CompTIA

Exam Questions 220-1102

CompTIA A+ Certification Exam: Core 2

NEW QUESTION 1
A user is no longer able to start the OS on a computer and receives an error message indicating there is no OS found. A technician reviews the audit logs and notes that the user's system posted a S.M.A.R.T. error just days before this issue. Which of the following is the MOST likely cause of this issue?

A. Boot order
B. Malware
C. Drive failure
D. Windows updates

Answer: C

Explanation:
A S.M.A.R.T. error is a warning that a hard drive is about to fail or has failed. This means that the OS cannot be loaded from the drive and the user will see an error message indicating there is no OS found. The most likely cause of this issue is drive failure.

NEW QUESTION 2
Which of the following is the MOST basic version of Windows that includes BitLocker?

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

Answer: D

Explanation:
The most basic version of Windows that includes BitLocker is Windows Pro. BitLocker is a feature of Windows Pro that provides full disk encryption for all data on a storage drive [1]. It helps protect data from unauthorized access or theft and can help secure data from malicious attacks. Pro for Workstations includes this feature, as well as other features such as support for up to 6 TB of RAM and ReFS.

NEW QUESTION 3
A developer receives the following error while trying to install virtualization software on a workstation:
VTx not supported by system
Which of the following upgrades will MOST likely fix the issue?

A. Processor
B. Hard drive
C. Memory
D. Video card

Answer: A

Explanation:
The processor is the component that determines if the system supports virtualization technology (VTx), which is required for running virtualization software. The hard drive, memory and video card are not directly related to VTx support, although they may affect the performance of the virtual machines. Verified References: https://www.comptia.org/blog/what-is-virtualization https://www.comptia.org/certifications/a

NEW QUESTION 4
A technician needs to provide recommendations about how to upgrade backup solutions for a site in an area that has frequent hurricanes and an unstable power grid. Which of the following should the technician recommend implementing?

A. High availability
B. Regionally diverse backups
C. On-site backups
D. Incremental backups

Answer: B

Explanation:
Regionally diverse backups are backups that are stored in different geographic locations, preferably far away from the primary site1. This way, if a disaster such as a hurricane or a power outage affects one location, the backups in another location will still be available and accessible2. Regionally diverse backups can help ensure business continuity and data recovery in case of a disaster3. The other options are not the best backup solutions for a site in an area that has frequent hurricanes and an unstable power grid. High availability is a feature that allows a system to remain operational and accessible even if one or more components fail, but it does not protect against data loss or corruption4. On-site backups are backups that are stored in the same location as the primary site, which means they are vulnerable to the same disasters that can affect the primary site. Incremental backups are backups that only store the changes made since the last backup, which means they require less storage space and bandwidth, but they also depend on previous backups to restore data and may not be sufficient for disaster recovery.

NEW QUESTION 5
A user reports a computer is running slow. Which of the following tools will help a technician identity the issued

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Resource Monitor will help a technician identify the issue when a user reports a computer is running slow1

NEW QUESTION 6
A user reports a PC is running slowly. The technician suspects it has a badly fragmented hard drive. Which of the following tools should the technician use?

A. resmon exe
B. msconfig.extf
C. dfrgui exe
D. msmfo32.exe

Answer: C

Explanation:
The technician should use dfrgui.exe to defragment the hard drive1

NEW QUESTION 7
A technician installed Windows 10 on a workstation. The workstation only has 3.5GB of usable RAM, even though the technician installed 8GB. Which of the following is the MOST likely reason this system is not utilizing all the
available RAM?

A. The system is missing updates.
B. The systems utilizing a 32-bit OS.
C. The system's memory is failing.
D. The system requires BIOS updates.

Answer: B

Explanation:
The most likely reason that the system is not utilizing all the available RAM is that it is running a 32-bit OS. A 32-bit OS can only address up to 4GB of RAM, and some of that is reserved for hardware and system use1. Therefore, even if the technician installed 8GB of RAM, the system can only use around 3.5GB of usable RAM. To use the full 8GB of RAM, the technician would need to install a 64-bit OS, which can address much more memory2. The system missing updates, the system’s memory failing, or the system requiring BIOS updates are not likely to cause this issue.
References: 2: https://support.microsoft.com/en-us/windows/windows-10-system-requirements-6d4e9a79-66bf-7950-467c-795cf0386715 1: https://www.makeuseof.com/tag/unlock-64gb-ram-32-bit-windows-pae-patch/

NEW QUESTION 8
A technician installed a new application on a workstation. For the program to function
properly, it needs to be listed in the Path Environment Variable. Which of the following Control Panel utilities should the technician use?

A. System
B. Indexing Options
C. Device Manager
D. Programs and Features

Answer: A

Explanation:
System is the Control Panel utility that should be used to change the Path Environment Variable. The Path Environment Variable is a system variable that specifies the directories where executable files are located. To edit the Path Environment Variable, the technician should go to System > Advanced system settings > Environment Variables and then select Path from the list of system variables and click Edit.

NEW QUESTION 9
A new spam gateway was recently deployed at a small business However; users still occasionally receive spam. The management team is concerned that users will open the messages and potentially
infect the network systems. Which of the following is the MOST effective method for dealing with this Issue?

A. Adjusting the spam gateway
B. Updating firmware for the spam appliance
C. Adjusting AV settings
D. Providing user training

Answer: D

Explanation:
The most effective method for dealing with spam messages in a small business is to provide user training1. Users should be trained to recognize spam messages and avoid opening them1. They should also be trained to report spam messages to the IT department so that appropriate action can be taken1. In addition, users should be trained to avoid clicking on links or downloading attachments from unknown sources1. By providing user training, the management team can reduce the risk of users opening spam messages and potentially infecting the network systems1.

NEW QUESTION 10
A user turns on a new laptop and attempts to log in to specialized software, but receives a message stating that the address is already in use. The user logs on to the old desktop and receives the same message. A technician checks the account and sees a comment that the user requires a specifically allocated address before connecting to the software. Which of the following should the technician do to MOST likely resolve the issue?

A. Bridge the LAN connection between the laptop and the desktop.
B. Set the laptop configuration to DHCP to prevent conflicts.

C. Remove the static IP configuration from the desktop.
D. Replace the network card in the laptop, as it may be defective.

Answer: C

Explanation:
The new laptop was set up with the static IP it needs to connect to the software. The old desktop is still configured with that IP, hence the conflict.

NEW QUESTION 10
A technician is investigating options to secure a small office's wireless network. One requirement is to allow automatic log-ins to the network using certificates instead of passwords. Which of the following should the wireless solution have in order to support this feature?

A. RADIUS
B. AES
C. EAP-EKE
D. MFA

Answer: A

Explanation:
RADIUS is the correct answer for this question. RADIUS stands for Remote Authentication Dial-In User Service, and it is a protocol that provides centralized authentication, authorization, and accounting for wireless networks. RADIUS can support certificate-based authentication, which allows users to log in to the network automatically without entering passwords. RADIUS also provides other benefits, such as enforcing security policies, logging user activities, and managing network access. AES, EAP-EKE, and MFA are not wireless solutions, but rather encryption algorithms, authentication methods, and security factors, respectively.
References:
? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 23
? CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide, page 459

NEW QUESTION 14
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 18
Which of the following macOS features can help a user close an application that has stopped responding?

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

Answer: D

Explanation:
The correct answer is D. Force Quit. Force Quit is a macOS feature that allows users to close an application that has stopped responding. To use Force Quit, users can press and hold Option (or Alt), Command, and Esc (Escape) keys together, or choose Force Quit from the Apple menu in the corner of the screen. A Force Quit window will open, where users can select the application that they want to close and click Force Quit123.
References and Explanation
? The web search results provide information about how to force an app to quit on
Mac using different methods, such as keyboard shortcuts, mouse clicks, or menu options. The results also explain what to do if the app cannot be forced to quit or if the Mac does not respond.
? The first result1 is from the official Apple Support website and provides detailed
instructions and screenshots on how to force an app to quit on Mac using the keyboard shortcut or the Apple menu. It also explains how to force quit the Finder app and how to restart or turn off the Mac if needed.
? The second result2 is from the same website but for a different region (UK). It has
the same content as the first result but with some minor differences in spelling and wording.
? The third result4 is from a website called Lifehacker that provides tips and tricks for
various topics, including technology. It compares how to close a program that is not responding on different operating systems, such as Windows, Mac, and Linux. It briefly mentions how to force quit an app on Mac using the keyboard shortcut or the mouse click.
? The fourth result3 is from a website called Parallels that provides software
solutions for running Windows on Mac. It focuses on how to force quit an app on Mac using the keyboard shortcut and provides a video tutorial and a screenshot on how to do it. It also suggests some alternative ways to close an app that is not responding, such as using Activity Monitor or Terminal commands.

NEW QUESTION 22
Antivirus software indicates that a workstation is infected with ransomware that cannot be quarantined. Which of the following should be performed first to prevent further damage to the host and other systems?

A. Turn off the machine.
B. Run a full antivirus scan.
C. Remove the LAN card.
D. Install a different endpoint solution.

Answer: A

Explanation:
Turning off the machine is the first and most urgent step to prevent further damage to the host and other systems. Ransomware can encrypt files, steal data, and spread to other devices on the network if the infected machine remains online. Turning off the machine will stop the ransomware process and isolate the machine from the network12. The other options are either ineffective or risky. Running a full antivirus scan may not detect or remove the ransomware, especially if it is a new or unknown variant. Removing the LAN card may disconnect the machine from the network, but it will not stop the ransomware from encrypting or deleting files on the local drive. Installing a different endpoint solution may not be possible or helpful if the ransomware has already compromised the system or blocked the installation.
References: 1 3 steps to prevent and recover from ransomware(https://www.microsoft.com/en-us/security/blog/2021/09/07/3-steps-to-prevent- and-recover-from-ransomware/)2 #StopRansomware Guide | CISA(https://www.cisa.gov/stopransomware/ransomware-guide).

NEW QUESTION 25
A company acquired a local office, and a technician is attempting to join the machines at the office to the local domain. The technician notes that the domain join option appears to be missing. Which of the following editions of Windows is MOST likely installed on the machines?

A. Windows Professional
B. Windows Education
C. Windows Enterprise
D. Windows Home

Answer: D

Explanation:
Windows Home is the most likely edition of Windows installed on the machines that do not have the domain join option. Windows Home is a consumer-oriented edition that does not support joining a domain or using Group Policy. Only Windows Professional, Education, and Enterprise editions can join a domain

NEW QUESTION 28
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 (220-1002) Certification Exam Objectives Version 4.0, Domain 3.3

NEW QUESTION 30
Windows updates need to be performed on a department's servers. Which of the following methods should be used to connect to the server?

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

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 31
A company is looking lot 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 33
Which of the following is also known as something you know, something you have, and something you are?

A. ACL
B. MFA
C. SMS
D. NFC

Answer: B

Explanation:
MFA stands for Multi-Factor Authentication, which is a method of verifying a user's identity using two or more different factors of authentication. The three factors of authentication are something you know, something you have, and something you are. These factors correspond to different types of information or evidence that only the legitimate user should possess or provide. For example:
? Something you know: a password, a PIN, a security question, etc.
? Something you have: a smart card, a token, a mobile device, etc.
? Something you are: a fingerprint, a face, an iris, etc.
MFA provides a higher level of security than single-factor authentication, which only uses one factor, such as a password. MFA reduces the risk of unauthorized access, identity theft, and data breaches, as an attacker would need to compromise more than one factor to impersonate a user. MFA is commonly used for online banking, email accounts, cloud services, and other sensitive applications

NEW QUESTION 38
A company-owned mobile device is displaying a high number of ads, receiving data-usage limit notifications, and experiencing slow response. After checking the device, a technician notices the device has been jailbroken. Which of the following should the technician do next?

A. Run an antivirus and enable encryption.
B. Restore the defaults and reimage the corporate OS.
C. Back up the files and do a system restore.
D. Undo the jailbreak and enable an antivirus.

Answer: B

Explanation:
The best course of action for the technician is to restore the defaults and reimage the corporate OS on the device. This will remove the jailbreak and any unauthorized or malicious apps that may have been installed on the device, as well as restore the security features and policies that the company has set for its devices. This will also ensure that the device can receive the latest updates and patches from the manufacturer and the company, and prevent any data leakage or compromise from the device.
Jailbreaking is a process of bypassing the built-in security features of a device to install software other than what the manufacturer has made available for that device1. Jailbreaking allows the device owner to gain full access to the root of the operating system and access all the features1. However, jailbreaking also exposes the device to various risks, such as:
? The loss of warranty from the device manufacturers2.
? Inability to update software until a jailbroken version becomes available2.
? Increased security vulnerabilities32.
? Decreased battery life2.
? Increased volatility of the device2.
Some of the signs of a jailbroken device are:
? A high number of ads, which may indicate the presence of adware or spyware on the device3.
? Receiving data-usage limit notifications, which may indicate the device is sending or receiving data in the background without the user's knowledge or consent3.
? Experiencing slow response, which may indicate the device is running unauthorized or malicious apps that consume resources or interfere with the normal functioning of the device3.
? Finding apps or icons that the user did not install or recognize, such as Cydia, which is a storefront for jailbroken iOS devices1.
The other options are not sufficient or appropriate for dealing with a jailbroken device. Running an antivirus and enabling encryption may not detect or remove all the threats or vulnerabilities that the jailbreak has introduced, and may not restore the device to its original state or functionality. Backing up the files and doing a system restore may not erase the jailbreak or the unauthorized apps, and may also backup the infected or compromised files. Undoing the jailbreak and enabling an antivirus may not be possible or effective, as the jailbreak may prevent the device from updating or installing security software, and may also leave traces of the jailbreak or the unauthorized apps on the device.
References:
? CompTIA A+ Certification Exam Core 2 Objectives4
? CompTIA A+ Core 2 (220-1102) Certification Study Guide5

? What is Jailbreaking & Is it safe? - Kaspersky1
? Is Jailbreaking Safe? The ethics, risks and rewards involved - Comparitech3
? Jailbreaking : Security risks and moving past them2

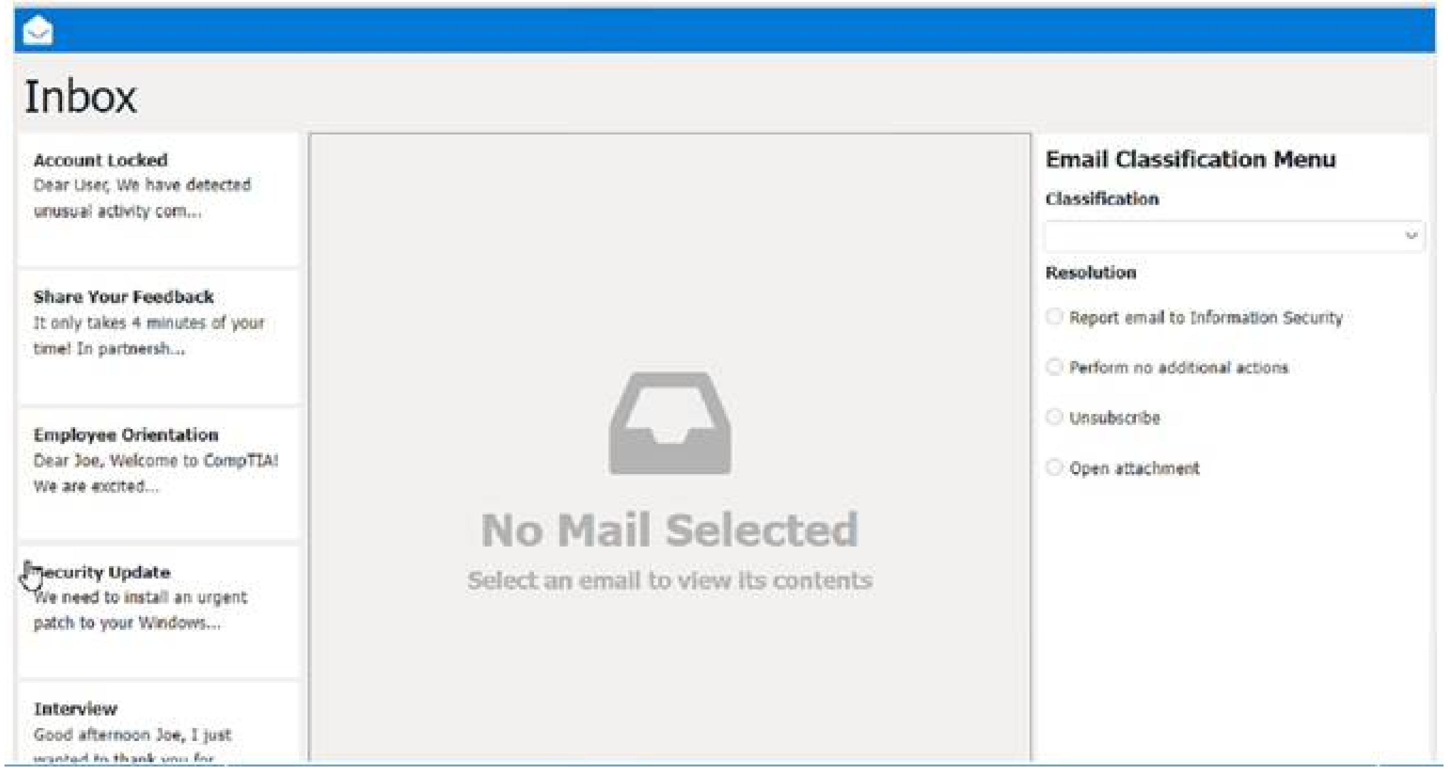
NEW QUESTION 43
A technician downloads a validated security tool and notes the vendor hash of a58e87a2. When the download is complete, the technician again validates the hash, but the value returns as 2a876a7d3. Which of the following is the MOST likely cause of the issue?

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 46
SIMULATION
As a corporate technician, you are asked to evaluate several suspect email messages on a client's computer. Corporate policy requires he 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



Inbox

Account Locked
Dear User, We have detected unusual activity com...

Share Your Feedback
It only takes 4 minutes of your time! In partnersh...

Employee Orientation
Dear Joe, Welcome to CompTIA! We are excited...

Security Update
We need to install an urgent patch to your Windows...

Interview
Good afternoon Joe, I just wanted to thank you for...

No Mail Selected
Select an email to view its contents

Email Classification Menu
Classification

Resolution
○ Report email to Information Security
○ Perform no additional actions
○ Unsubscribe
○ Open attachment

Answer:
See the Full solution in Explanation below.

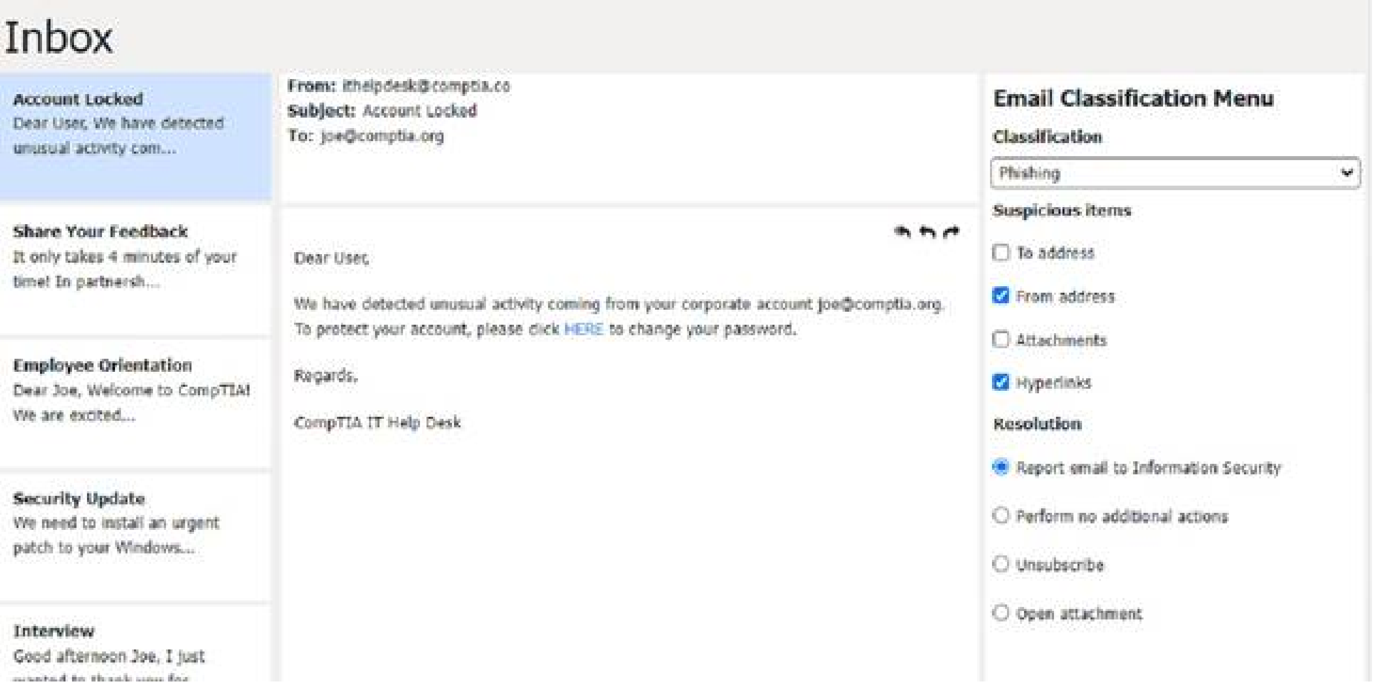
A. Mastered
B. Not Mastered

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.



Inbox

Account Locked
Dear User, We have detected unusual activity com...

Share Your Feedback
It only takes 4 minutes of your time! In partnersh...

Employee Orientation
Dear Joe, Welcome to CompTIA! We are excited...

Security Update
We need to install an urgent patch to your Windows...

Interview
Good afternoon Joe, I just

From: ithelpdesk@comptia.co
Subject: Account Locked
To: joe@comptia.org

Dear User,

We have detected unusual activity coming from your corporate account joe@comptia.org. To protect your account, please click HERE to change your password.

Regards,

CompTIA IT Help Desk

Email Classification Menu

Classification

Phishing

Suspicious items

☐ To address
☑ From address
☐ Attachments
☑ Hyperlinks

Resolution

● Report email to Information Security
○ Perform no additional actions
○ Unsubscribe
○ Open attachment

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:

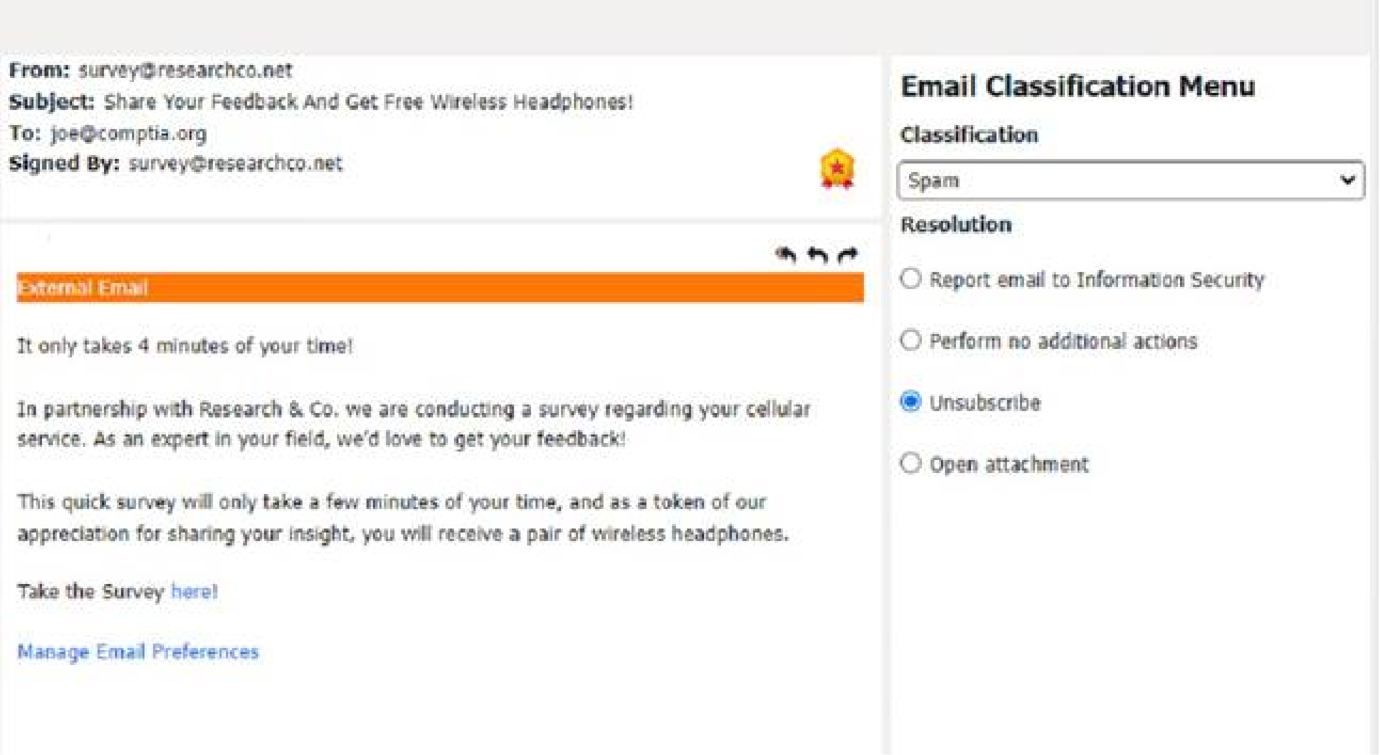
? The email offers a free wireless headphone as an incentive, which is too good to be true.

? 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.



From: survey@researchco.net
Subject: Share Your Feedback And Get Free Wireless Headphones!
To: joe@comptia.org
Signed By: survey@researchco.net

External Email

It only takes 4 minutes of your time!

In partnership with Research & Co. we are conducting a survey regarding your cellular service. As an expert in your field, we'd love to get your feedback!

This quick survey will only take a few minutes of your time, and as a token of our appreciation for sharing your insight, you will receive a pair of wireless headphones.

Take the Survey here!

Manage Email Preferences

Email Classification Menu

Classification

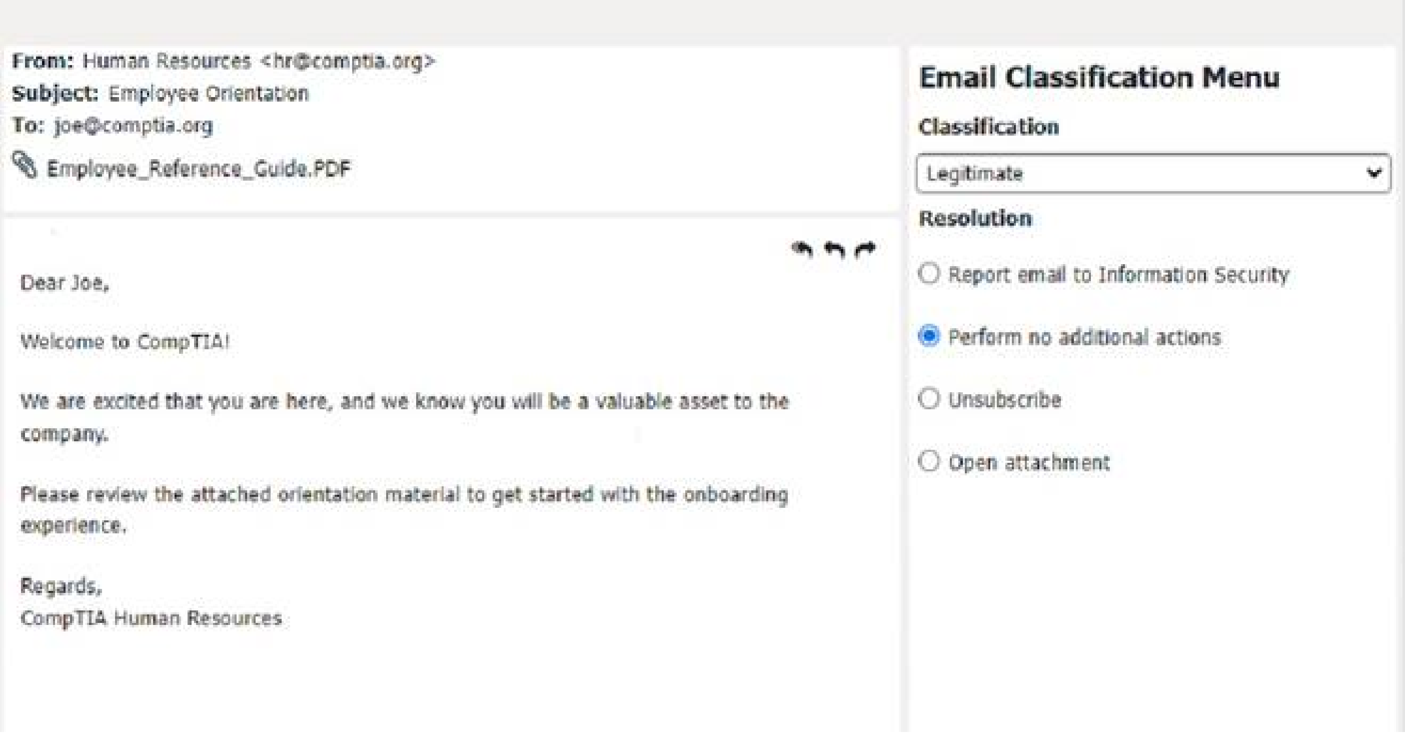
Spam

Resolution

○ Report email to Information Security
○ Perform no additional actions
● Unsubscribe
○ Open attachment

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.



From: Human Resources <hr@comptia.org>
Subject: Employee Orientation
To: joe@comptia.org
Employee_Reference_Guide.PDF

Dear Joe,

Welcome to CompTIA!

We are excited that you are here, and we know you will be a valuable asset to the company.

Please review the attached orientation material to get started with the onboarding experience.

Regards,
CompTIA Human Resources

Email Classification Menu

Classification

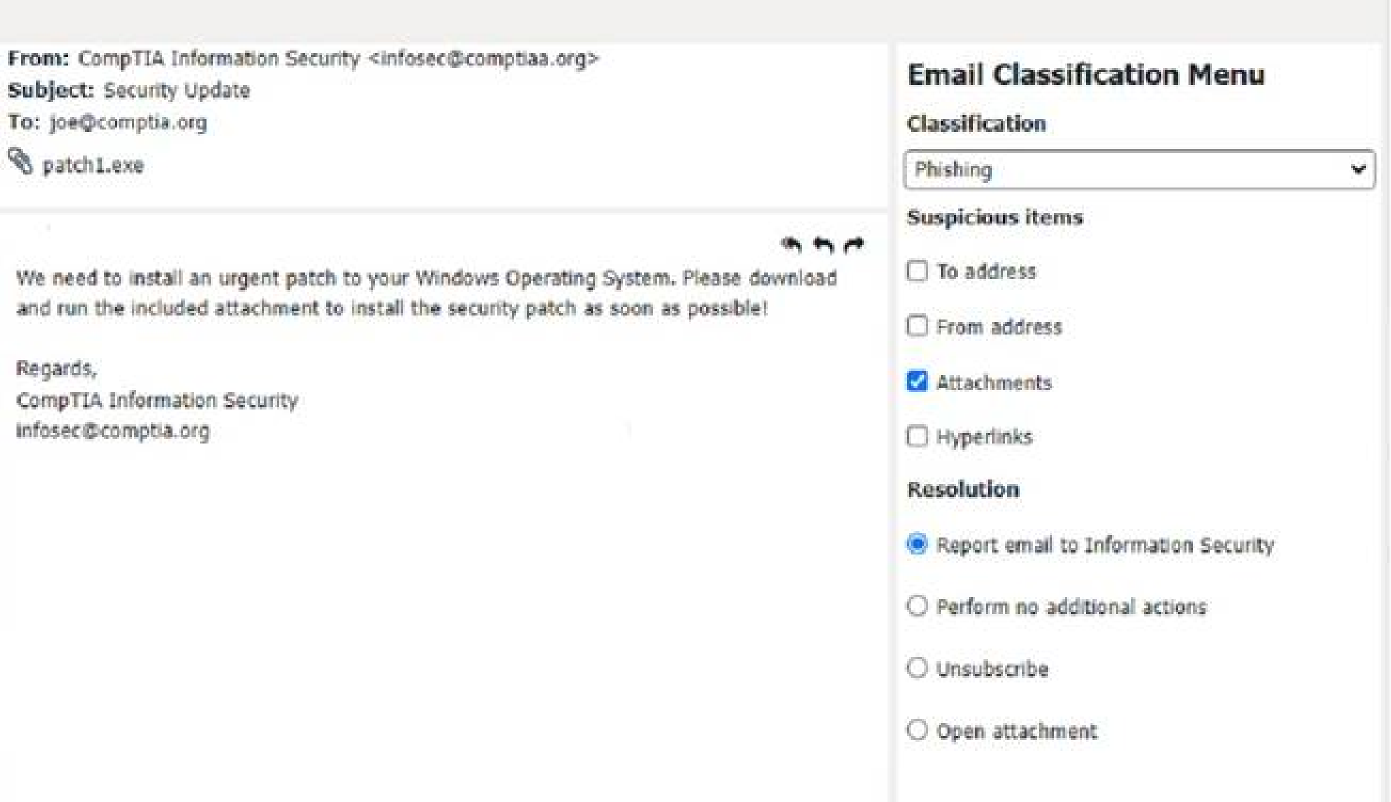
Legitimate

Resolution

○ Report email to Information Security
● Perform no additional actions
○ Unsubscribe
○ Open attachment

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.



From: CompTIA Information Security <infosec@comptiaa.org>
Subject: Security Update
To: joe@comptia.org
patch1.exe

We need to install an urgent patch to your Windows Operating System. Please download and run the included attachment to install the security patch as soon as possible!

Regards,
CompTIA Information Security
infosec@comptia.org

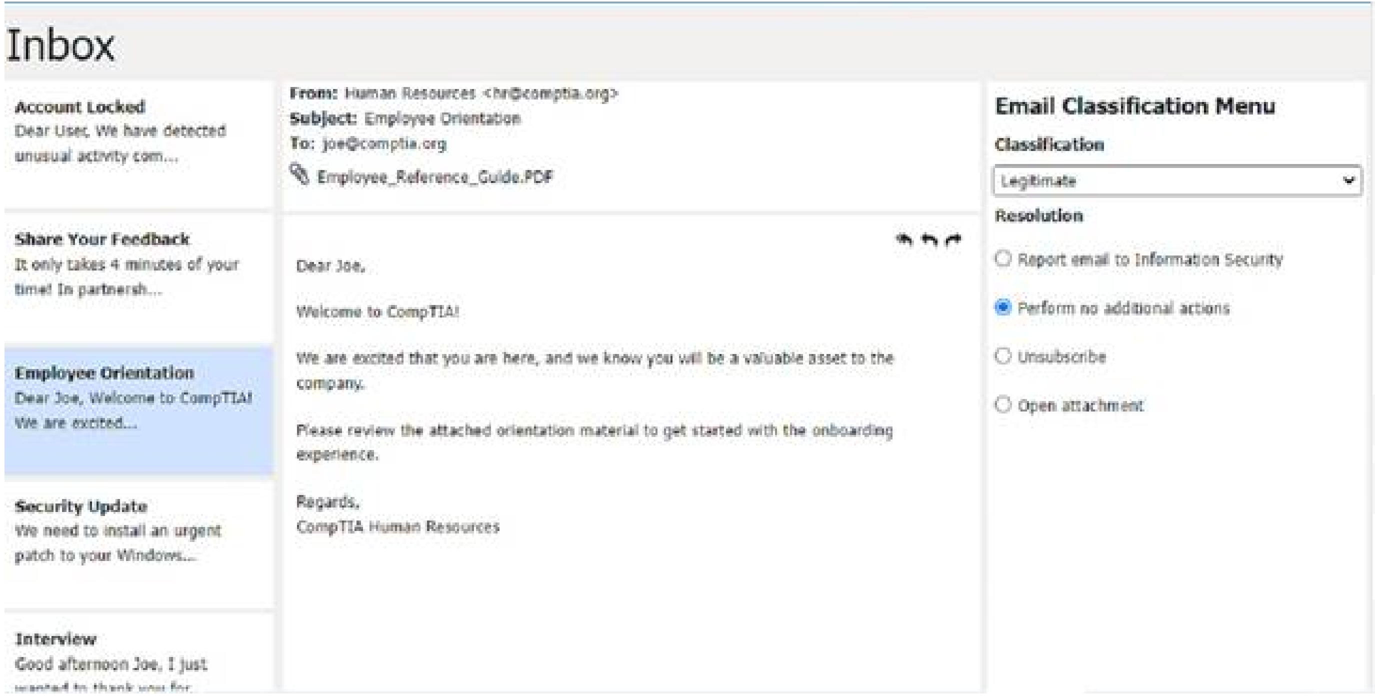
Email Classification Menu

Classification
Phishing

Suspicious items
□ To address
□ From address
☑ Attachments
□ Hyperlinks

Resolution
● Report email to Information Security
○ Perform no additional actions
○ Unsubscribe
○ Open attachment

A screenshot of a computer
Description automatically generated



Inbox

Account Locked
Dear User, We have detected unusual activity com...

Share Your Feedback
It only takes 4 minutes of your time! In partnersh...

Employee Orientation
Dear Joe, Welcome to CompTIA! We are excited...

Security Update
We need to install an urgent patch to your Windows...

Interview
Good afternoon Joe, I just wanted to thank you for

From: Human Resources <hr@comptia.org>
Subject: Employee Orientation
To: joe@comptia.org
Employee_Reference_Guide.PDF

Dear Joe,

Welcome to CompTIA!

We are excited that you are here, and we know you will be a valuable asset to the company.

Please review the attached orientation material to get started with the onboarding experience.

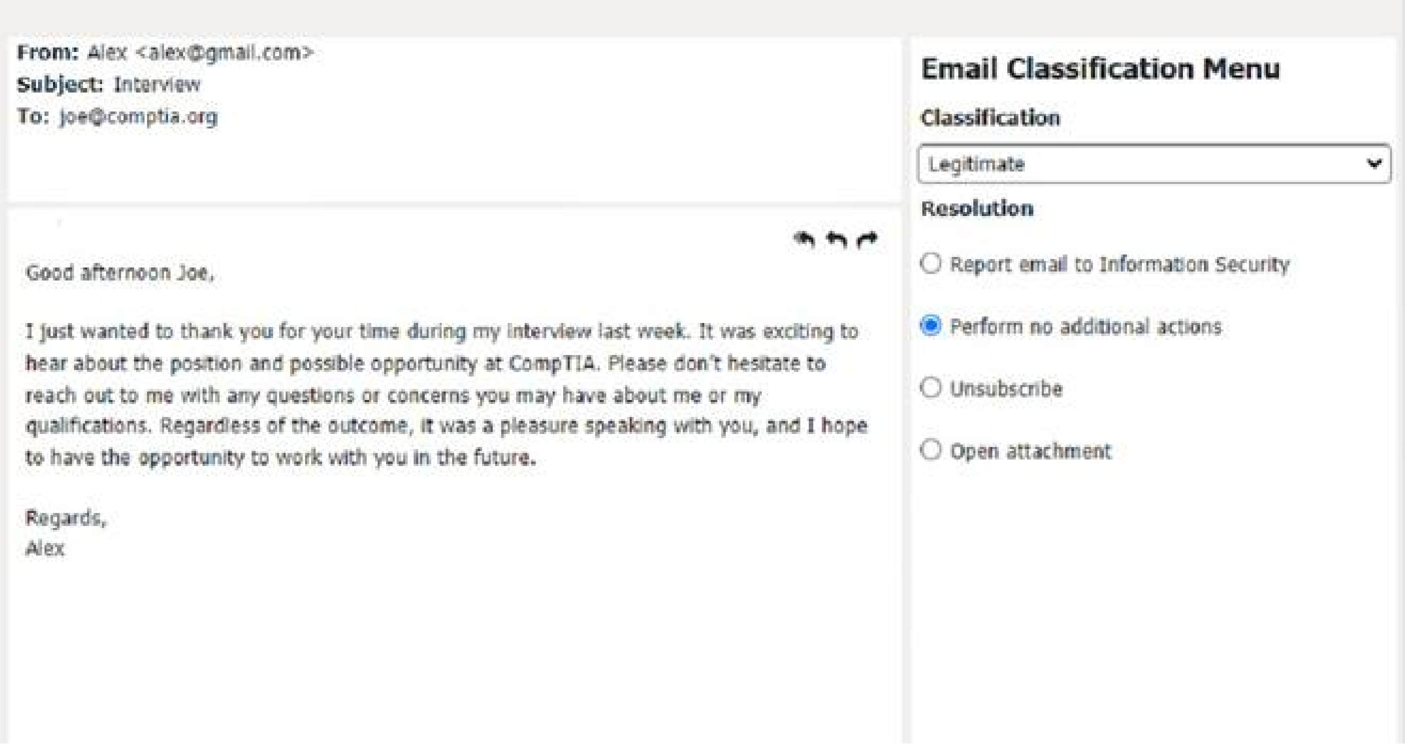
Regards,
CompTIA Human Resources

Email Classification Menu

Classification
Legitimate

Resolution
○ Report email to Information Security
● Perform no additional actions
○ Unsubscribe
○ Open attachment

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.



From: Alex <alex@gmail.com>
Subject: Interview
To: joe@comptia.org

Good afternoon Joe,

I just wanted to thank you for your time during my interview last week. It was exciting to hear about the position and possible opportunity at CompTIA. Please don't hesitate to reach out to me with any questions or concerns you may have about me or my qualifications. Regardless of the outcome, it was a pleasure speaking with you, and I hope to have the opportunity to work with you in the future.

Regards,
Alex

Email Classification Menu

Classification
Legitimate

Resolution
○ Report email to Information Security
● Perform no additional actions
○ Unsubscribe
○ Open attachment

A screenshot of a computer
Description automatically generated

NEW QUESTION 47
Which of the following should be documented to ensure that the change management plan is followed?

A. Scope of the change
B. Purpose of the change
C. Change rollback plan
D. Change risk analysis

Answer: A

Explanation:
The scope of the change is one of the elements that should be documented to ensure that the change management plan is followed. The scope of the change defines the boundaries and limitations of the change, such as what is included and excluded, what are the deliverables and outcomes, what are the assumptions and constraints, and what are the dependencies and risks. The scope of the change helps to clarify the expectations and objectives of the change, as well as to prevent scope creep or deviation from the original plan. The scope of the change also helps to measure the progress and success of the change, as well as to communicate the change to the stakeholders and the team

NEW QUESTION 48
A hard drive that previously contained PI I needs to be repurposed for a public access workstation. Which of the following data destruction methods should a technician use to ensure data is completely removed from the hard drive?

A. Shredding
B. Degaussing
C. Low-level formatting
D. Recycling

Answer: A

Explanation:
Shredding is a data destruction method that physically destroys the hard drive by cutting it into small pieces using a machine. Shredding ensures that data is completely removed from the hard drive and cannot be recovered by any means. Shredding is suitable for hard drives that contain PII (personally identifiable information), which is any information that can be used to identify, contact, or locate an individual. Degaussing, low-level formatting, and recycling are not data destruction methods that can guarantee complete data removal from a hard drive.

NEW QUESTION 49
Upon downloading a new ISO, an administrator is presented with the following string: 59d15a16ce90cBcc97fa7c211b767aB
Which of the following BEST describes the purpose of this string?

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

Answer: C

Explanation:
Hash verification is a process that verifies the integrity of a file by comparing the hash value of the downloaded file to the hash value provided by the source1

NEW QUESTION 54
A technician is troubleshooting a customer's PC and receives a phone call. The technician does not take the call and sets the phone to silent. Which of the following BEST describes the technician's actions?

A. Avoid distractions
B. Deal appropriately with customer's confidential material
C. Adhere to user privacy policy
D. Set and meet timelines

Answer: A

Explanation:
The technician has taken the appropriate action by not taking the call and setting the phone to silent in order to avoid any distractions and remain focused on the task at hand. This is a good example of how to maintain focus and productivity when working on a customer's PC, and will help to ensure that the job is completed in a timely and efficient manner.

NEW QUESTION 55
A user reports an issue when connecting a mobile device to Bluetooth. The user states the mobile device's Bluetooth is turned on. Which of the following steps should the technician take NEXT to resolve the issue?

A. Restart the mobile device.
B. Turn on airplane mode.
C. Check that the accessory is ready to pair.
D. Clear all devices from the phone's Bluetooth settings.

Answer: C

Explanation:
The first step in troubleshooting a Bluetooth connection issue is to check that the accessory is ready to pair with the mobile device. Some accessories may have a button or a switch that needs to be pressed or turned on to initiate pairing mode. If the accessory is not ready to pair, the mobile device will not be able to detect it.
Reference: CompTIA A+ Core 2 Exam Objectives, Section 2.4

NEW QUESTION 58
A company is experiencing a ODDS attack. Several internal workstations are the source of the traffic Which of the following types of infections are the workstations most likely experiencing? (Select two)

A. Zombies
B. Keylogger
C. Adware
D. Botnet
E. Ransomvvare
F. Spyware

Answer: AD

Explanation:
The correct answers are A and D. Zombies and botnets are types of infections that allow malicious actors to remotely control infected computers and use them to launch distributed denial-of-service (DDoS) attacks against a target. A DDoS attack is a type of cyberattack that aims to overwhelm a server or a network with a large volume of traffic from multiple sources, causing it to slow down or crash.
A keylogger is a type of malware that records the keystrokes of a user and sends them to a remote server, often for the purpose of stealing passwords, credit card numbers, or other sensitive information.
Adware is a type of software that displays unwanted advertisements on a user’s computer, often in the form of pop-ups, banners, or redirects. Adware can also collect user data and compromise the security and performance of the system.
Ransomware is a type of malware that encrypts the files or locks the screen of a user’s computer and demands a ransom for their restoration. Ransomware can also threaten to delete or expose the user’s data if the ransom is not paid.
Spyware is a type of software that covertly monitors and collects information about a user’s online activities, such as browsing history, search queries, or personal data. Spyware can also alter the settings or functionality of the user’s system without their consent.

NEW QUESTION 61
A technician downloaded software from the Internet that required the technician to scroll through a text box and at the end of the text box, click a button labeled Accept Which of the following agreements IS MOST likely in use?

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 65
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 technician is hardening a company file server and needs to prevent unauthorized LAN devices from accessing stored files. Which of the following should the technician use?

A. Software firewall
B. Password complexity
C. Antivirus application
D. Anti-malware scans

Answer: A

Explanation:
A software firewall is a program that monitors and controls the incoming and outgoing network traffic on a computer or a server. A software firewall can help prevent unauthorized LAN devices from accessing stored files on a company file server by applying rules and policies that filter the network packets based on their source, destination,
protocol, port, or content. A software firewall can also block or allow specific applications or services from communicating with the network, and alert the administrator of any
suspicious or malicious activity12.
A software firewall is a better option than the other choices because:
? Password complexity (B) is a good practice to protect the file server from unauthorized access, but it is not sufficient by itself. Password complexity refers to the use of strong passwords that are hard to guess or crack by attackers, and that are changed frequently and securely. Password complexity can prevent brute force attacks or credential theft, but it cannot stop network attacks that exploit vulnerabilities in the file server software or hardware, or that bypass the authentication process34.
? Antivirus application © and anti-malware scans (D) are important tools to protect
the file server from viruses and malware that can infect, damage, or encrypt the stored files. However, they are not effective in preventing unauthorized LAN devices from accessing the files in the first place. Antivirus and anti-malware tools can only detect and remove known threats, and they may not be able to stop zero- day attacks or advanced persistent threats that can evade or disable
them. Moreover, antivirus and anti-malware tools cannot control the network traffic or the file server permissions, and they may not be compatible with all file server platforms or configurations56.
References:
1: What is a Firewall and How Does it Work? - Cisco1 2: How to Harden Your Windows Server - ServerMania2 3: Password Security: Complexity vs. Length - Norton7 4: Password Hardening: 5 Ways to Protect Your Passwords - Infosec 5: What is Antivirus Software and How Does it Work? - Kaspersky 6: What is Anti-Malware? - Malwarebytes

NEW QUESTION 70
Which of the following filesystem types does macOS use?

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

Answer: D

Explanation:
APFS stands for Apple File System and it is the default filesystem type for macOS since High Sierra (10.13) version1. APFS is optimized for flash storage and supports features such as encryption, snapshots, cloning, and space sharing1.

NEW QUESTION 75
An organization is updating the monitors on kiosk machines. While performing the upgrade, the organization would like to remove physical input devices. Which of the following utilities in the Control Panel can be used to turn on the on-screen keyboard to replace the physical input devices?

A. Devices and Printers
B. Ease of Access
C. Programs and Features
D. Device Manager

Answer: B

Explanation:
Ease of Access is a utility in the Control Panel that allows users to adjust various accessibility settings on Windows, such as the on-screen keyboard, magnifier, narrator, high contrast, etc. The on-screen keyboard can be turned on by going to Ease of Access > Keyboard and toggling the switch to On12. Alternatively, the on-screen keyboard can be opened by pressing Windows + Ctrl + O keys or by typing osk.exe in the Run dialog box3.
References: 1 Use the On-Screen Keyboard (OSK) to type(https://support.microsoft.com/en-us/windows/use-the-on-screen-keyboard-osk-to-type- ecbb5e08-5b4e-d8c8-f794-81dbf896267a)2 How to Enable or Disable the On-Screen Keyboard in Windows 10 - Lifewire(https://www.lifewire.com/enable-or-disable-on-screen-keyboard-in-windows-10-5180667)3 On-Screen Keyboard Settings, Tips and Tricks in Windows 11/10(https://www.thewindowsclub.com/windows-onscreen-keyboard).

NEW QUESTION 76
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 77
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 79
Which of the following must be maintained throughout the forensic evidence life cycle when dealing with a piece of evidence?

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

Answer: B

Explanation:
The aspect of forensic evidence life cycle that must be maintained when dealing with a piece of evidence is chain of custody. This is because chain of custody is the documentation of the movement of evidence from the time it is collected to the time it is presented in court, and it is important to maintain the integrity of the evidence

NEW QUESTION 81
The network was breached over the weekend System logs indicate that a single user's account was successfully breached after 500 attempts with a dictionary attack. Which of the following would BEST mitigate this threat?

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

Answer: B

Explanation:
Account lockout would best mitigate the threat of a dictionary attack1

NEW QUESTION 85
A technician is setting up a desktop computer in a small office. The user will need to access files on a drive shared from another desktop on the network. Which of the following configurations should the technician employ to achieve this goal?

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

Answer: A

Explanation:
The technician should configure the network as private to allow the user to access files on a drive shared from another desktop on the network1

NEW QUESTION 90
A technician is setting 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:
Windows 10

The correct answer is D. Unattended installation. An unattended installation is a way of installing Windows 10 without requiring any user input or interaction. It uses a configuration file called answer file that contains the settings and preferences for the installation, such as the product key, language, partition, and network settings. An unattended installation can be performed by using a bootable USB flash drive or DVD that contains the Windows 10 installation files and the answer file1. This is the fastest way for the technician to install Windows 10 on a newly built computer, as it automates the whole process and saves time. A factory reset is a way of restoring a computer to its original state by deleting all the data and applications and reinstalling the operating system. A factory reset can be performed by using the recovery partition or media that came with the computer, or by using the Reset this PC option in Windows 10 settings2. A factory reset is not a way of installing Windows 10 on a newly built computer, as it requires an existing operating system to be present.
A system restore is a way of undoing changes to a computer's system files and settings by using a restore point that was created earlier. A system restore can be performed by using the System Restore option in Windows 10 settings or by using the Advanced Startup Options menu3. A system restore is not a way of installing Windows 10 on a newly built computer, as it requires an existing operating system and restore points to be present.
An in-place upgrade is a way of upgrading an existing operating system to a newer version without losing any data or applications. An in-place upgrade can be performed by using the Windows 10 Media Creation Tool or by running the Setup.exe file from the Windows 10 installation media. An in-place upgrade is not a way of installing Windows 10 on a newly built computer, as it requires an existing operating system to be present.

NEW QUESTION 94
An Android user reports that when attempting to open the company's proprietary mobile application it immediately doses. The user states that the issue persists, even after rebooting the phone. The application contains critical information that cannot be lost. Which of the following steps should a systems administrator attempt FIRST?

A. Mastered
B. Not Mastered

Answer: A

Explanation:
The systems administrator should clear the application cach1e2
If clearing the application cache does not work, the systems administrator should uninstall and reinstall the application12
Resetting the phone to factory settings is not necessary at this point12
Installing an alternative application with similar functionality is not necessary at this point12

NEW QUESTION 97
Which of the following Is a package management utility for PCs that are running the Linux operating system?

A. chmod
B. yum
C. man
D. grep

Answer: B

Explanation:
yum (Yellowdog Updater Modified) is a package management utility for PCs that are running the Linux operating system. It can be used to install, update and remove software packages from repositories. chmod (change mode) is a command that changes the permissions of files and directories in Linux. man (manual) is a command that displays the documentation of other commands in Linux. grep (global regular expression print) is a command that searches for patterns in text files in Linux. Verified References: https://www.comptia.org/blog/linux-package-management https://www.comptia.org/certifications/a

NEW QUESTION 101
An architecture firm is considering upgrading its computer-aided design (CAD) software to the newest version that forces storage of backups of all CAD files on the software's cloud server. Which of the following is MOST likely to be of concern to the IT manager?

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

Answer: C

Explanation:
The IT manager is most likely to be concerned about network utilization being significantly increased due to the size of CAD files.
Backing up all CAD files to the software's cloud server can result in a large amount of data being transferred over the network, which can cause network congestion and slow down other network traffic.

NEW QUESTION 104
A help desk technician runs the following script: Inventory.py. The technician receives the following error message:
How do you want to Open this file?
Which of the following is the MOST likely reason this script is unable to run?

A. Scripts are not permitted to run.
B. The script was not built for Windows.
C. The script requires administrator privileges,
D. The runtime environment is not installed.

Answer: D

Explanation:
The error message is indicating that the script is not associated with any program on the computer that can open and run it. This means that the script requires a runtime environment, such as Python, to be installed in order for it to execute properly. Without the appropriate runtime environment, the script will not be able to run.

NEW QUESTION 108
The Chief Executive Officer at a bark recently saw a news report about a high-profile cybercrime where a remote-access tool that the bank uses for support was also used in this crime. The report stated that attackers were able to brute force passwords to access systems. Which of the following would BEST limit the bark's risk? (Select TWO)

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

Answer: AF

Explanation:
The best ways to limit the bank’s risk are to enable multifactor authentication for each support account and enforce account lockouts after five bad password attempts. Multifactor authentication adds an extra layer of security to the login process, making it more difficult for attackers to gain access to systems. Account lockouts after five bad password attempts can help to prevent brute force attacks by locking out accounts after a certain number of failed login attempts.

NEW QUESTION 111
A technician is editing the hosts file on a few PCs in order to block certain domains. Which of the following would the technician need to execute after editing the hosts file?

A. Enable promiscuous mode.
B. Clear the browser cache.
C. Add a new network adapter.
D. Reset the network adapter.

Answer: D

Explanation:
Resetting the network adapter is the best way to apply the changes made to the hosts file on a few PCs. The hosts file is a text file that maps hostnames to IP addresses and can be used to block certain domains by redirecting them to invalid or local addresses. Resetting the network adapter will clear the DNS cache and force the PC to use the new entries in the hosts file.

NEW QUESTION 112
Which of the following Linux commands would be used to install an application?

A. yum
B. grep
C. Is
D. sudo

Answer: D

Explanation:
The Linux command used to install an application is sudo. The sudo command allows users to run programs with the security privileges of another user, such as the root user. This is necessary to install applications because it requires administrative privileges1

NEW QUESTION 117
A user is trying to use proprietary software, but it crashes intermittently. The user notices that the desktop is displaying a "low memory" warning message. Upon restarting the desktop, the issue persists. Which of the following should a technician do next to troubleshoot the issue?

A. Reimage the computer.
B. Replace the system RAM.
C. Reinstall and update the failing software.
D. Decrease the page file size.

Answer: C

Explanation:
The most likely cause of the intermittent crashes is that the proprietary software is incompatible, outdated, or corrupted. Reinstalling and updating the software can fix these issues and ensure the software runs smoothly. Reimaging the computer or replacing the system RAM are too drastic and unnecessary steps. Decreasing the page file size can worsen the low memory problem and affect the performance of other applications.

NEW QUESTION 119

Which of the following file types allows a user to easily uninstall software from macOS by simply placing it in the trash bin?

A. .exe
B. .dmg
C. . app
D. . rpm
E. .pkg

Answer: C

Explanation:
app files are application bundles that contain all the necessary files and resources for a Mac app. They can be easily deleted by dragging them to the Trash or using Launchpad12. Other file types, such as .exe, .dmg, .rpm, and .pkg, are either not compatible with macOS or require additional steps to uninstall34.
References: 1 Uninstall apps on your Mac - Apple Support(https://support.apple.com/en- us/102610)2 How to Uninstall Apps on a Mac (and Make Sure Leftover Files Are
…(https://www.pcmag.com/how-to/uninstall-delete-apps-from-mac)3 How to install and uninstall software on a Mac - Laptop Mag(https://www.laptopmag.com/articles/install- unininstall-mac-software)4 How to completely uninstall an app on a Mac and delete all junk files(https://www.xda-developers.com/how-to-uninstall-app-mac/).

NEW QUESTION 122
Which of the following is a consequence of end-of-lite operating systems?

A. Operating systems void the hardware warranty.
B. Operating systems cease to function.
C. Operating systems no longer receive updates.
D. Operating systems are unable to migrate data to the new operating system.

Answer: C

Explanation:
End-of-life operating systems are those which have reached the end of their life cycle and are no longer supported by the software developer. This means that the operating system will no longer receive updates, security patches, or other new features. This can leave users vulnerable to security threats, as the system will no longer be protected against the latest threats. Additionally, this can make it difficult to migrate data to a newer operating system, as the old system is no longer supported.

NEW QUESTION 125
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 126
A user notices a small USB drive is attached to the user's computer after a new vendor visited the office. The technician notices two files named grabber.exe and output.txt. Which of the following attacks is MOST likely occurring?

A. Trojan
B. Rootkit
C. Cryptominer
D. Keylogger

Answer: D

Explanation:

A keylogger is a type of malware that records the keystrokes of a user and sends them to a remote attacker1. The attacker can use the captured information to steal passwords, credit card numbers, or other sensitive data. A keylogger can be installed on a computer by attaching a small USB drive that contains a malicious executable file, such as grabber.exe2. The output.txt file may contain the recorded keystrokes. The user should remove the USB drive and scan the computer for malware.
References: 2: What is grabber.exe? (https://www.freefixer.com/library/file/grabber.exe- 55857/) 1: What is a keylogger? (https://www.kaspersky.com/resource-center/definitions/keylogger)

NEW QUESTION 127
A user's corporate laptop with proprietary work Information was stolen from a coffee shop. The user togged 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 132
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 137
A technician is replacing the processor in a desktop computer prior to opening the computer, the technician wants to ensure the internal components are protected. Which of the following safety procedures would BEST protect the components in the PC? (Select TWO).

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

Answer: AC

Explanation:
The two safety procedures that would best protect the components in the PC are:
? Utilizing an ESD strap
? Placing the PSU in an antistatic bag

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

NEW QUESTION 140
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 141

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 capabilities12

NEW QUESTION 142
A user is unable to access a web-based application. A technician verifies the computer cannot access any web pages at all. The computer obtains an IP address from the DHCP server. Then, the technician verifies the user can ping localhost. the gateway, and known IP addresses on the interne! and receive a response. Which of the following Is the MOST likely reason tor the Issue?

A. A firewall is blocking the application.
B. The wrong VLAN was assigned.
C. The incorrect DNS address was assigned.
D. The browser cache needs to be cleared

Answer: C

Explanation:
DNS (domain name system) is a protocol that translates domain names to IP addresses. If the computer has an incorrect DNS address assigned, it will not be able to

resolve the domain names of web-based applications and access them. A firewall, a VLAN (virtual local area network) and a browser cache are not the most likely reasons for the issue, since the computer can ping known IP addresses on the internet and receive a response. Verified References: https://www.comptia.org/blog/what-is-dns https://www.comptia.org/certifications/a

NEW QUESTION 143
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 147

Which of the following is the best reason for sandbox testing in change management?

A. To evaluate the change before deployment
B. To obtain end-user acceptance
C. To determine the affected systems
D. To select a change owner

Answer: A

Explanation:
Sandbox testing is a method of testing changes in a simulated environment that mimics the real one, without affecting the actual production system. Sandbox testing is useful for change management because it allows the testers to evaluate the change before deployment, and ensure that it works as intended, does not cause any errors or conflicts, and meets the requirements and expectations of the stakeholders. Sandbox testing also helps to protect the investment in the existing system, as it reduces the risk of introducing bugs or breaking functionality that could harm the customer experience or the business operations. Sandbox testing also gives the testers more control over the customer experience, as they can experiment with different scenarios and configurations, and optimize the change for the best possible outcome.
References:
1: Change Management and Sandbox - Quickbase1 2: Embracing change: Build, test, and adapt in a sandbox environment - Zendesk3

NEW QUESTION 148
A help desk technician is troubleshooting a workstation in a SOHO environment that is running above normal system baselines. The technician discovers an unknown executable with a random string name running on the system. The technician terminates the process, and the system returns to normal operation. The technician thinks the issue was an infected file, but the antivirus is not detecting a threat. The technician is concerned other machines may be infected with this unknown virus. Which of the following is the MOST effective way to check other machines on the network for this unknown threat?

A. Run a startup script that removes files by name.
B. Provide a sample to the antivirus vendor.
C. Manually check each machine.
D. Monitor outbound network traffic.

Answer: C

Explanation:
The most effective way to check other machines on the network for this unknown threat is to manually check each machine. This can help to identify any other machines that may be infected with the unknown virus and allow them to be cleaned.

NEW QUESTION 149
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:
Removing the applications from startup can improve the boot time of a PC by reducing the number of programs that load automatically when the PC starts. Some applications may add themselves to the startup list without the user's knowledge or consent, which can slow down the PC's performance. Running the Disk Cleanup utility can also improve the boot time of a PC by deleting unnecessary or temporary files that take up disk space and affect the PC's speed. Disk Cleanup can also remove old system files that may cause conflicts or errors during booting. Installing additional RAM, installing a faster SSD, defragmenting the hard drive, and ending the processes in the Task Manager are not operations that would be best to do to resolve the issue of slow boot time at a minimal expense, as they may require purchasing new hardware or software, or may have negative impacts on other aspects of the PC's performance.

NEW QUESTION 154
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 meth1od
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 data1

NEW QUESTION 156
A customer calls desktop support and begins yelling at a technician. The customer claims to have submitted a support ticket two hours ago and complains that the issue still has not been resolved. Which of the following describes how the technician should respond?

A. Place the customer on hold until the customer calms down.
B. Disconnect the call to avoid a confrontation.
C. Wait until the customer is done speaking and offer assistance.
D. Escalate the issue to a supervisor.

Answer: C

Explanation:
The best way to deal with an angry customer who is yelling at a technician is to wait until the customer is done speaking and offer assistance. This shows respect, empathy, and professionalism, and allows the technician to understand the customer’s problem and find a solution. According to the CompTIA A+ Core 2 (220-1102) Certification Study Guide1, some of the steps to handle angry customers are:
? Stay calm and do not take it personally.
? Listen actively and acknowledge the customer’s feelings.
? Apologize sincerely and offer to help.
? Restate the customer’s issue and ask for clarification if needed.
? Explain the possible causes and solutions for the problem.
? Provide clear and realistic expectations for the resolution.

? Follow up with the customer until the issue is resolved.

The other options are not appropriate ways to deal with angry customers, as they may worsen the situation or damage the customer relationship. Placing the customer on hold may make them feel ignored or dismissed. Disconnecting the call may make them feel disrespected or abandoned. Escalating the issue to a supervisor may make them feel frustrated or powerless, unless the technician cannot resolve the issue or the customer requests to speak to a supervisor.

References:
? CompTIA A+ Certification Exam Core 2 Objectives2
? CompTIA A+ Core 2 (220-1102) Certification Study Guide1
? How To Deal with Angry Customers (With Examples and Tips)3
? 17 ways to deal with angry customers: Templates and examples4
? Six Ways to Handle Angry Customers5

NEW QUESTION 158

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:

A change request form is a document that describes the proposed change, the reason for the change, the impact of the change, and the approval process for the change. A change request form is required for any planned changes to the network, such as adding a new network printer, to ensure that the change is authorized, documented, and communicated to all stakeholders. Submitting a change request form should happen immediately before network use is authorized, as stated in the Official CompTIA A+ Core 2 Study Guide. The other options are either too late (documenting the date and time of the change) or too early (determining the risk level of the change and requesting an unused IP address) in the change management process.

NEW QUESTION 163

The audio on a user's mobile device is inconsistent when the user uses wireless headphones and moves around. Which of the following should a technician perform to troubleshoot the issue?

A. Verify the Wi-Fi connection status.
B. Enable the NFC setting on the device.
C. Bring the device within Bluetooth range.
D. Turn on device tethering.

Answer: C

Explanation:

Bringing the device within Bluetooth range is the best way to troubleshoot the issue of inconsistent audio when using wireless headphones and moving around. Bluetooth is a wireless technology that allows devices to communicate over short distances, typically up to 10 meters or 33 feet. If the device is too far from the headphones, the Bluetooth signal may be weak or interrupted, resulting in poor audio quality or loss of connection.

NEW QUESTION 164

A user attempts to install additional software and receives a UAC prompt. Which of the following is the BEST way to resolve this issue?

A. Add a user account to the local administrator's group.
B. Configure Windows Defender Firewall to allow access to all networks.
C. Create a Microsoft account.
D. Disable the guest account.

Answer: A

Explanation:
A user account that belongs to the local administrator’s group has the permission to install software on a Windows machine. If a user receives a UAC (user account control) prompt when trying to install software, it means the user does not have enough privileges and needs to enter an administrator’s password or switch to an administrator’s account. Adding the user account to the local administrator’s group can resolve this issue. Configuring Windows Defender Firewall, creating a Microsoft account and disabling the guest account are not related to this issue. Verified References: https://www.comptia.org/blog/user-account-control https://www.comptia.org/certifications/a

NEW QUESTION 165
Which of the following is the most likely to use NTFS as the native filesystem?

A. macOS
B. Linux
C. Windows
D. Android

Answer: C

Explanation:
NTFS stands for New Technology File System, which is a proprietary file system developed by Microsoft4. NTFS is the default file system for the Windows NT family of operating systems, which includes Windows 10, Windows Server 2019, and other versions5. NTFS provides features such as security, encryption, compression, journaling, and large volume support45. NTFS is not the native file system for other operating systems, such as macOS, Linux, or Android, although some of them can read or write to NTFS volumes with third-party drivers or tools

NEW QUESTION 167
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.
Restore the computer from the last known backup.
C
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 172
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 follows12:
? 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?1
? Comparison of operating systems3
? Windows 10 vs 11 Minimum System Requirements: Why Need a New One?2
? macOS Monterey - Technical Specifications
? Chrome OS - Wikipedia
? Android - Wikipedia
? Installation/SystemRequirements - Community Help Wiki

NEW QUESTION 174
A technician is trying to encrypt a single folder on a PC. Which of the following should the technician use to accomplish this task?

A. FAT32
B. exFAT
C. BitLocker
D. EFS

Answer: D

Explanation:
EFS (Encrypting File System) is a feature that allows a user to encrypt a single folder or file on a Windows PC. It uses a public key encryption system to protect the data from unauthorized access. FAT32 and exFAT are file system formats that do not support encryption. BitLocker is a feature that encrypts the entire drive, not a single folder or file. Verified References: https://www.comptia.org/blog/what-is-efs https://www.comptia.org/certifications/a

NEW QUESTION 176
A customer has a USB-only printer attached to a computer. A technician is configuring an arrangement that allows other computers on the network to use the printer. In which of the following locations on the customer's desktop should the technician make this configuration?

A. Printing Preferences/Advanced tab
B. Printer Properties/Sharing tab
C. Printer Properties/Security tab
D. Printer Properties/Ports tab

Answer: B

Explanation:
The correct answer is B. Printer Properties/Sharing tab. This is the location where the technician can enable printer sharing and assign a share name for the USB printer. This will allow other computers on the network to access the printer by using the share name or the IP address of the computer that has the printer attached1.
1: CompTIA A+ Certification Exam: Core 2 Objectives, page 15, section 1.9.

NEW QUESTION 179
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 company implemented a BYOD policy and would like to reduce data disclosure caused by malware that may infect these devices. Which of the following should the company deploy to address these concerns?

A. UAC
B. MDM
C. LDAP

D. SSO

Answer: B

Explanation:
MDM stands for mobile device management, which is a type of software solution that allows remote management and security of mobile devices. MDM can help a company reduce data disclosure caused by malware that may infect these devices by enforcing security policies, such as encryption, password protection, antivirus software, and remote wipe. MDM can also monitor and control the access of personal devices to corporate data and networks. UAC stands for user account control, which is a feature of Windows that prompts users for permission or an administrator password before making changes that affect the system. UAC may not be effective in preventing malware infection or data disclosure on personal devices. LDAP stands for lightweight directory access protocol, which is a protocol for accessing and managing information stored in a directory service, such as user names and passwords. LDAP does not directly address the issue of malware infection or data disclosure on personal devices. SSO stands for single sign-on, which is a feature that allows users to access multiple applications or services with one set of credentials. SSO may not prevent malware infection or data disclosure on personal devices, and may even increase the risk if the credentials are compromised.
https://www.nist.gov/news-events/news/2021/03/mobile-device-security-bring-your-own-device-byod-draft-sp-1800-22

NEW QUESTION 182
A remote user contacts the help desk about an email that appears to be distorted. The technician is unsure what the user means and needs to view the email to assist with troubleshooting. Which of the following should the technician use to assist the user?

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

Answer: D

Explanation:
The best tool to use to assist the user with viewing the email is RMM, which stands for remote monitoring and management. This is a software that allows the technician to remotely access, monitor, and manage the user's computer and applications. The technician can use RMM to view the user's screen, control the mouse and keyboard, and troubleshoot the email issue. The other tools are not suitable for this task. VNC is a software that allows remote desktop sharing, but it requires the user to install and configure
it on their computer, which may not be feasible or convenient. SSH is a protocol that allows secure remote access to a command-line interface, but it is not useful for viewing graphical applications such as email. VPN is a technology that creates a secure and encrypted connection over a public network, but it does not provide remote access or control of the user's computer.

NEW QUESTION 184
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 185
A technician is asked to resize a partition on the internal storage drive of a computer running macOS. Which of the followings tools should the technician use to accomplish this task?

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

Answer: B

Explanation:
The technician should use Disk Utility to resize a partition on the internal storage drive of a computer running macOS. Disk Utility is a built-in utility that allows users to manage disks, partitions, and volumes on a Mac. It can be used to resize, create, and delete partitions, as well as to format disks and volumes.

NEW QUESTION 187
A police officer often leaves a workstation for several minutes at a time. Which of the following is the BEST way the officer can secure the workstation quickly when walking away?

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

Answer: A

Explanation:
The BEST way to secure the workstation quickly when walking away is to use a key combination to lock the computer when leaving1

NEW QUESTION 189
A network administrator is deploying a client certificate to be used for Wi-Fi access for all devices in an organization. The certificate will be used in conjunction with the user's existing username and password. Which of the following BEST describes the security benefits realized after this deployment?

A. Multifactor authentication will be forced for Wi-Fi.
B. All Wi-Fi traffic will be encrypted in transit.
C. Eavesdropping attempts will be prevented.
D. Rogue access points will not connect.

Answer: B

Explanation:
The security benefits realized after deploying a client certificate to be used for Wi-Fi access for all devices in an organization are that all Wi-Fi traffic will be encrypted in transit. This means that any data transmitted over the Wi-Fi network will be protected from eavesdropping attempts. Rogue access points will not connect to the network because they will not have the client certificate. However, multifactor authentication will not be forced for Wi-Fi because the client certificate is being used in conjunction with the user's existing username and password12

NEW QUESTION 190
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 194
A technician successfully removed malicious software from an infected computer after running updates and scheduled scans to mitigate future risks. Which of the following should the technician do next?

A. Educate the end user on best practices for security.
B. Quarantine the host in the antivirus system.
C. Investigate how the system was infected with malware.
D. Create a system restore point.

Answer: A

Explanation:
Educating the end user on best practices for security is the next step that the technician should take after successfully removing malicious software from an infected computer. Educating the end user on best practices for security is an important part of preventing future infections and mitigating risks. The technician should explain to the end user how to avoid common sources of malware, such as phishing emails, malicious websites, or removable media. The technician should also advise the end user to use strong passwords, update software regularly, enable antivirus and firewall protection, and backup data frequently. Educating the end user on best practices for security can help the end user become more aware and responsible for their own security and reduce the likelihood of recurrence of malware infections. Quarantining the host in the antivirus system, investigating how the system was infected with malware, and creating a system restore point are not the next steps that the technician should take after successfully removing malicious software from an infected computer. Quarantining the host in the antivirus system is a step that the technician should take before removing malicious software from an infected computer. Quarantining the host in the antivirus system means isolating the infected computer from the network or other devices to prevent the spread of malware. Investigating how the system was infected with malware is a step that the technician should take during or after removing malicious software from an infected computer. Investigating how the system was infected with malware means identifying the source, type, and impact of malware on the system and documenting the findings and actions taken. Creating a system restore point is a step that the technician should take before removing malicious software from an infected computer. Creating a system restore point means saving a snapshot of the system's configuration and settings at a certain point in time, which can be used to restore the system in case of failure or corruption. References:
? Official CompTIA learning resources CompTIA A+ Core 1 and Core 2, page 15
? CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide, page 458

NEW QUESTION 196
A Windows user reported that a pop-up indicated a security issue. During inspection, an antivirus system identified malware from a recent download, but it was unable to remove the malware. Which of the following actions would be BEST to remove the malware while also preserving the user's files?

A. Run the virus scanner in an administrative mode.
B. Reinstall the operating system.
C. Reboot the system in safe mode and rescan.
D. Manually delete the infected files.

Answer: C

Explanation:

Rebooting the system in safe mode will limit the number of programs and processes running, allowing the antivirus system to more effectively identify and remove the malware. Rescanning the system will allow the antivirus system to identify and remove the malware while preserving the user's files.

NEW QUESTION 201
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 204
A user reports a computer is running slow. Which of the following tools will help a technician identify the issue?

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

Answer: D

Explanation:
Resource Monitor is a Windows utility that can be used to monitor and analyze the system resources and processes running on a computer. It can be used to identify and troubleshoot any issues that might be causing the computer to run slowly, such as CPU usage, memory usage, disk I/O, and network usage.

NEW QUESTION 205
A technician receives a help desk ticket from a user who is unable to update a phone. The technician investigates the issue and notices the following error message: Insufficient storage space
While analyzing the phone, the technician does not discover any third-party' applications or photos. Which of the following is the best way to resolve the issue?

A. Exchange the device for a newer one.
B. Upgrade the onboard storage
C. Allocate more space by removing factory applications
D. Move factory applications to external memory.

Answer: D

Explanation:
The best way to resolve the issue is to move factory applications to external memory. This will free up some space on the phone's internal storage, which is required for updating the phone. To do this, you can follow these steps1:
? Insert a microSD card into your phone if you don't have one already.
? Go to Settings > Apps and tap on the app you want to move.
? Tap on Storage and then on Change.
? Select the SD card option and tap on Move.
You may need to repeat this process for multiple apps until you have enough space to update your phone. Alternatively, you can also clear the cache and data of some apps, or uninstall the apps that you don't use frequently. You can find more information on how to fix insufficient storage error on your phone in these articles234. I hope this helps.

NEW QUESTION 208
A user's Windows computer seems to work well at the beginning of the day. However, its performance degrades throughout the day, and the system freezes when several applications are open. Which of the following should a technician do to resolve the issue? (Select two).

A. Install the latest GPU drivers.
B. Reinstall the OS.
C. Increase the RAM.
D. Increase the hard drive space.
E. Uninstall unnecessary software.
F. Disable scheduled tasks.

Answer: CE

Explanation:
The most likely causes of the user's Windows computer performance degradation and freezing are insufficient RAM and excessive software running in the background. Therefore, the technician should do the following to resolve the issue:
? Increase the RAM. RAM is the memory that the computer uses to store and run applications and processes. If the RAM is not enough to handle the workload, the computer will use the hard drive as a virtual memory, which is much slower and can cause performance issues. Increasing the RAM will allow the computer to run more applications and processes smoothly and avoid freezing. The technician should check the system requirements of the applications that the user needs to run, and install additional RAM modules that are compatible with the motherboard and the existing RAM. The technician should also make sure that the system is managing the page file size automatically, or adjust it manually to optimize the virtual memory usage12.
? Uninstall unnecessary software. Software that the user does not need or use can take up valuable disk space and system resources, and can interfere with

performance of other applications. Some software may also run in the background or start automatically when the computer boots the up, which can slow down the system and cause freezing. The technician should help the user to identify and uninstall unnecessary software from the control panel or the settings app, and disable unnecessary startup programs from the task manager or the system configuration tool. The technician should also check for and remove viruses and malware that may affect the system performance134.
References:
1: Tips to improve PC performance in Windows - Microsoft Support1 2: How to Upgrade or Install RAM on Your Windows PC - Lifewire5 3: How to Uninstall Programs on Windows 10
- PCMag6 4: How to Fix a Windows Computer that Hangs or Freezes - wikiHow

NEW QUESTION 209
A user needs assistance changing the desktop wallpaper on a Windows 10 computer. Which of the following methods will enable the user to change the wallpaper using a Windows 10 Settings tool?

A. Open Settings, select Accounts, select Your info, click Browse, and then locate and open the image the user wants to use as the wallpaper.
B. Open Settings, select Personalization, click Browse, and then locate and open the image the user wants to use as the wallpaper.
C. Open Settings, select System, select Display, click Browse, and then locate and open the image the user wants to use as the wallpaper.
D. Open Settings, select Apps, select Apps & features, click Browse, and then locate and open the image the user wants to use as the wallpaper.

Answer: B

Explanation:
The user can change the wallpaper using a Windows 10 Settings tool by following these steps12:
? Open Settings by pressing the Windows key and typing Settings, or by clicking the gear icon in the Start menu.
? Select Personalization from the left navigation menu.
? On the right side of the window, click Background.
? In the Background settings, click the drop-down menu and select Picture as the background type.
? Click Browse and then locate and open the image the user wants to use as the wallpaper.
The other options are incorrect because they do not lead to the Background settings or they do not allow the user to browse for an image. Accounts, System, and Apps are not related to personalization settings. Your info, Display, and Apps & features are not related to wallpaper settings.
References: 1: https://support.microsoft.com/en-us/windows/change-your-desktop-background-image-175618be-4cf1-c159-2785-ec2238b433a8 2: https://www.computerhope.com/issues/ch000592.htm

NEW QUESTION 214
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 devices1. BitLocker helps mitigate unauthorized data access by enhancing file and system protections, rendering data inaccessible when BitLocker-protected devices are decommissioned or recycled1. 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 Learn1
? The Official CompTIA A+ Core 2 Study Guide2, page 315.

NEW QUESTION 219
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. Runa 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 2 220-1002 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 221
While staying at a hotel, a user attempts to connect to the hotel Wi-Fi but notices that multiple SSIDs have very similar names. Which of the following social-engineering attacks is being attempted?

A. Evil twin
B. Impersonation
C. Insider threat
D. Whaling

Answer: A

Explanation:
An evil twin is a type of social-engineering attack that involves setting up a rogue wireless access point that mimics a legitimate one. The attacker can then intercept
or modify the traffic of the users who connect to the fake SSID. The attacker may also use phishing or malware to steal credentials or personal information from the users

NEW QUESTION 223
A call center technician receives a call from a user asking how to update Windows Which of the following describes what the technician should do?

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

Answer: C

Explanation:
The technician should guide the user to update Windows through the built-in "Check for Updates" feature. This can be done by having the user click in the Search field, type "Check for Updates", and then press the Enter key. This will bring up the Windows Update function, which will search for any available updates and give the user the option to install them.

NEW QUESTION 228
Which of the following combinations meets the requirements for mobile device multifactor authentication?

A. Password and PIN
B. Password and swipe
C. Fingerprint and password
D. Swipe and PIN

Answer: C

Explanation:
Mobile device multifactor authentication (MFA) is a method of verifying a user's identity by requiring two or more factors, such as something the user knows (e.g., password, PIN, security question), something the user has (e.g., smartphone, OTP app, security key), or something the user is (e.g., fingerprint, face, iris)12. The combination of fingerprint and password meets the requirements for mobile device MFA because it uses two different factors: something the user is (fingerprint) and something the user knows (password). The other combinations do not meet the requirements because they use only one factor: something the user knows (password or PIN) or something the user does (swipe). References1: Set up the Microsoft Authenticator app as your verification method2: What is Multi-Factor Authentication (MFA)? | OneLogin

NEW QUESTION 232
A suite of security applications was installed a few days ago on a user's home computer.
The user reports that the computer has been running slowly since the installation. The user notices the hard drive activity light is constantly solid. Which of the following should be checked FIRST?

A. Services in Control Panel to check for overutilization
B. Performance Monitor to check for resource utilization
C. System File Checker to check for modified Windows files
D. Event Viewer to identify errors

Answer: C

Explanation:
System File Checker to check for modified Windows files. System File Checker (SFC) is a Windows utility that can be used to scan for and restore corrupt Windows system files. SFC can be used to detect and fix any modified or corrupted system files on a computer, and thus should be checked first when a user reports that their computer has been running slowly since the installation of security applications [1][2]. By checking SFC, any modified or corrupted system files can be identified and fixed, potentially improving the overall performance of the computer.

NEW QUESTION 236
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 238
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 241
Malware is installed on a device after a user clicks on a link in a suspicious email. Which of the following is the best way to remove the malware?

A. Run System Restore.
B. Place in recovery mode.
C. Schedule a scan.
D. Restart the PC.

Answer: B

Explanation:
Recovery mode is a special boot option that allows the user to access advanced tools and features to troubleshoot and remove malware from the device. Recovery mode can also restore the system to a previous state or reset the device to factory settings. Running System Restore, scheduling a scan, or restarting the PC may not be effective in removing the malware, as it may still be active or hidden in the system files.

NEW QUESTION 242
In an organization with a standardized set of installed software, a developer submits a request to have new software installed. The company does not currently have a license for this software, but the developer already downloaded the installation file and is requesting that the technician install it. The developer states that the management team approved the business use of this software. Which of the following is the best action for the technician to take?

A. Contact the software vendor to obtain the license for the user, and assist the user with installation once the license is purchased.
B. Run a scan on the downloaded installation file to confirm that it is free of malicious software, install the software, and document the software installation process.
C. Indicate to the developer that formal approval is needed; then, the IT team should investigate the software and the impact it will have on the organization before installing the software.
D. Install the software and run a full system scan with antivirus software to confirm that the operating system is free of malicious software.

Answer: C

Explanation:
Installing new software on an organization’s system or device can have various implications, such as compatibility, security, performance, licensing, and compliance issues. Therefore, it is important to follow the best practices for software installation, such as doing research on the software, checking the system requirements, scanning the installation file for malware, and obtaining the proper license345. The technician should not install the software without formal approval from the management team, as this could violate the organization’s policies or regulations. The technician should also not install the software without investigating the software and its impact on the organization, as this could introduce potential risks or problems to the system or device. The technician should indicate to the developer that formal approval is needed, and then work with the IT team to evaluate the software and its suitability for the organization before installing it

NEW QUESTION 244
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 245
A user's company phone was stolen. Which of the following should a technician do next?

A. Perform a low-level format.
B. Remotely wipe the device.
C. Degauss the device.
D. Provide the GPS location of the device.

Answer: B

Explanation:
Remotely wiping the device is the best option to prevent unauthorized access to the company data stored on the phone. A low-level format, degaussing, or providing the GPS location of the device are not feasible or effective actions to take in this scenario.
References: The Official CompTIA A+ Core 2 Study Guide1, page 315.

NEW QUESTION 250
A technician needs to establish a remote access session with a user who has a Windows workstation. The session must allow for simultaneous viewing of the workstation by both the user and technician. Which of the following remote access technologies should be used?

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

Answer: D

Explanation:
MSRA (Microsoft Remote Assistance) is a remote access technology that allows a technician to establish a session with a user who has a Windows workstation. The session allows for simultaneous viewing of the workstation by both the user and technician, as well as remote control and file transfer capabilities. RDP (remote desktop protocol) is another remote access technology, but it does not allow simultaneous viewing by default. VPN (virtual private network) and SSH (secure shell) are protocols that create secure tunnels between two devices over the internet, but they do not allow remote access sessions. Verified References: https://www.comptia.org/blog/what-is-msra https://www.comptia.org/certifications/a

NEW QUESTION 255
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 258
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 SSIO 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 259
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 Disable12.
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), etc34.

NEW QUESTION 263
......