the user will need to access advanced features and configuration settings for several applications while adhering to corporate policy requiring a least privilege environment is a standard account. This is because a standard account allows the user to access advanced features and configuration settings for several applications while adhering to corporate policy requiring a least privilege environment<sup>1</sup>.

#### NEW QUESTION 71

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:

A firewall is a security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. In this scenario, the user is concerned about an installed application transmitting data in the background, so a firewall would be the best solution to address their concern. By installing and configuring a firewall, the user can block unauthorized connections to and from the device, and receive alerts whenever an application tries to access the internet.

#### NEW QUESTION 72

A technician is installing RAM in a new workstation and needs to protect against electrostatic discharge. Which of the following will best resolve this concern?

- A. Battery backup
- B. Thermal paste
- C. ESD strap
- D. Consistent power

**Answer:** C

#### Explanation:

An ESD strap, also known as an antistatic wrist strap, is a device that prevents electrostatic discharge (ESD) from damaging sensitive electronic components such as RAM. ESD is the sudden flow of electricity between two objects with different electrical charges, which can cause permanent damage or malfunction to electronic devices. An ESD strap connects the technician's wrist to a grounded surface, such as a metal case or a mat, and equalizes the electrical potential between the technician and the device. Battery backup, thermal paste, and consistent power are not devices that can protect against ESD.

#### NEW QUESTION 75

A systems administrator needs to reset a user's password because the user forgot it. The systems administrator creates the new password and wants to further protect the user's account. Which of the following should the systems administrator do?

- A. Require the user to change the password at the next log-in.
- B. Disallow the user from changing the password.
- C. Disable the account
- D. Choose a password that never expires.

**Answer:** A

#### Explanation:

This will ensure that the user is the only one who knows their password, and that the new password is secure.

The CompTIA A+ Core 2 220-1102 exam covers this topic in the domain 1.4 Given a scenario, use appropriate data destruction and disposal methods.

#### NEW QUESTION 78

A developer's Type 2 hypervisor is performing inadequately when compiling new source code. Which of the following components should the developer upgrade to improve the hypervisor's performance?

- A. Amount of system RAM
- B. NIC performance
- C. Storage IOPS
- D. Dedicated GPU

**Answer:** A

#### Explanation:

The correct answer is A. Amount of system RAM. A Type 2 hypervisor is a virtualization software that runs on top of a host operating system, which means it shares the system resources with the host OS and other applications. Therefore, increasing the amount of system RAM can improve the performance of the hypervisor and the virtual machines running on it. RAM is used to store data and instructions that are frequently accessed by the CPU, and having more RAM can reduce the need for swapping data to and from the storage device, which is slower than RAM.

NIC performance, storage IOPS, and dedicated GPU are not as relevant for improving the hypervisor's performance in this scenario. NIC performance refers to the speed and quality of the network interface card, which is used to connect the computer to a network. Storage IOPS refers to the number of input/output operations per second that can be performed by the storage device, which is a measure of its speed and efficiency. Dedicated GPU refers to a separate graphics processing unit that can handle complex graphics tasks, such as gaming or video editing. These components may affect other aspects of the computer's performance, but they are not directly related to the hypervisor's ability to compile new source code.

#### NEW QUESTION 79

A systems administrator is tasked with configuring desktop systems to use a new proxy server that the organization has added to provide content filtering. Which of the following Windows utilities IS the BEST choice for accessing the necessary configuration to complete this goal?

- A. Security and Maintenance
- B. Network and Sharing Center
- C. Windows Defender Firewall
- D. Internet Options

**Answer:** D

#### Explanation:

The best choice for accessing the necessary configuration to configure the desktop systems to use a new proxy server is the Internet Options utility. This utility can be found in the Control Panel and allows you to configure the proxy settings for your network connection. As stated in the CompTIA A+ Core 2 exam objectives, technicians should be familiar with the Internet Options utility and how to configure proxy settings.

#### NEW QUESTION 80

A technician has just used an anti-malware removal tool to resolve a user's malware issue on a corporate laptop. Which of the following BEST describes what the technician should

do before returning the laptop to the user?

- A. Educate the user on malware removal.
- B. Educate the user on how to reinstall the laptop OS.
- C. Educate the user on how to access recovery mode.
- D. Educate the user on common threats and how to avoid them.

**Answer:** D

#### Explanation:

educating the user on common threats and how to avoid them (D) would be a good step before returning the laptop to the user. This can help prevent similar issues from happening again.

#### NEW QUESTION 84

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? (Select TWO)

- A. Mastered
- B. Not Mastered

**Answer:** A



**Explanation:**

"The user thought the company-provided antivirus software would prevent this issue." The most likely steps to resolve the issue are to deploy an ad-blocking extension to the browser and perform a reset on the user's web browser. Ad-blocking extensions can help to prevent pop-ups and other unwanted content from appearing in the browser, and resetting the browser can help to remove any malicious extensions or settings that may be causing the issue.

**NEW QUESTION 86**

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 file type that the technician will MOST likely use when installing new software on a macOS computer is .app. This is because .app is the file extension for applications on macOS.

**NEW QUESTION 87**

Which of the following macOS utilities uses AES-128 to encrypt the startup disk?

- A. fdisk
- B. Diskpart
- C. Disk Utility
- D. FileVault

**Answer: D**

**Explanation:**

FileVault is a macOS utility that uses AES-128 (Advanced Encryption Standard) to encrypt the startup disk of a Mac computer. It protects the data from unauthorized access if the computer is lost or stolen. fdisk and Diskpart are disk partitioning utilities for Linux and Windows, respectively. Disk Utility is another macOS utility that can perform disk management tasks, such as formatting, resizing, repairing, etc. Verified References: <https://www.comptia.org/blog/what-is-filevault> <https://www.comptia.org/certifications/a>

**NEW QUESTION 92**

A technician needs administrator access on a Windows workstation to facilitate system changes without elevating permissions. Which of the following would best accomplish this task?

- A. Group Policy Editor
- B. Local Users and Groups
- C. Device Manager
- D. System Configuration

**Answer: B**

**Explanation:**

Local Users and Groups is the best option to accomplish this task. Local Users and Groups is a tool that allows managing the local user accounts and groups on a Windows workstation. The technician can use this tool to create a new user account with administrator privileges or add an existing user account to the Administrators group. This way, the technician can log in with the administrator account and make system changes without elevating permissions. Group Policy Editor, Device Manager, and System Configuration are not correct answers for this question. Group Policy Editor is a tool that allows configuring policies and settings for users and computers in a domain environment. Device Manager is a tool that allows managing the hardware devices and drivers on a Windows workstation. System Configuration is a tool that allows modifying the startup options and services on a Windows workstation. None of these tools can directly grant administrator access to a user account. References:

? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 13

? CompTIA A+ Complete Study Guide: Core 1 Exam 220-1101 and Core 2 Exam ..., page 103

#### NEW QUESTION 95

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

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

**Answer:** C

#### Explanation:

Maintaining the chain of custody is important to control evidence and maintain integrity. The chain of custody is a process that documents who handled, accessed, or modified a piece of evidence, when, where, how, and why. The chain of custody ensures that the evidence is preserved, protected, and authenticated throughout the incident response process. Maintaining the chain of custody can help prevent tampering, alteration, or loss of evidence, as well as establish its reliability and validity in legal proceedings. Maintaining an information security policy, properly identifying the issue, and gathering as much information as possible are not reasons why maintaining the chain of custody is important. Maintaining an information security policy is a general practice that defines the rules and guidelines for securing an organization's information assets and resources. Properly identifying the issue is a step in the incident response process that

involves analyzing and classifying the incident based on its severity, impact, and scope. Gathering as much information as possible is a step in the incident response process that involves collecting and documenting relevant data and evidence from various sources, such as logs, alerts, or witnesses. References: ? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 26

#### NEW QUESTION 100

Which of the following best describes when to use the YUM command in Linux?

- A. To add functionality
- B. To change folder permissions
- C. To show documentation
- D. To list file contents

**Answer:** A

#### Explanation:

YUM stands for Yellowdog Updater Modified and it is a command-line tool that allows users to install, update, remove, and manage software packages in Linux. YUM can be used to add functionality to a Linux system by installing new software packages or updating existing ones. To change folder permissions, show documentation, or list file contents, other commands such as chmod, man, or ls can be used in Linux.

#### NEW QUESTION 105

A user's corporate laptop with proprietary work information was stolen from a coffee shop. The user logged in to the laptop with a simple password, and no other security mechanisms were in place. Which of the following would MOST likely prevent the stored data from being recovered?

- A. Biometrics
- B. Full disk encryption
- C. Enforced strong system password
- D. Two-factor authentication

**Answer:** B

#### Explanation:

Full disk encryption is a security mechanism that encrypts the entire data on a hard drive, making it unreadable without the correct decryption key or password. It can prevent the stored data from being recovered by unauthorized persons who steal or access the laptop. Biometrics, enforced strong system password and two-factor authentication are other security mechanisms, but they only protect the login access to the laptop, not the data on the hard drive. Verified References: <https://www.comptia.org/blog/what-is-full-disk-encryption> <https://www.comptia.org/certifications/a>

#### NEW QUESTION 107

Which of the following physical security controls can prevent laptops from being stolen?

- A. Encryption
- B. LoJack
- C. Multifactor authentication
- D. Equipment lock
- E. Bollards

**Answer:** D

#### Explanation:

An equipment lock is a physical security device that attaches a laptop to a fixed object, such as a desk or a table, with a cable and a lock. This can prevent the laptop from being stolen by unauthorized persons. Encryption, LoJack, multifactor authentication and bollards are other security measures, but they do not physically prevent theft. Verified References: <https://www.comptia.org/blog/physical-security> <https://www.comptia.org/certifications/a>

#### NEW QUESTION 109

A technician has identified malicious traffic originating from a user's computer. Which of the following is the best way to identify the source of the attack?

- A. Investigate the firewall logs.
- B. Isolate the machine from the network.
- C. Inspect the Windows Event Viewer.
- D. Take a physical inventory of the device.

**Answer:** B

#### Explanation:

Isolating the machine from the network is the best way to identify the source of the attack, because it prevents the malicious traffic from spreading to other devices or reaching the attacker. Isolating the machine can also help preserve the evidence of the attack, such as the malware files, the network connections, the registry entries, or the system logs. By isolating the machine, a technician can safely analyze the machine and determine the source of the attack, such as a phishing email, a compromised website, a removable media, or a network vulnerability.

#### NEW QUESTION 114

Which of the following operating systems is considered closed source?

- A. Ubuntu
- B. Android
- C. CentOS
- D. OSX

**Answer:** D

#### Explanation:

OSX (now macOS) is an operating system that is considered closed source, meaning that its source code is not publicly available or modifiable by anyone except its

developers. It is owned and maintained by Apple Inc. Ubuntu, Android and CentOS are operating systems that are considered open

source, meaning that their source code is publicly available and modifiable by anyone who wants to contribute or customize them. Verified References:  
<https://www.comptia.org/blog/open-source-vs-closed-source-software> <https://www.comptia.org/certifications/a>

**NEW QUESTION 119**

A large company is selecting a new Windows operating system and needs to ensure it has built-in encryption and endpoint protection. Which of the following Windows versions will MOST likely be selected?

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

**Answer:** D

**Explanation:**

When selecting a new Windows operating system for a large company that needs built-in encryption and endpoint protection, the Enterprise edition is the most likely choice. This edition provides advanced security features such as Windows Defender Advanced Threat Protection (ATP), AppLocker, and BitLocker Drive Encryption. These features can help to protect the company's data and endpoints against malware attacks, unauthorized access, and data theft.

The Home and Pro editions of Windows do not include some of the advanced security features provided by the Enterprise edition, such as Windows Defender ATP and AppLocker. The Pro for Workstations edition is designed for high-performance and high-end hardware configurations, but it does not provide additional security features beyond those provided by the Pro edition.

**NEW QUESTION 122**

Which of the following should be used to control security settings on an Android phone in a domain environment?

- A. MDM
- B. MFA
- C. ACL
- D. SMS

**Answer:** A

**Explanation:**

The best answer to control security settings on an Android phone in a domain environment is to use “Mobile Device Management (MDM)”. MDM is a type of software that is used to manage and secure mobile devices such as smartphones and tablets. MDM can be used to enforce security policies, configure settings, and remotely wipe data from devices. In a domain environment, MDM can be used to manage Android phones and enforce security policies such as password requirements, encryption, and remote wipe capabilities<sup>12</sup>

**NEW QUESTION 127**

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 132**

A technician wants to enable BitLocker on a Windows 10 laptop and is unable to find the BitLocker Drive Encryption menu item in Control Panel. Which of the following explains why the technician unable to find this menu item?

- A. The hardware does not meet BitLocker's minimum system requirements.
- B. BitLocker was renamed for Windows 10.
- C. BitLocker is not included on Windows 10 Home.
- D. BitLocker was disabled in the registry of the laptop

**Answer:** C

**Explanation:**

BitLocker is only available on Windows 10 Pro, Enterprise, and Education editions<sup>1</sup>. Therefore, the technician is unable to find the BitLocker Drive Encryption menu item in Control Panel because it is not included in the Windows 10 Home edition<sup>1</sup>.

**NEW QUESTION 133**

A technician is finalizing a new workstation for a user. The user's PC will be connected to the internet but will not require the same private address each time. Which of the following protocols will the technician MOST likely utilize?

- A. DHCP
- B. SMTP
- C. DNS
- D. RDP

**Answer:** A

**Explanation:**

DHCP stands for Dynamic Host Configuration Protocol and it is used to assign IP addresses and other network configuration parameters to devices on a network automatically. This is useful for devices that do not require the same private address each time they connect to the internet.

**NEW QUESTION 136**

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 steps 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 technician should escalate the ticket to ensure that the CEO's device is returned as soon as possible<sup>1</sup>

**NEW QUESTION 141**

A technician is setting up a backup method on a workstation that only requires two sets of

tapes to restore. Which of the following would BEST accomplish this task?

- A. Differential backup
- B. Off-site backup
- C. Incremental backup
- D. Full backup

**Answer:** D

**Explanation:**

To accomplish this task, the technician should use a Full backup method



A full backup only requires two sets of tapes to restore because it backs up all the data from the workstation. With a differential backup, the backups need to be taken multiple times over a period of time, so more tapes would be needed to restore the data<sup>1</sup>

#### NEW QUESTION 144

A macOS user reports seeing a spinning round cursor on a program that appears to be frozen. Which of the following methods does the technician use to force the program to close in macOS?

- A. The technician presses the Ctrl+Alt+Del keys to open the Force Quit menu, selects the frozen application in the list, and clicks Force Quit.
- B. The technician clicks on the frozen application and presses and holds the Esc key on the keyboard for 10 seconds Which causes the application to force quit.
- C.

The technician opens Finder, navigates to the Applications folder, locates the application that is frozen in the list, right-clicks on the application, and selects the Force Quit option.

- D. The technician opens the Apple icon menu, selects Force Quit, selects the frozen application in the list, and clicks Force Quit.

**Answer:** D

#### Explanation:

The technician opens the Apple icon menu, selects Force Quit, selects the frozen application in the list, and clicks Force Quit. This is the most common method of force quitting a program in macOS. This can be done by clicking on the Apple icon in the top left of the screen, selecting Force Quit, selecting the frozen application in the list, and then clicking Force Quit. This will force the application to quit and the spinning round cursor will disappear.

#### NEW QUESTION 145

A SOHO client is having trouble navigating to a corporate website. Which of the following should a technician do to allow access?

- A. Adjust the content filtering.
- B. Unmap port forwarding.
- C. Disable unused ports.
- D. Reduce the encryption strength

**Answer:** A

#### Explanation:

Content filtering is a process that manages or screens access to specific emails or webpages based on their content categories<sup>1</sup>. Content filtering can be used by organizations to control content access through their firewalls and enforce corporate policies around information system management<sup>2</sup>. A SOHO client may have

content filtering enabled on their network and may need to adjust it to allow access to a corporate website that is blocked by default. The client can use a software program, a hardware device, or a subscription service to configure the content filtering settings and whitelist the desired website<sup>2</sup>.

References: 1: Web content filtering (<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/web-content-filtering?view=o365-worldwide>) 2: What is Content Filtering? Definition and Types of Content Filters (<https://www.fortinet.com/resources/cyberglossary/content-filtering>)

#### NEW QUESTION 146

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? (Select TWO).

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

The technician can close unnecessary applications and turn on autorotation to resolve these issues with minimal impact. Autorotation can help the device to switch between portrait and landscape modes automatically. Closing unnecessary applications can help to free up the device's memory and reduce the device's temperature<sup>1</sup>

Reference:

CompTIA A+ Certification Exam: Core 2 (220-1102) Exam Objectives Version 4.0. Retrieved from [https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-\(3-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-(3-0))

#### NEW QUESTION 147

A technician sees a file that is requesting payment to a cryptocurrency address. Which of the following should the technician do first?

- A. Quarantine the computer.
- B. Disable System Restore.
- C. Update the antivirus software definitions.
- D. Boot to safe mode.

**Answer:** A

#### Explanation:

Quarantining the computer means isolating it from the network and other devices to prevent the spread of malware or ransomware. Ransomware is a type of malware that encrypts the files on a computer and demands payment (usually in cryptocurrency) to restore them. If a technician sees a file that is requesting payment to a cryptocurrency address, it is likely that the computer has been infected by ransomware. Quarantining the computer should be the first step to contain the infection and prevent further damage. Disabling System Restore, updating the antivirus software definitions, and booting to safe mode are not steps that should be done before quarantining the computer.

#### NEW QUESTION 152

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:

Badge readers are used to implement secure physical access to a data center. They are used to read the identification information on an employee's badge and grant access to the data center if the employee is authorized<sup>2</sup>.

This system requires individuals to have an access badge that contains their identification information or a unique code that can be scanned by a reader. After the badge is scanned, the system compares the information on the badge with the authorized personnel database to authenticate if the individual has the required clearance to enter that area. The other options listed, such as a geofence, alarm system, or motion sensor are security measures that may be used in conjunction with badge readers, but do not provide identification and authentication features.

#### NEW QUESTION 153

A user clicks a link in an email. A warning message in the user's browser states the site's certificate cannot be verified. Which of the following is the most appropriate action for a technician to take?

- A. Click proceed.
- B. Report the employee to the human resources department for violating company policy.
- C. Restore the computer from the last known backup.
- D. Close the browser window and report the email to IT security.

**Answer:** D

#### Explanation:

A warning message in the user's browser stating the site's certificate cannot be verified indicates that the site may be insecure, fraudulent, or malicious. This could be a sign of a phishing attempt, where the sender of the email tries to trick the user into clicking a link that leads to a fake website that mimics a legitimate one, in order to steal the user's personal or financial information. The most appropriate action for a technician to take in this situation is to close the browser window and report the email to IT security, who can investigate the source and content of the email, and take the necessary steps to protect the user and the network from potential harm. Clicking proceed could expose the user to malware, identity theft, or data breach. Reporting the employee to the human resources

department for violating company policy is unnecessary and harsh, as the user may not have been aware of the phishing attempt or the company policy. Restoring the computer from the last known backup is premature and ineffective, as the user may not have been infected by anything, and the backup may not remove the email or the link from the user's inbox

#### NEW QUESTION 157

Which of the following would typically require the most computing resources from the host computer?

- A. Chrome OS
- B. Windows
- C. Android
- D. macOS
- E. Linux

**Answer:** B

#### Explanation:

Windows is the operating system that typically requires the most computing resources from the host computer, compared to the other options. Computing resources include hardware components such as CPU, RAM, disk space, graphics card, and network adapter. The minimum system requirements for an operating system indicate the minimum amount of computing resources needed to install and run the operating system on a computer. The higher the minimum system requirements, the more computing resources the operating system consumes.

According to the web search results, the minimum system requirements for Windows 10 and Windows 11 are as follows<sup>12</sup>:

? CPU: 1 GHz or faster with two or more cores (Windows 10); 1 GHz or faster with

two or more cores on a compatible 64-bit processor (Windows 11)

? RAM: 1 GB for 32-bit or 2 GB for 64-bit (Windows 10); 4 GB (Windows 11)

? Disk space: 16 GB for 32-bit or 32 GB for 64-bit (Windows 10); 64 GB (Windows 11)

? Graphics card: DirectX 9 or later with WDDM 1.0 driver (Windows 10); DirectX 12 compatible with WDDM 2.0 driver (Windows 11)

? Network adapter: Ethernet or Wi-Fi (Windows 10); Ethernet or Wi-Fi that supports 5 GHz (Windows 11)

The minimum system requirements for macOS Ventura are as follows:

? CPU: Intel Core i3 or higher, or Apple M1 chip

? RAM: 4 GB

? Disk space: 35.5 GB

? Graphics card: Metal-capable

? Network adapter: Ethernet or Wi-Fi

The minimum system requirements for Chrome OS are as follows:

? CPU: Intel Celeron or higher

? RAM: 2 GB

? Disk space: 16 GB

? Graphics card: Integrated

? Network adapter: Ethernet or Wi-Fi

The minimum system requirements for Android are as follows:

? CPU: 1 GHz or higher

? RAM: 512 MB

? Disk space: 8 GB

? Graphics card: OpenGL ES 2.0

? Network adapter: Ethernet or Wi-Fi

The minimum system requirements for Linux vary depending on the distribution, but a common example is Ubuntu, which has the following minimum system requirements:

? CPU: 2 GHz dual core processor or better

? RAM: 4 GB

? Disk space: 25 GB

? Graphics card: 1024 x 768 screen resolution

? Network adapter: Ethernet or Wi-Fi

Based on the comparison of the minimum system requirements, Windows has the highest requirements for CPU, RAM, disk space, and graphics card, while Chrome OS and Android have the lowest requirements. macOS and Linux have moderate requirements, depending on the hardware and software configuration. Therefore, Windows is the operating system that typically requires the most computing resources from the host computer.

References:

? Windows, macOS, Chrome OS, or Linux: Which Operating System Is Right for You?<sup>1</sup>

? Comparison of operating systems<sup>3</sup>

? Windows 10 vs 11 Minimum System Requirements: Why Need a New One?<sup>2</sup>

? macOS Monterey - Technical Specifications

? Chrome OS - Wikipedia

? Android - Wikipedia

? Installation/SystemRequirements - Community Help Wiki

#### NEW QUESTION 162

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

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

**Answer:** A

#### Explanation:

The feature that BEST addresses the user's concern is remote wipe. This is because remote wipe allows the user to erase all data on the mobile device if it is lost or stolen, which will prevent unauthorized access to the device<sup>1</sup>.

#### NEW QUESTION 165

A technician is tasked with configuring a computer for a visually impaired user. Which of the following utilities should the technician use?

- A. Device Manager
- B. Ease of Access Center
- C. System
- D. Programs and Features

**Answer: C**

**Explanation:**

The Ease of Access Center is a built-in utility in Windows that provides tools and options for making a computer easier to use for individuals with disabilities, including the visually impaired. In the Ease of Access Center, the technician can turn on options like high contrast display, screen magnification, and screen reader software to help the user better interact with the computer.

**NEW QUESTION 169**

An implementation specialist is replacing a legacy system at a vendor site that has only one wireless network available. When the specialist connects to Wi-Fi, the specialist realizes the insecure network has open authentication. The technician needs to secure the vendor's sensitive data. Which of the following should the specialist do FIRST to protect the company's data?

- A. Manually configure an IP address, a subnet mask, and a default gateway.
- B. Connect to the vendor's network using a VPN.
- C. Change the network location to private.
- D. Configure MFA on the network.

**Answer: B**

**Explanation:**

The first thing that the specialist should do to protect the company's data on an insecure network with open authentication is to connect to the vendor's network using a VPN. A VPN stands for Virtual Private Network and is a technology that creates a secure and encrypted connection over a public or untrusted network. A VPN can protect the company's data by preventing eavesdropping, interception or modification of the network traffic by unauthorized parties. A VPN can also provide access to the company's internal network and resources remotely. Manually configuring an IP address, a subnet mask and a default gateway may not be necessary or possible if the vendor's network uses DHCP to assign network configuration parameters automatically. Manually configuring an IP address, a subnet mask and a default gateway does not protect the company's data from network attacks or threats. Changing the network location to private may not be advisable or effective if the vendor's network is a public or untrusted network. Changing the network location to private does not protect the company's data from network attacks or threats. Configuring MFA on the network may not be feasible or sufficient if the vendor's network has open authentication and does not support or require MFA. Configuring MFA on the network does not protect the company's data from network attacks or threats. References: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 3.3

**NEW QUESTION 173**

Users access files in the department share. When a user creates a new subfolder, only that user can access the folder and its files. Which of the following will MOST likely allow all users to access the new folders?

- A. Assigning share permissions
- B. Enabling inheritance
- C. Requiring multifactor authentication
- D. Removing archive attribute

**Answer: B**

**Explanation:**

Enabling inheritance is a method that allows new subfolders to inherit the permissions and settings from their parent folder. If users can access files in the department share, but not in the new subfolders created by other users, it may indicate that inheritance is disabled and that each new subfolder has its own permissions and settings that restrict access to only the creator. Enabling inheritance can help resolve this issue by allowing all users to access the new subfolders with the same permissions and settings as the department share. Assigning share permissions, requiring multifactor authentication, and removing archive attribute are not methods that can most likely allow all users to access the new folders.

**NEW QUESTION 178**

Which of the following is an example of MFA?

- A. Fingerprint scan and retina scan
- B. Password and PIN
- C. Username and password
- D. Smart card and password

**Answer: D**

**Explanation:**

Smart card and password is an example of two-factor authentication (2FA), not multi-factor authentication (MFA). MFA requires two or more authentication factors. Smart card and password is an example of two-factor authentication (2FA2)

**NEW QUESTION 181**

A payroll workstation has data on it that needs to be readily available and can be recovered quickly if something is accidentally removed. Which of the following backup methods should be used to provide fast data recovery in this situation?

- A. Full
- B. Differential
- C. Synthetic
- D. Incremental

**Answer:** A

**Explanation:**

A full backup does not depend on any previous backups, unlike differential or incremental backups, which only save the changes made since the last backup. A synthetic backup is a type of full backup that combines an existing full backup with incremental backups to create a new full backup, but it still requires multiple backup sets to recover data. Therefore, a full backup is the most suitable for the payroll workstation that needs to have its data readily available and recoverable. You can learn more about the differences between full, differential, incremental, and synthetic backups from this article.

**NEW QUESTION 186**

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. Rollback plan
- C. Risk level
- D. End user acceptance

**Answer:** C

**Explanation:**

The rollback plan should be updated before requesting approval again. A rollback plan is a plan for undoing a change if it causes problems, and it is an important part of any change management process. If the change advisory board did not approve the requested change due to the lack of alternative actions if implementation failed, then updating the rollback plan would be the best way to address this concern.

**NEW QUESTION 187**

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:**

Bollards are the best solution to enhance building security in order to prevent vehicles from driving into the building while also maintaining easy access for customers. References: 2. Bollards. Retrieved from <https://en.wikipedia.org/wiki/Bollard>

**NEW QUESTION 191**

A user tries to access commonly used web pages but is redirected to unexpected websites. Clearing the web browser cache does not resolve the issue. Which of the following should a technician investigate NEXT to resolve the issue?

- A. Enable firewall ACLs.
- B. Examine the localhost file entries.
- C. Verify the routing tables.
- D. Update the antivirus definitions.

**Answer:** B

**Explanation:**

A possible cause of the user being redirected to unexpected websites is that the localhost file entries have been modified by malware or hackers to point to malicious or unwanted websites. The localhost file is a text file that maps hostnames to IP addresses and can override DNS settings. By examining the localhost file entries, a technician can identify and remove any suspicious or unauthorized entries that may cause the redirection issue. Enabling firewall ACLs may not resolve the issue if the firewall rules do not block the malicious or unwanted websites. Verifying the routing tables may not resolve the issue if the routing configuration is correct and does not affect the web traffic. Updating the antivirus definitions may help prevent future infections but may not remove the existing malware or changes to the localhost file. References: CompTIA A+ Core 2 (220-1102) Certification Exam Objectives Version 4.0, Domain 1.3

**NEW QUESTION 196**

An organization's Chief Financial Officer (CFO) is concerned about losing access to very sensitive, legacy unmaintained PII on a workstation if a ransomware outbreak occurs. The CFO has a regulatory requirement to retain this data for many years. Which of the following backup methods would BEST meet the requirements?

- A. A daily, incremental backup that is saved to the corporate file server
- B. An additional, secondary hard drive in a mirrored RAID configuration
- C. A full backup of the data that is stored off-site in cold storage
- D. Weekly, differential backups that are stored in a cloud-hosting provider

**Answer:** C

**Explanation:**

According to CompTIA A+ Core 2 objectives, a full backup stored off-site provides the greatest protection against data loss in the event of a ransomware attack or other data disaster. By storing the backup in a separate physical location, it is less likely to be affected by the same event that could cause data loss on the original system. Cold storage is a term used for data archiving, which typically refers to a long-term storage solution that is used for retaining data that is infrequently accessed, but still needs to be kept for regulatory or compliance reasons.



#### NEW QUESTION 201

During an enterprise rollout of a new application, a technician needs to validate compliance with an application's EULA while also reducing the number of licenses to manage. Which of the following licenses would best accomplish this goal?

- A. Personal use license
- B. Corporate use license
- C. Open-source license
- D. Non-expiring license

**Answer: B**

#### Explanation:

A corporate use license, also known as a volume license, is a type of software license that allows an organization to purchase and use multiple copies of a software product with a single license key. A corporate use license can help validate compliance with an application's EULA (end-user license agreement), which is a legal contract that defines the terms and conditions of using the software. A corporate use license can also reduce the number of licenses to manage, as it eliminates the need to activate and track individual licenses for each copy of the software. Personal use license, open-source license, and non-expiring license are not types of licenses that can best accomplish this goal.

#### NEW QUESTION 203

Which of the following command-line tools will delete a directory?

- A. md
- B. del
- C. dir
- D. rd
- E. cd

**Answer: D**

#### Explanation:

To delete an empty directory, enter `rd Directory` or `rmdir Directory`. If the directory is not empty, you can remove files and subdirectories from it using the `/s` switch. You can also use the `/q` switch to suppress confirmation messages (quiet mode).

#### NEW QUESTION 206

Which of the following involves sending arbitrary characters in a web page request?

- A. SMS
- B. SSL
- C. XSS
- D. VPN

**Answer: C**

#### Explanation:

XSS stands for cross-site scripting, which is a web security vulnerability that allows an attacker to inject malicious code into a web page that is viewed by other users<sup>1</sup>. XSS involves sending arbitrary characters in a web page request, such as a query string, a form field, a cookie, or a header, that contain a malicious script.

The web server does not validate or encode the input, and returns it as part of the web page response. The browser then executes the script, which can perform various actions on behalf of the attacker, such as stealing cookies, session tokens, or other sensitive information, redirecting the user to a malicious site, or displaying fake content.

#### NEW QUESTION 209

A technician needs to add an individual as a local administrator on a Windows home PC. Which of the following utilities would the technician MOST likely use?

- A. Settings > Personalization
- B. Control Panel > Credential Manager
- C. Settings > Accounts > Family and Other Users
- D. Control Panel > Network and Sharing Center

**Answer: C**

#### Explanation:

The technician would most likely use Settings > Accounts > Family and Other Users to add an individual as a local administrator on a Windows home PC. Settings > Accounts > Family and Other Users allows users to add and manage other user accounts on their Windows PC. The technician can add an individual as a local administrator by selecting Add someone else to this PC under Other users and following the steps to create a new user account with administrator privileges. Settings > Personalization allows users to customize the appearance and behavior of their desktop, such as themes, colors, backgrounds, lock screen and screensaver. Settings > Personalization is not related to adding an individual as a local administrator on a Windows home PC but to configuring desktop settings and preferences. Control Panel > Credential Manager allows users to view and manage their web credentials and Windows credentials stored on their Windows PC. Control Panel > Credential Manager is not related to adding.

#### NEW QUESTION 214

A systems administrator installed the latest Windows security patch and received numerous tickets reporting slow performance the next day. Which of the following should the administrator do to resolve this issue?

- A. Rebuild user profiles.
- B. Roll back the updates.
- C. Restart the services.
- D. Perform a system file check.

**Answer:**

B

**Explanation:**

Rolling back the updates is the best way to resolve the issue of slow performance caused by installing the latest Windows security patch. This can be done by using the System Restore feature or by uninstalling the specific update from the Control Panel. Rebuilding user profiles, restarting the services and performing a system file check are not likely to fix the issue, since they do not undo the changes made by the update. Verified References: <https://www.comptia.org/blog/how-to-roll-back-windows-updates> <https://www.comptia.org/certifications/a>

**NEW QUESTION 219**

A user connected an external hard drive but is unable to see it as a destination to save files. Which of the following tools will allow the drive to be formatted?

- A. Disk Management
- B. Device Manager
- C. Disk Cleanup
- ☒ D. Disk Defragmenter

**Answer:** A

**Explanation:**

Disk Management is a tool that allows users to create, format, delete, shrink, extend, and manage partitions on hard drives. If the external hard drive is not formatted or has an incompatible filesystem type, Disk Management can be used to format it with a supported filesystem type such as NTFS, FAT32, or exFAT. Device Manager, Disk Cleanup, and Disk Defragmenter are not tools that can format a hard drive.

**NEW QUESTION 223**

A technician is selling up a newly built computer. Which of the following is the FASTEST way for the technician to install Windows 10?

- A. Factory reset
- B. System Restore
- ☒ C. In-place upgrade
- D. Unattended installation

**Answer:** D

**Explanation:**

An unattended installation is the fastest way to install Windows 10 on a newly built computer. It uses an answer file that contains all the configuration settings and preferences for the installation, such as language, product key, partition size, etc. It does not require any user interaction or input during the installation process. Factory reset, System Restore and in-place upgrade are not methods of installing Windows 10 on a new computer, but ways of restoring or updating an existing Windows installation. Verified References: <https://www.comptia.org/blog/what-is-an-unattended-installation> <https://www.comptia.org/certifications/a>

**NEW QUESTION 224**

A technician wants to mitigate unauthorized data access if a computer is lost or stolen. Which of the following features should the technician enable?

- A. Network share
- B. Group Policy
- C. BitLocker
- D. Static IP

**Answer:** C

**Explanation:**

BitLocker is a Windows security feature that provides encryption for entire volumes, addressing the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned devices<sup>1</sup>. BitLocker helps mitigate unauthorized data access by enhancing file and system protections, rendering data inaccessible when BitLocker-protected devices are decommissioned or recycled<sup>1</sup>. Network share, Group Policy, and Static IP are not features that can prevent unauthorized data access if a computer is lost or stolen.

References:

- ? BitLocker overview - Windows Security | Microsoft Learn<sup>1</sup>
- ? The Official CompTIA A+ Core 2 Study Guide<sup>2</sup>, page 315.

**NEW QUESTION 229**

Sensitive data was leaked from a user's smartphone. A technician discovered an unapproved application was installed, and the user has full access to the device's command shell. Which of the following is the NEXT step the technician should take to find the cause of the leaked data?

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

**Answer:** B

**Explanation:**

The technician should disable the user's access to the device's command shell. This will prevent the user from accessing sensitive data and will help to prevent further data leaks. The technician should then investigate the unapproved application to determine if it is the cause of the data leak. If the application is found to be the cause of the leak, the technician should uninstall the application and restore the device to factory settings. If the application is not the cause of the leak, the technician should investigate further to determine the cause of the leak. Disabling the ability to install applications from unknown sources can help to prevent future data leaks, but it is not the next step the technician should take in this scenario. Ensuring the device is connected to the corporate WiFi network is not relevant to this scenario<sup>1</sup>

**NEW QUESTION 232**

A technician received a call stating that all files in a user's documents folder appear to be Changed, and each of the files now has a look file extension Which pf the following actions is the FIRST step the technician should take?

- A. Run a live disk clone.
- B. Run a full antivirus scan.
- C. Use a batch file to rename the files-
- D. Disconnect the machine from the network

**Answer:** D

**Explanation:**

The CompTIA A+ Core 2 220-1102 exam covers this topic in the following domains: 1.2 Given a scenario, use appropriate resources to support users and 1.3 Explain the importance of security awareness.

**NEW QUESTION 236**

A technician is troubleshooting an issue that requires a user profile to be rebuilt. The technician is unable to locate Local Users and Groups in the Mtv1C console. Which of the following is the NEXT step the technician should take to resolve the issue?

- A. Run the antivirus scan.
- B. Add the required snap-in.
- C. Restore the system backup
- D. use the administrator console.

**Answer:** B

**Explanation:**

Local Users and Groups is a Microsoft Management Console (MMC) snap-in that allows you to manage user accounts or groups on your computer1. If you cannot find it in the MMC console, you can add it manually by following these steps2:

? Press Windows key + R to open the Run dialog box, or open the Command Prompt.

? Type mmc and hit Enter. This will open a blank MMC console.

? Click File and then Add/Remove Snap-in.

? In the Add or Remove Snap-ins window, select Local Users and Groups from the Available snap-ins list, and click Add.

? In the Select Computer window, choose Local computer or Another computer, depending on which computer you want to manage, and click Finish.

? Click OK to close the Add or Remove Snap-ins window. You should now see Local Users and Groups in the MMC console.

**NEW QUESTION 240**

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 OS utility used to change the color of the cursor in Windows is Ease of Access Center 12

The user can change the cursor color by opening the Settings app,

selecting Accessibility in the left sidebar, selecting Mouse pointer and touch under Vision, and choosing one of the cursor options. The user can select Custom to pick a color and

use the Size slider to make the cursor larger or smaller2r

The Ease of Access Center in the Windows OS provides accessibility options for users with disabilities or impairments. One of these options allows the user to change the color and size of the cursor, making it more visible and easier to locate on the screen. The Keyboard and Touchpad settings do not offer the option to change cursor color, and Display Settings are used to adjust the resolution and other properties of the display. Therefore, C is the best answer. This information is covered in the CompTia A+ Core2 documents/guide under the Accessibility section.

**NEW QUESTION 243**

Following a recent power outage, several computers have been receiving errors when booting. The technician suspects file corruption has occurred. Which of the following steps should the technician try FIRST to correct the issue?

- A. Rebuild the Windows profiles.
- B. Restore the computers from backup.
- C. Reimage the computers.
- D. Run the System File Checker.

**Answer:** D

**Explanation:**

The technician should run the System File Checker (SFC) first to correct file corruption errors on computers after a power outage. SFC is a command-line utility that scans for and repairs corrupted system files. It can be run from the command prompt or from the Windows Recovery Environment. Rebuilding the Windows profiles, restoring the computers from backup, and reimaging the computers are more drastic measures that should be taken only if SFC fails to correct the issue1

**NEW QUESTION 247**

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:**

Vishing is a type of social engineering attack where a fraudulent caller impersonates a legitimate entity, such as a bank or financial institution, in order to gain access to sensitive information. The caller will typically use a variety of techniques, such as trying to scare the target or providing false information, in order to get the target to provide the information they are after. Vishing is often used to gain access to usernames, passwords, bank account information, and other sensitive data.

**NEW QUESTION 251**

The battery life on an employee's new phone seems to be drastically less than expected, and the screen stays on for a very long time after the employee sets the phone down. Which of the following should the technician check first to troubleshoot this issue? (Select two).

- A. Screen resolution
- B. Screen zoom
- C. Screen timeout
- D. Screen brightness
- E. Screen damage
- F. Screen motion smoothness

**Answer:** CD

**Explanation:**

Screen timeout is the setting that determines how long the screen stays on after the user stops interacting with the phone. Screen brightness is the setting that determines how much light the screen emits. Both of these settings affect the battery life of the phone, as keeping the screen on longer and brighter consumes more power than turning it off sooner and dimmer. A technician should check these settings first to troubleshoot the issue of low battery life and adjust them accordingly. Screen resolution, screen zoom, screen damage, and screen motion smoothness are not settings that directly affect the battery life or the screen staying on for a long time.

**NEW QUESTION 254**

An administrator responded to an incident where an employee copied financial data to a portable hard drive and then left the company with the data. The administrator documented the movement of the evidence. Which of the following concepts did the administrator demonstrate?

- A. Preserving chain of custody
- B. Implementing data protection policies
- C. Informing law enforcement
- D. Creating a summary of the incident

**Answer:** A

**Explanation:**

Preserving chain of custody is a concept that refers to the documentation and tracking of who handled, accessed, modified, or transferred a piece of evidence, when, where, why, and how. Preserving chain of custody can help establish the authenticity, integrity, and reliability of the evidence, as well as prevent tampering, alteration, or loss of the evidence. An administrator who documented the movement of the evidence demonstrated the concept of preserving chain of custody. Implementing data protection policies, informing law enforcement, and creating a summary of the incident are not concepts that describe the action of documenting the movement of the evidence.

**NEW QUESTION 256**

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 technician should not proceed with initiating a full scan and removal of the viruses using the presented interface or call the phone number displayed in the interface of the antivirus removal tool<sup>12</sup>

Shutting down the infected computer and swapping it with another computer is not necessary at this point<sup>12</sup>

The technician should not immediately assume that the message is legitimate or perform any actions without knowing what the interface is and what triggered it to pop up. It is important to investigate the issue further, including checking the legitimacy of the antivirus program and the message it is displaying.

**NEW QUESTION 261**

A computer technician is investigating a computer that is not booting. The user reports that the computer was working prior to shutting it down last night. The technician notices a removable USB device is inserted, and the user explains the device is a prize the user received in the mail yesterday. Which of the following types of attacks does this describe?

- A. Phishing



- B. Dumpster diving
- C. Tailgating
- D. Evil twin

**Answer:** A

**Explanation:**

Phishing is the correct answer for this question. Phishing is a type of attack that uses fraudulent emails or other messages to trick users into revealing sensitive information or installing malicious software. Phishing emails often impersonate legitimate entities or individuals and offer incentives or threats to lure users into clicking on malicious links or attachments. In this scenario, the user received a removable USB device in the mail as a prize, which could be a phishing attempt to infect the user's computer with malware or gain access to the user's data. Dumpster diving, tailgating, and evil twin are not correct answers for this question. Dumpster diving is a type of attack that involves searching through trash bins or recycling containers to find discarded documents or devices that contain valuable information. Tailgating is a type of attack that involves following an authorized person into a restricted area without proper identification or authorization. Evil twin is a type of attack that involves setting up a rogue wireless access point that mimics a legitimate one to intercept or manipulate network traffic. References:  
? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 25  
? [CompTIA Security+ SY0-601 Certification Study Guide], page 1004

**NEW QUESTION 265**

A technician is working on a way to register all employee badges and associated computer IDs. Which of the following options should the technician use in order to achieve this objective?

- A. Database system
- B. Software management
- C. Active Directory description
- D. Infrastructure as a Service

**Answer:** A

**Explanation:**

A database system is a software application that allows storing, organizing, and managing data in a structured way. A database system can be used to register all employee badges and associated computer IDs by creating a table or a record for each employee that contains their badge number, computer ID, name, and other relevant information. A database system can also facilitate searching, updating, and deleting data as needed. Software management is a general term that refers to the process of planning, developing, testing, deploying, and maintaining software applications. It does not directly address the issue of registering employee badges and computer IDs. Active Directory description is a field in Active Directory that can be used to store additional information about an object, such as a user or a computer. It is not a software application that can be used to register employee badges and computer IDs by itself. Infrastructure as a Service (IaaS) is a cloud computing model that provides servers, storage, networking, and software over the internet. It does not directly address the issue of registering employee badges and computer IDs either.  
<https://www.idcreator.com/>  
<https://www.alphacard.com/photo-id-systems/card-type/employee-badges>

**NEW QUESTION 270**

A change advisory board authorized a setting change so a technician is permitted to implement the change. The technician successfully implemented the change. Which of the following should be done NEXT?

- A. Document the date and time of change.
- B. Document the purpose of the change.
- C. Document the risk level.
- D. Document findings of the sandbox test.

**Answer:** A

**Explanation:**

After implementing a change authorized by the change advisory board (CAB), the technician should document the date and time of change as part of the post-implementation review. This helps to track the change history, verify the success of the change, and identify any issues or incidents caused by the change1. Documenting the purpose of the change, the risk level, and the findings of the sandbox test are all part of the pre-implementation activities that should be done before submitting the change request to the CAB2.  
References: 2: <https://www.manageengine.com/products/service-desk/itil-change-management/cab-change-advisory-board.html> 1: <https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/success/quick-answer/change-advisory-board-setup.pdf>

**NEW QUESTION 271**

A user purchased a netbook that has a web-based, proprietary operating system. Which of the following operating systems is MOST likely installed on the netbook?

- A. macOS
- B. Linux
- C. Chrome OS
- D. Windows

**Answer:** C

**Explanation:**

4. Chrome OS. Retrieved from [https://en.wikipedia.org/wiki/Chrome\\_OS](https://en.wikipedia.org/wiki/Chrome_OS) 5. What is Chrome OS? Retrieved from <https://www.google.com/chromebook/chrome-os/>  
A netbook with a web-based, proprietary operating system is most likely running Chrome OS. Chrome OS is a web-based operating system developed by Google that is designed to work with web applications and cloud storage. It is optimized for netbooks and other low- power devices and is designed to be fast, secure, and easy to use.

**NEW QUESTION 275**



Which of the following allows access to the command line in macOS?

- A. PsExec
- B. command.com
- C. Terminal
- D. CMD

**Answer: C**

**Explanation:**

Terminal is an application that allows access to the command line in macOS. The command line is an interface that allows users to interact with the operating system and perform various tasks by typing commands and arguments. Terminal can be used to launch programs, manage files and folders, configure settings, troubleshoot issues, and run scripts in macOS. PsExec, command.com, and CMD are not applications that allow access to the command line in macOS.

**NEW QUESTION 280**

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

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 282**

A PC is taking a long time to boot Which of the following operations would be best to do to resolve the issue at a minimal expense? (Select two).

- A. Installing additional RAM
- B. Removing the applications from startup
- C. Installing a faster SSD
- D. Running the Disk Cleanup utility
- E. Defragmenting the hard drive
- F. Ending the processes in the Task Manager

**Answer: BD**

**Explanation:**

The best operations to do to resolve the issue of a long boot time at a minimal expense are B. Removing the applications from startup and D. Running the Disk Cleanup utility. These are two simple and effective ways to speed up your PC's boot time without spending any money on hardware upgrades.

Removing the applications from startup means preventing unnecessary programs from launching automatically when you turn on your computer. This can reduce the load on your system resources and make the boot process faster. You can do this in Windows 10 by pressing Ctrl + Alt + Esc to open the Task Manager, and going to the Startup tab. There, you can see a list of programs that start with your computer, and their impact on the startup performance. You can disable any program that you don't need by right-clicking on it and choosing Disable<sup>12</sup>.

Running the Disk Cleanup utility means deleting temporary files, system files, and other unnecessary data that may be taking up space and slowing down your computer. This can free up some disk space and improve the performance of your system. You can do this in Windows 10 by typing disk cleanup in the search box and selecting the Disk Cleanup app. There, you can choose which files you want to delete, such as Recycle Bin, Temporary Internet Files, Thumbnails, etc. You can also click on Clean up system files to delete more files, such as Windows Update Cleanup, Previous Windows installation(s), etc<sup>34</sup>.

**NEW QUESTION 285**

A user connected a laptop to a wireless network and was tricked into providing login credentials for a website. Which of the following threats was used to carry out the attack?

- A. Zero day
- B. Vishing
- C. DDoS
- D. Evil twin

**Answer: B**

**Explanation:**

Vishing, also known as voice phishing, is a type of social engineering attack where the attacker tricks the victim into divulging sensitive information over the phone. In this case, the attacker tricked the user into providing login credentials for a website.

**NEW QUESTION 287**

A corporate smartphone was stored for five months after setup. During this time, the company did not have any system updates. When the phone is turned on, an application runs, but it crashes intermittently. Which of the following should a technician do next?

- A. Restart the phone.
- B. Reimage the OS.
- C. Reinstall the application.
- D. Clear the cache.

**Answer:** C

**Explanation:**

Reinstalling the application is the best option to fix the intermittent crashing of the application on the corporate smartphone. Reinstalling the application will ensure that the latest version of the app is installed, which may have bug fixes and compatibility updates that can resolve the crashing issue. Reinstalling the app will also clear any corrupted or outdated data or cache that may cause the app to malfunction.

The other options are not as effective or appropriate as reinstalling the app. Restarting the phone may temporarily fix the issue, but it will not address the root cause of the app crashing, which may be related to the app itself or its data. Reimaging the OS is a drastic and unnecessary measure that will erase all the data and settings on the phone and restore it to its factory state. This will also remove all the other apps and files that may be important for the corporate use of the phone. Clearing the cache may help to free up some space and improve the performance of the app, but it will not update the app or fix any bugs that may cause the app to crash.

References:

? Top 5 Reasons Behind Your App Crash and Solutions To Fix Them<sup>1</sup>

? How to Stop Apps From Crashing on Android<sup>2</sup>

? Why are my Android phone apps crashing or closing & how to fix the issue<sup>3</sup>

**NEW QUESTION 290**

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. Most Voted
- C. A risk assessment can be performed to determine if the software is needed.
- D. End users can be aware of the scope of the change.
- E. A rollback plan can be implemented in case the software breaks an application.

**Answer:** A

**Explanation:**

change management process can help ensure that owners are notified of changes being made and can monitor them for performance impact (A). This can help prevent unexpected issues from arising.

**NEW QUESTION 295**

A technician is setting up a backup method on a workstation that only requires two sets of tapes to restore. Which of the following would BEST accomplish this task?

- A. Differential backup
- B. Off-site backup
- C. Incremental backup
- D. Full backup

**Answer:** D

**Explanation:**

A full backup involves creating a copy of all data on the workstation, including system files and user-created data, and storing it on a set of tapes. This ensures that all data is backed up, and ensures that the data can be restored in the event of a system failure or data loss.

**NEW QUESTION 296**

A technician cannot uninstall a system driver because the driver is currently in use. Which of the following tools should the technician use to help uninstall the driver?

- A. msinfo32.exe
- B. dxdiag.exe
- C. msconfig.exe
- D. regedit.exe

**Answer:** C

**Explanation:**

The msconfig.exe tool, also known as the System Configuration utility, is a tool that allows users to modify various system settings, such as startup options, services, boot options, and more. One of the features of msconfig.exe is the ability to disable or enable device drivers that are loaded during the system startup. By using msconfig.exe, a technician can prevent a driver from being loaded and used by the system, which will allow them to uninstall it without any errors. To use msconfig.exe to disable a driver, the technician can follow these steps:

? Open the Run dialog box by pressing the Windows key + R.

? Type msconfig.exe and press Enter.

? Click on the Boot tab and then click on Advanced options.

? Check the box next to No GUI boot and click OK. This will prevent the graphical user interface from loading during the boot process, which will also prevent some drivers from loading.

? Click on the Services tab and check the box next to Hide all Microsoft services.

This will show only the third-party services and drivers that are running on the system.

? Find the service or driver that corresponds to the device that the technician wants

to uninstall and uncheck the box next to it. This will disable the service or driver from starting during the system startup.

? Click Apply and OK and then restart the computer.

? After the computer restarts, the technician can use the Device Manager or the Control Panel to uninstall the driver that was previously in use.

References:

? How to Completely Remove/Uninstall a Driver in Windows, section 31

? The Official CompTIA A+ Core 2 Study Guide (220-1102), page 2212

#### NEW QUESTION 297

Which of the following change management documents includes how to uninstall a patch?

- A. Purpose of change
- B. Rollback plan
- C. Scope of change
- D. Risk analysis

**Answer: B**

#### Explanation:

The change management document that includes how to uninstall a patch is called the “rollback plan”. The rollback plan is a document that outlines the steps that should be taken to undo a change that has been made to a system. In the case of a patch, the rollback plan would include instructions on how to uninstall the patch if it causes problems or conflicts with other software<sup>12</sup>

#### NEW QUESTION 298

A user needs assistance installing software on a Windows PC but will not be in the office. Which of the following solutions would a technician MOST likely use to assist the user without having to install additional software?

- A. VPN
- B. MSRA
- C. SSH
- D. RDP

**Answer: B**

#### Explanation:

MSRA stands for Microsoft Remote Assistance, and it is a feature that allows a technician to remotely view and control another user's Windows PC with their permission. MSRA is built-in to Windows and does not require any additional software installation. To use MSRA, the technician and the user need to follow these steps:

? On the user's PC, type msra in the search box on the taskbar and select Invite someone to connect to your PC and help you, or offer to help someone else.

? Select Save this invitation as a file and choose a location to save the file. This file contains a password that the technician will need to connect to the user's PC.

? Send the file and the password to the technician via email or another secure method.

? On the technician's PC, type msra in the search box on the taskbar and select Help someone who has invited you.

? Select Use an invitation file and browse to the location where the file from the user is saved. Enter the password when prompted.

? The user will see a message asking if they want to allow the technician to connect to their PC. The user should select Yes.

? The technician will see the user's desktop and can request control of their PC by clicking Request control on the top bar. The user should allow this request by clicking Yes.

? The technician can now view and control the user's PC and assist them with installing software.

#### NEW QUESTION 300

A technician was assigned a help desk ticket and resolved the issue. Which of the following should the technician update to assist other technicians in resolving similar issues?

- A. End user training
- B. Progress notes
- C. Knowledge base
- D. Acceptable use policy document

**Answer: C**

#### Explanation:

A knowledge base is a centralized repository of information that can be used by technicians to find solutions to common problems, best practices, troubleshooting guides, and other useful resources<sup>12</sup>. Updating the knowledge base with the details of the

issue and the resolution can help other technicians who encounter similar issues in the future. It can also reduce the number of tickets and improve customer satisfaction<sup>3</sup>. References<sup>1</sup>: The Official CompTIA A+ Core 2 Student Guide (Exam 220-1102), page 10-11 <sup>2</sup>: CompTIA A+ Certification Exam Core 2 Objectives, page 13 <sup>3</sup>: CompTIA A+ Core 2 (220-1102) Certification Study Guide, page 10-12

#### NEW QUESTION 301

A technician discovers user input has been captured by a malicious actor. Which of the following malware types is MOST likely being used?

- A. Cryptominers
- B. Rootkit
- C. Spear phishing
- D. Keylogger

**Answer: D**

#### Explanation:

A keylogger is a type of malware that captures user input, such as keystrokes, mouse clicks, and clipboard data, and sends it to a malicious actor. Keyloggers can be used to steal passwords, credit card numbers, personal information, and other sensitive data.

Reference: CompTIA A+ Core 2 Exam Objectives, Section 5.1

#### NEW QUESTION 302

An administrator has submitted a change request for an upcoming server deployment. Which of the following must be completed before the change can be approved?

- A. Risk analysis
- B. Sandbox testing
- C. End user acceptance
- D. Lessons learned

**Answer:** A

**Explanation:**

A risk analysis must be completed before a change request for an upcoming server deployment can be approved 1

Risk analysis is an important step in the change management process because it helps identify and mitigate potential risks before changes are implemented. Once the risks have been analyzed and the appropriate measures have been taken to minimize them, the change can be approved and implemented.

**NEW QUESTION 305**

A technician receives a call from a user who is having issues with an application. To best understand the issue, the technician simultaneously views the user's screen with the user. Which of the following would BEST accomplish this task?

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

**Answer:** C

**Explanation:**

VNC (Virtual Network Computing) is a protocol that allows a technician to simultaneously view and control a user's screen remotely. VNC uses a server-client model, where the user's computer runs a VNC server and the technician's computer runs a VNC client. VNC can work across different platforms and operating systems3. SSH (Secure Shell) is a protocol that allows a technician to access a user's command-line interface remotely, but not their graphical user interface. VPN (Virtual Private Network) is a technology that creates a secure and encrypted connection over a public network, but does not allow screen sharing. RDP (Remote Desktop Protocol) is a protocol that allows a technician to access a user's desktop remotely, but not simultaneously with the user.

**NEW QUESTION 310**

A department manager submits a help desk ticket to request the migration of a printer's port utilization from USB to Ethernet so multiple users can access the printer. This will be a new network printer, thus a new IP address allocation is required. Which of the following should happen immediately before network use is authorized?

- A. Document the date and time of the change.
- B. Submit a change request form
- C. Determine the risk level of this change
- D. Request an unused IP address.

**Answer:** B

**Explanation:**

The correct answer is B. Submit a change request form. A change request form is a document that describes the proposed change, the reason for the change, the expected benefits and impacts, the risks and mitigation strategies, the implementation plan, and the approval process. A change request form is an essential part of change management best practices, as it helps to ensure that the change is well-planned, communicated, and authorized before it is implemented12.

A change request form should be submitted immediately before network use is authorized, because it provides the necessary information and justification for the change to the relevant stakeholders, such as the network administrator, the IT manager, and the department manager. The change request form also allows the stakeholders to review and approve or reject the change, or request more information or modifications. The change request form also serves as a record of the change history and status12.

**NEW QUESTION 314**

A user calls the help desk and reports a workstation is infected with malicious software. Which of the following tools should the help desk technician use to remove the malicious software? (Select TWO).

- A. File Explorer
- B. User Account Control
- C. Windows Backup and Restore
- D. Windows Firewall
- E. Windows Defender
- F. Network Packet Analyzer

**Answer:** AE

**Explanation:**

The correct answers are E. Windows Defender and A. File Explorer.

Windows Defender is a built-in antivirus program that can detect and remove malicious software from a workstation. File Explorer can be used to locate and delete files associated with the malicious software1

**NEW QUESTION 315**

.....

## Relate Links

**100% Pass Your 220-1102 Exam with ExamBible Prep Materials**

<https://www.exambible.com/220-1102-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>