 Custom View Settings

[Empty content area]

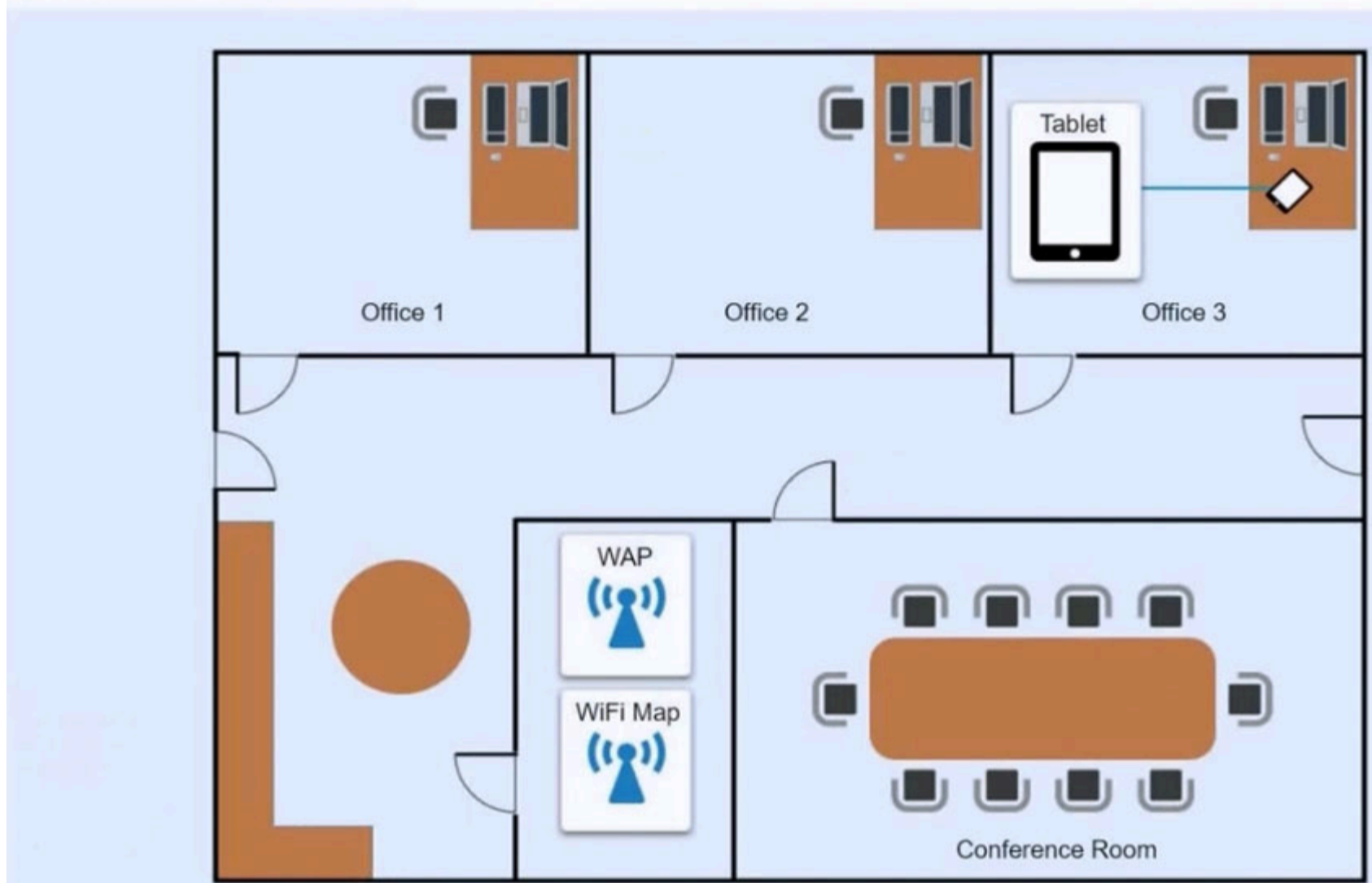
SIMULATION -

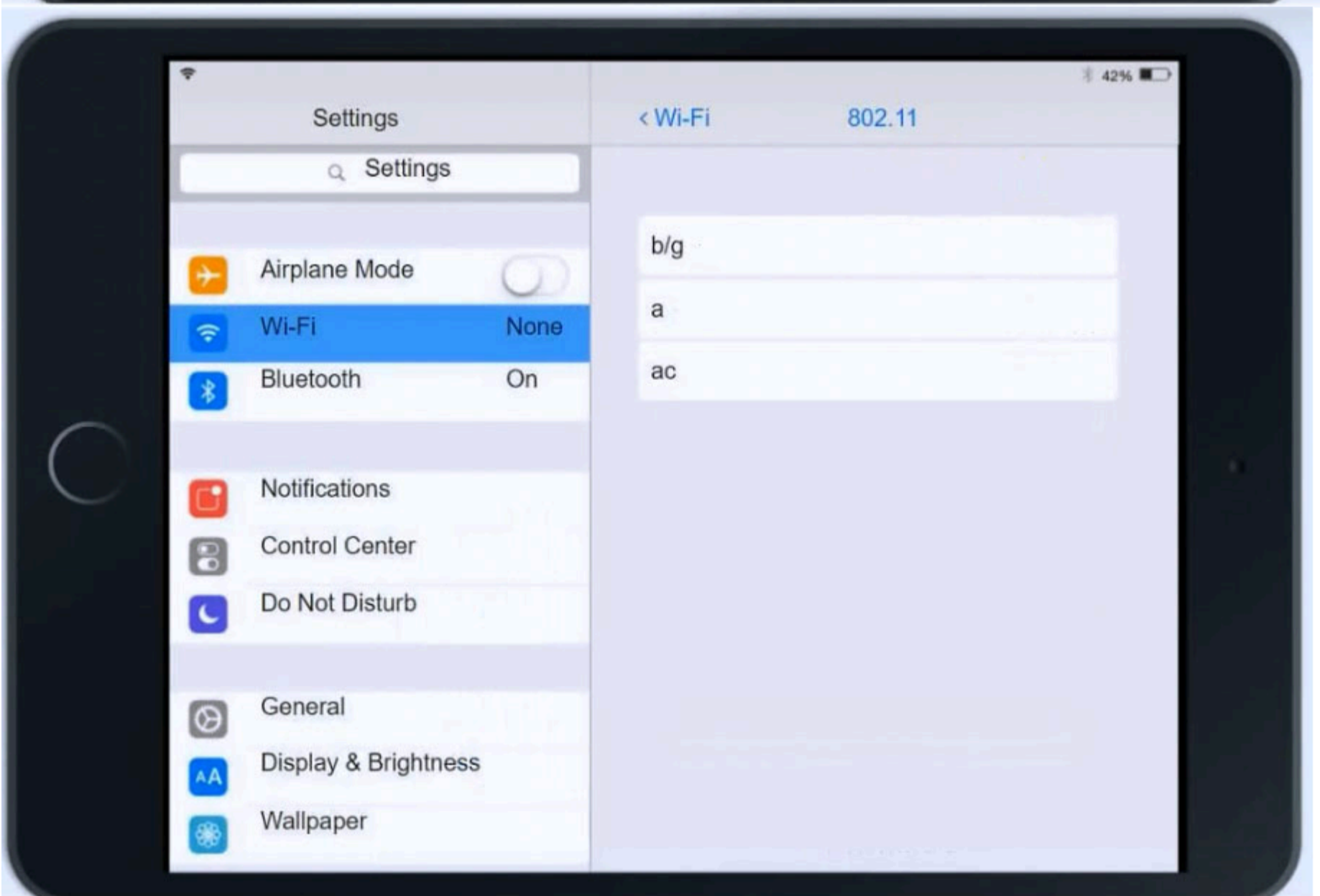
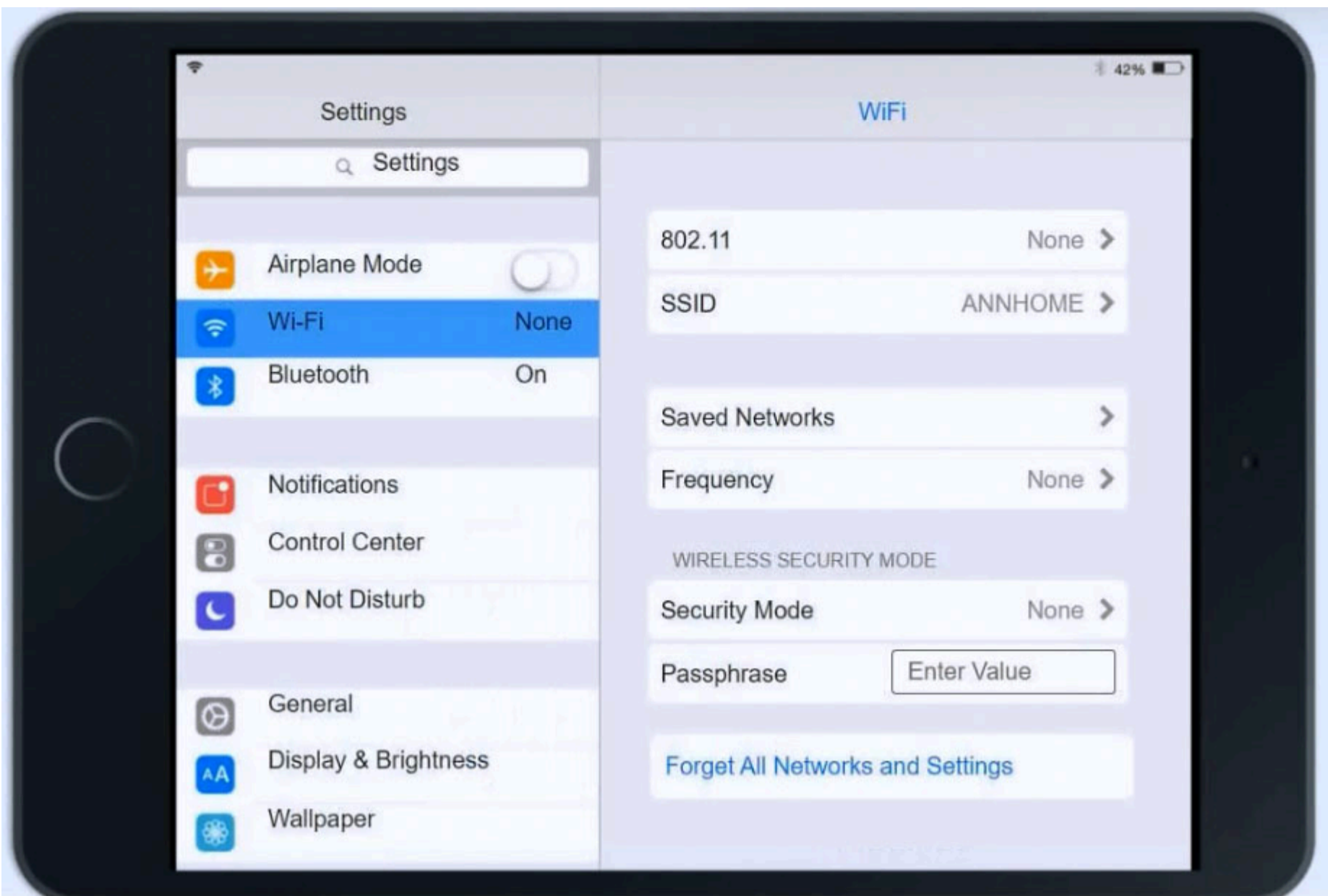
Ann, a CEO, has purchased a new consumer-class tablet for personal use, but she is unable to connect to the wireless network. Other users have reported that their personal devices are connecting without issues. She has asked you to assist with getting the device online without adjusting her home WiFi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

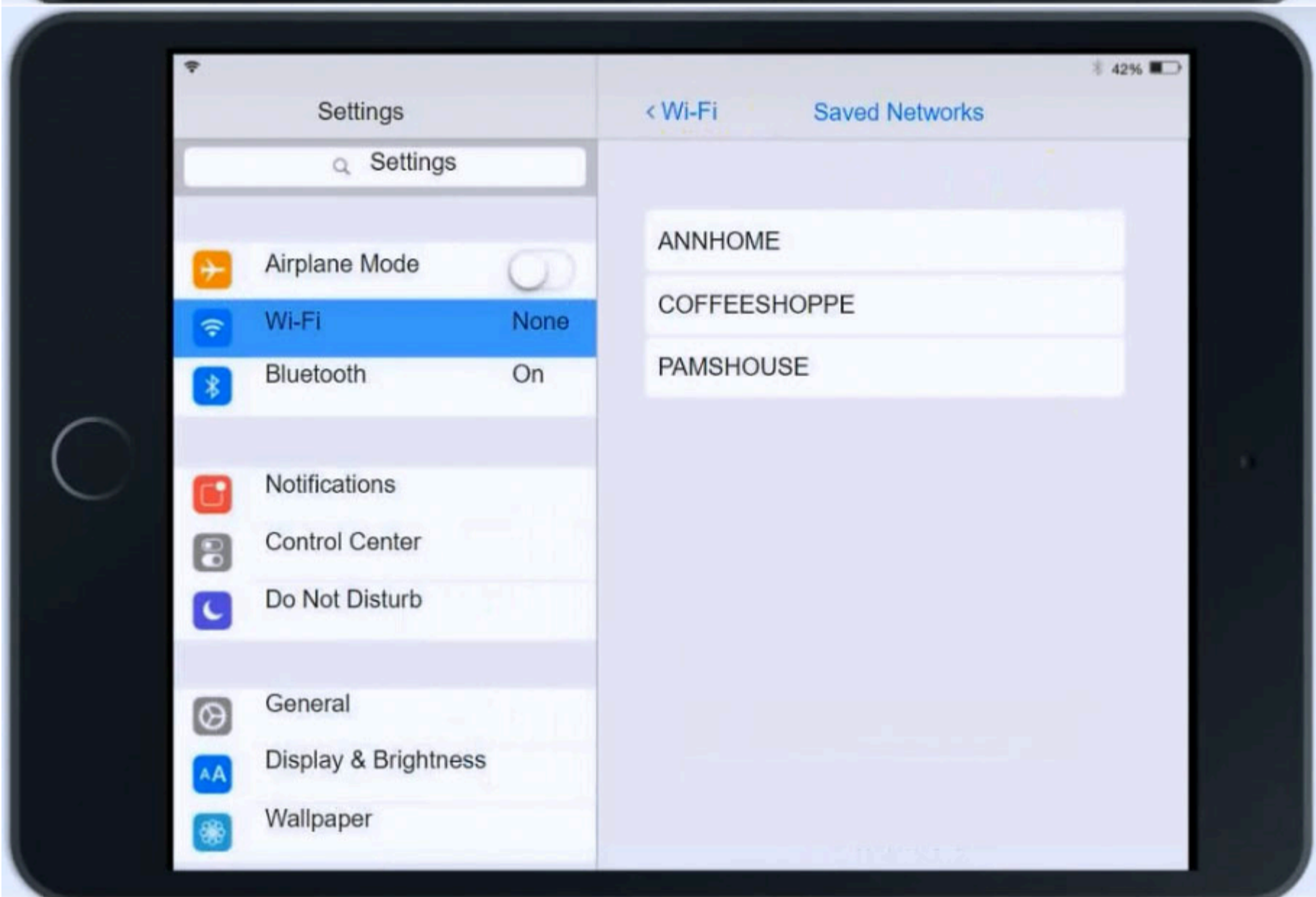
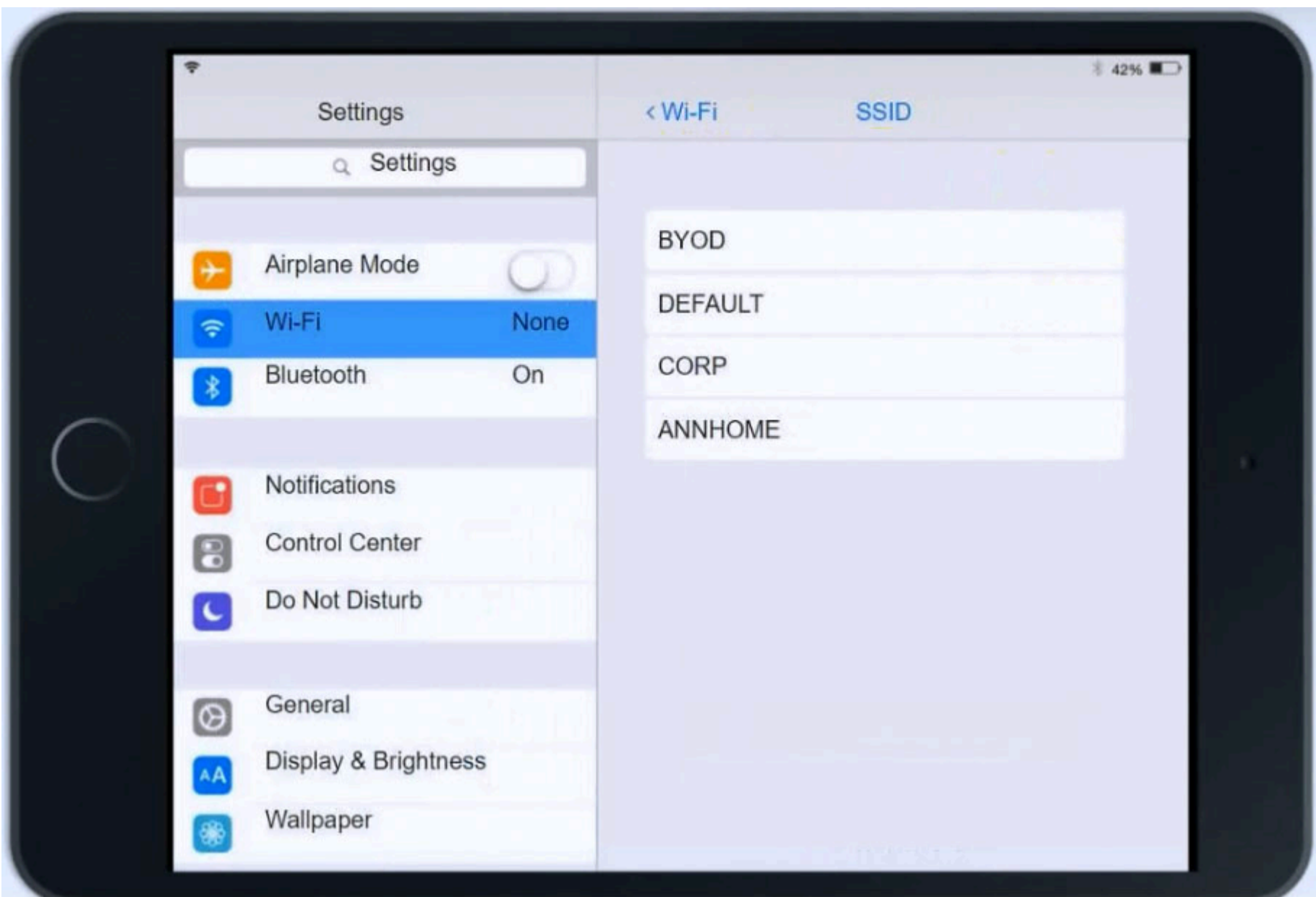
INSTRUCTIONS -

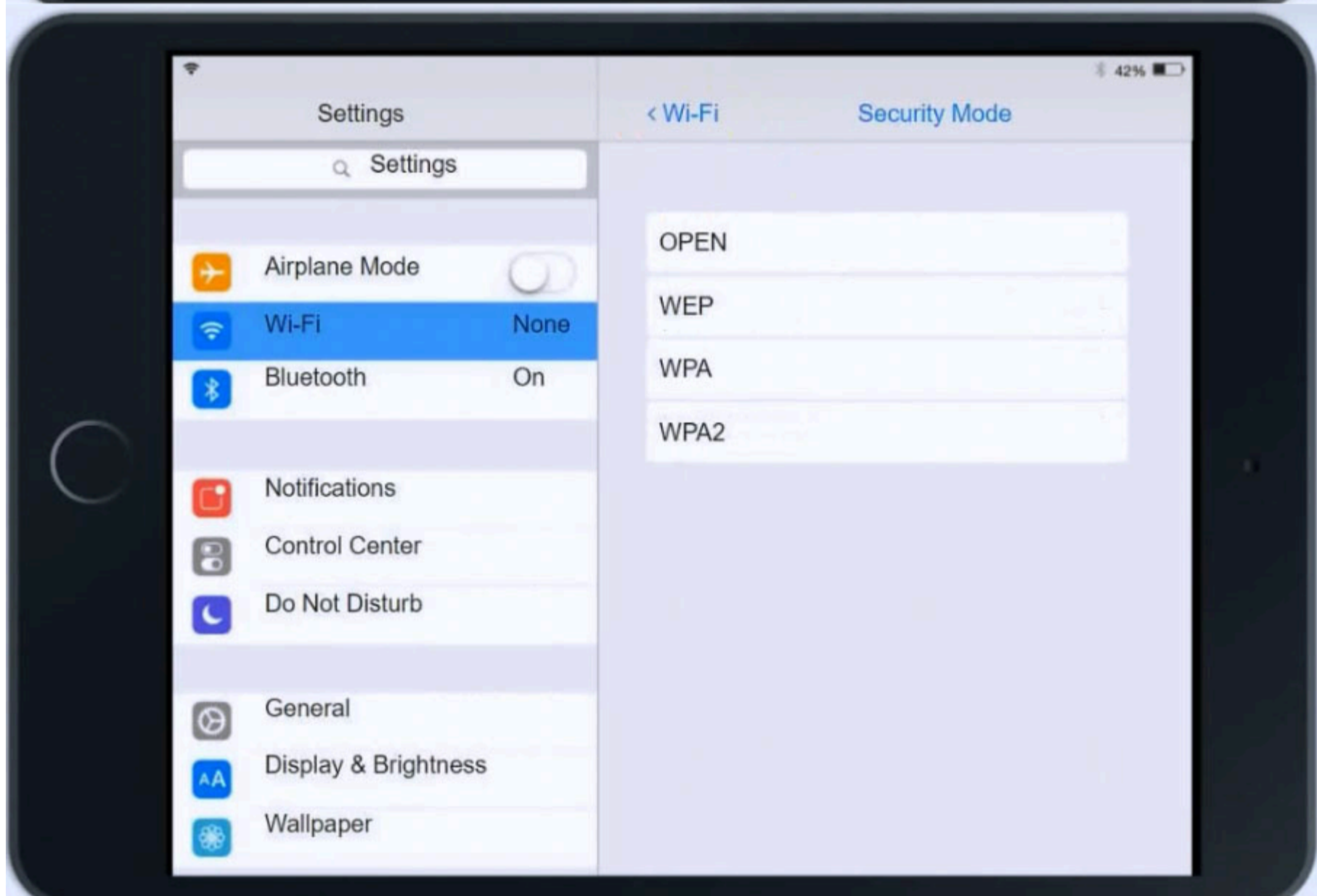
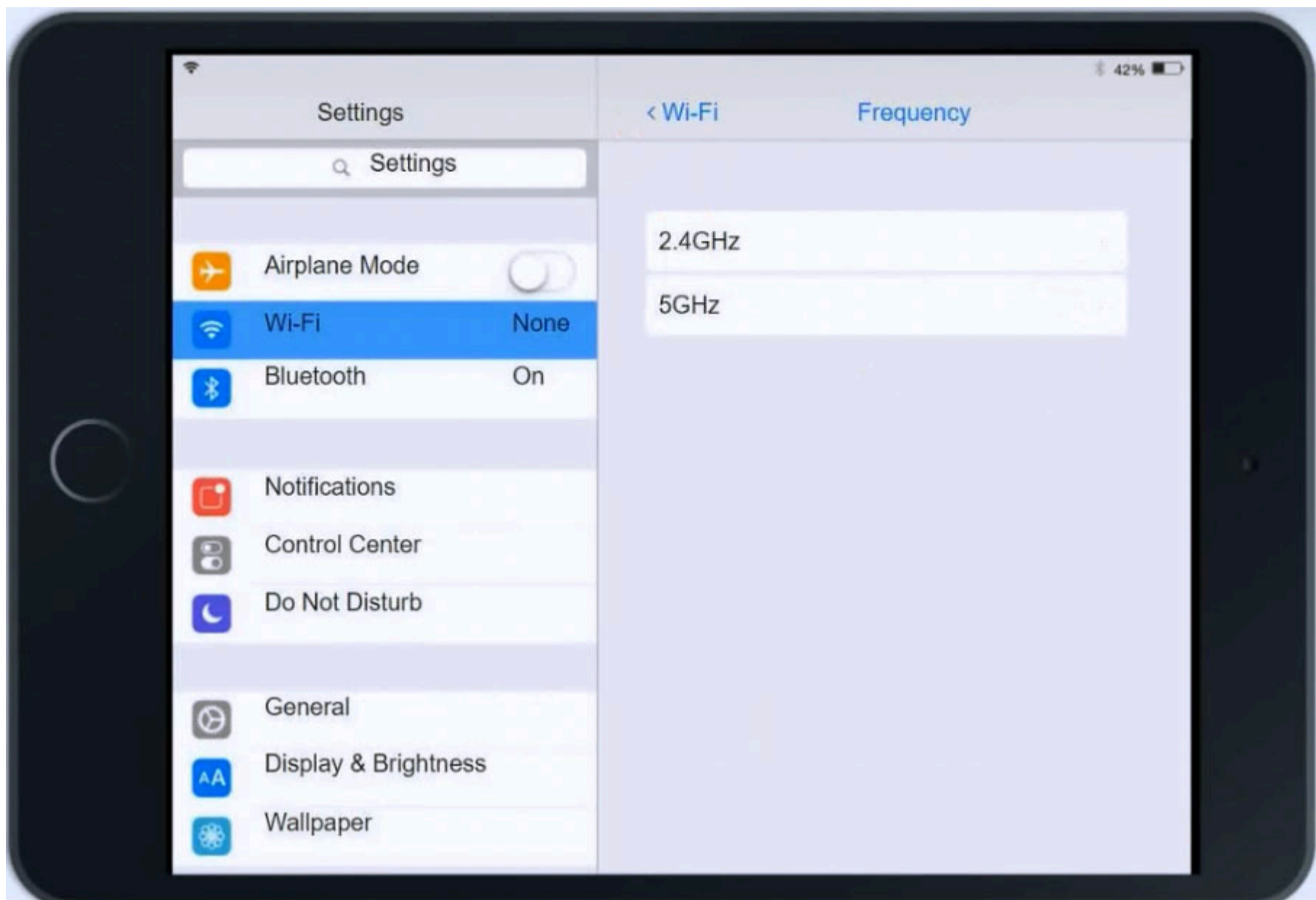
Review the network diagrams and device configurations to determine the cause of the problem and resolve any discovered issues.

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

Mobile Device Configuration







Settings



Site

Wireless Networks

Wireless Networks

Networks

Guest Control

Admins

User Groups

VOIP

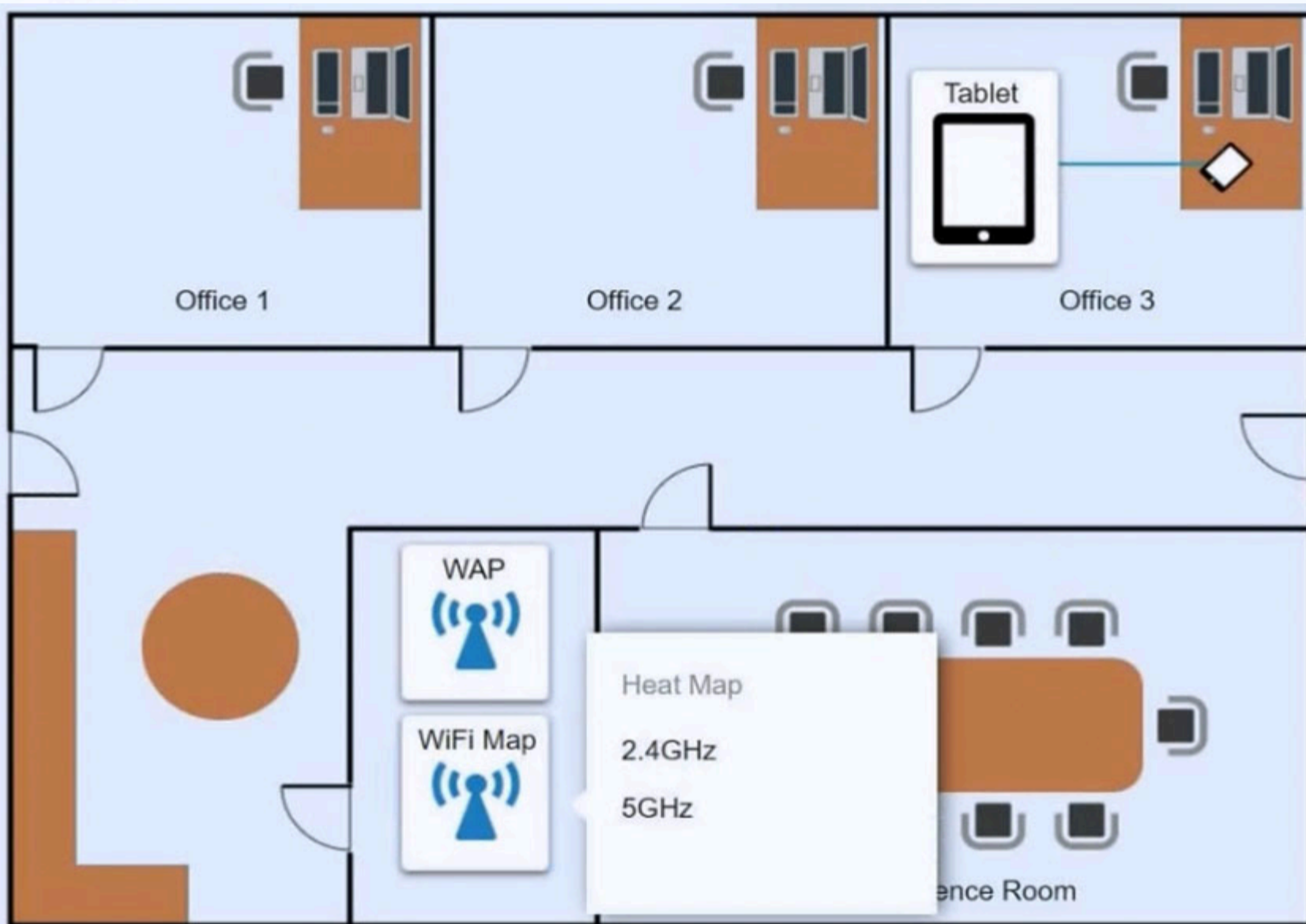
Controller

Cloud Access

Maintenance

SSID	Frequency	Security	TotallySecure!
CORP	2.4GHz/5GHz	WPA2	Corpsecure1
BYOD	2.4GHz/5GHz	WPA-PSK	TotallySecure!

Create New Wireless Network



Correct Answer: See explanation below.

Click on 802.11 and Select ac -

Click on SSID and select BYOD -

Click on Frequency and select 5GHz

At Wireless Security Mode, Click on Security Mode
Select the WPA and the password should be set to TotallySecure!

The screenshot shows a 'Settings' window with a sidebar on the left containing menu items: Site, Wireless Networks, Networks, Guest Control, Admins, User Groups, VOIP, Controller, Cloud Access, and Maintenance. The main content area is titled 'Wireless Networks' and contains a table with the following data:

SSID	Frequency	Security	TotallySecure!
CORP	2.4GHz/5GHz	WPA2	Corpsecure1
BYOD	2.4GHz/5GHz	WPA-PSK	TotallySecure!

Below the table is a button labeled 'Create New Wireless Network'.

Bogardinc Highly Voted 1 year, 8 months ago

Took 1102 today (Passed) and this was not on my exam. There were 3 practical's. One asked how to set up a SOHO with backup power. You have to select the power source for the surge protector in one column and UPS in the other column. You have to drag the following to both columns: CPU, monitor, printer/scanner, modem, and router. The other question was technical support via messenger. The user complained that her work email stopped working on her phone. I had to go through the steps for trouble shooting i.e. Were there any recent changes?, change the port channel to 993, and Educate the user. The next question asked to resolve two trouble call tickets, identify why and the command line to resolve the problem. Mind you I don't have any IT experience but I hope this helps.

upvoted 42 times

BigBilly 1 year, 8 months ago

Were the other questions still accurate?

upvoted 1 times

Cuddles 1 year, 7 months ago

I got the same ones. No clue if I did them correctly, but I can't find them anywhere.

upvoted 1 times

Mar7yi6 1 year, 7 months ago

does someone know where these can be found?

upvoted 2 times

frostxbite 1 year, 7 months ago

If you search on youtube for a guy named Learn-IT academy, he has videos on the simulations

upvoted 1 times

[Removed] 1 year, 7 months ago

Are you saying we should put that order exact order of devices for both columns?

upvoted 1 times

alexandrasexy 1 year, 8 months ago

I can confirm! I had exactly the same practical's today!

upvoted 3 times

Joms26 Highly Voted 11 months ago

click on 801.11 and select b/g

click on SSID and select BYOD (since the ipad is personal and BYOD means bring your own device)

click on frequency and select 2.4Ghz (it has longer range that can penetrate in which 5Ghz is poor at.)

At Wireless Security Mode, Click on Security Mode,Select the WPA2 and the password should be set to TotallySecure!

(WPA2 or Enterprise mode, more suited to organizational or business use. while WPA-PSK relies on a shared passcode for access and is usually used in home environments.)

upvoted 18 times

Avengers_inc 5 months, 2 weeks ago



I would say select AC for the 802.11 then select WPA-PSK because its already configuredd that way in the 2nd to the last snapshpt shown. Yes I strongly recommend 2.4GHz as well because that has a longer reach

upvoted 1 times

  **MikeNY85** Most Recent 1 month ago

The question mentions a personal device to be operated in a corporation so we need to pick "BYOD", the reason for 2.4 GHz is that the heating map which not provided in the question should show 2.4 GHz covering room 3, unlike the 5 GHz spectrum (according to the heating map which is missed) then follow security procedures according to configuration page (BYOD)

upvoted 1 times

  **willyww** 1 month, 3 weeks ago


So what is the correct solution for this ?

upvoted 1 times

  **zhen009** 1 month, 4 weeks ago

Has anyone recently used these questions to pass the exam? And how close are the questions to the actual exam? Are they word for word even the wrong answers are the same?

upvoted 1 times

  **Cyberpleb** 5 months, 2 weeks ago

B/G
CORP
ANNHOME
2.4
WPA2

upvoted 1 times

  **44034** 9 months, 2 weeks ago

hi, I have 5 days left before my code expires, I didn't study at all. is it possible if I study these questions will I pass?

upvoted 1 times

  **willyww** 1 month, 3 weeks ago

did you pass?

upvoted 2 times

  **DonnieDuckoe** 1 year, 4 months ago

I have a question for the community and for the moderators running this wonderful website:

When you reveal the answer and it shows you the "correct" answer, is this always fact? The fact that the given correct answer often contradicts what the community believes is true is confusing. I saw in one comment that this is intentional due to copyright infringement. Can anyone confirm or shed some light on this?

I appreciate your time!

upvoted 2 times

  **[Removed]** 1 year ago

Im not too sure but I think these are official exam questions meaning they are not allowed to give the correct answer otherwise the site would get take down. So I assume that is the whole point of the discussions and the most voted option the questions so they are indirectly giving you the right answer if that makes any sense.

upvoted 9 times

  **jayblack1** 7 months, 3 weeks ago



So this means the answers on the site are wrong?

upvoted 1 times

  **billysunshine** 1 year, 5 months ago

took 1102 today, had 3 pracs: the UPS/surge protector, telephone support for mobile with no email and two helpdesk tickets, how to fix - these are at beginning of q's and at very end - 197/198 I think? Also had a question about stopping a recently installed program from auto starting, answer - use task manager (startup tab). There were a few changed questions in there, but if you know these 198 quite well you will do it. Enjoy!

upvoted 2 times

  **Riderzz** 1 year, 4 months ago

Hi, Do you mean that the 2 helpdesk tickets are after questions 197/198 on this site and what are they about/answers to them too? Also, what were answers to the UPS/surge protector question?

upvoted 4 times

  **[Removed]** 1 year, 7 months ago

All of these questions are on the pearson Vue test right?

upvoted 3 times

  **jackjames** 1 year, 7 months ago

I had this simulation where I had to set up SOHO with two columns, UPS and Surge Protector. But I couldn't figure out what they were asking to properly solve this SIM. Did anyone encounter this SIM?

upvoted 2 times

  **[Removed]** 1 year, 7 months ago

do you know which devices goes in each Column?

upvoted 1 times

  **Cuddles** 1 year, 7 months ago

I assumed everything besides the printer would go in the UPS section but I'm not sure

upvoted 2 times

  **[Removed]** 1 year, 7 months ago



And the surge protector?, and are all these questions on the pearson Vue test
upvoted 1 times

  **JJ_Stone** 1 year, 3 months ago

Yes they are
upvoted 2 times

  **JJ_Stone** 1 year, 3 months ago

Nvm I miss read
upvoted 1 times

  **user82** 1 year, 10 months ago



Why isn't WPA2 the answer? It is more secure than WPA.
And when it states b/g, is this referring to 802.b and 802.g ? In other words 2.4GHz. Why would that be correct?
upvoted 3 times

  **[Removed]** 1 year, 9 months ago

Because ExamTopics did not show the heat map on this site. On the actual exam, there will be a heat map that you can toggle, and it will show that only the 2.4 GHz frequency can reach Ann's office. Thus, you have to use the 2.4 GHz frequency range, which is 802.11b/g. Also, WPA is used because the BYOD (Bring Your Own Device) network uses WPA-PSK.
upvoted 16 times

  **UnfilteredMonkey** 1 year, 8 months ago



WPA2 uses PSK though
upvoted 2 times

  **dbo98** 1 year, 10 months ago

The exam does have the heat map functioning. Unless they change it the Wi-Fi should be b/g with 2.4 GHz.
upvoted 2 times

  **Thejphall** 1 year, 10 months ago

i'm leaning towards b/g but still a bit confused with the way the standards work. My understanding of 802.11ac is that due to its backwards compatibility and use of dualband that it should be the choice in most cases (basing this on most articles i've read about it that are dated later than 2013).
upvoted 1 times

  **dbo98** 1 year, 10 months ago



802.11ac runs at 5GHz. The ac supports beamforming which helps overcome the fact that range is shorter than 2.4. But the heat map is the key to the whole PBQ.
upvoted 5 times

  **ExamLSMotor** 1 year, 10 months ago


Just took the test and the heat map for 5GHz was in red for office space 3, meaning 5GHz does not reach the room. 2.4GHz is green over office 3. So the correct answer would be "2.4GHz" and for 802.11 select "b/g".
upvoted 10 times

  **Thejphall** 1 year, 10 months ago



unless this is explained in the exam wouldn't red on a heatmap mean that area is reached?
upvoted 1 times

  **dbo98** 1 year, 10 months ago

Yes but it has the lowest signal quality. You'd have to see the heat map to understand why it would be 2.4GHz.
upvoted 4 times

  **Monyluv** 1 year, 10 months ago



Thanks for your help I greatly appreciate it. I test next week for Core 2 and this is what I am going to go with now. Do you recall there being any additional labs on the exam or was this the only one? I remember Core 1 having 3 and that's why I ask. Thanks in advance!
upvoted 1 times

  **dbo98** 1 year, 10 months ago

I had 3 PBQs when I took the Core 2 Friday. Brush up on your Command line tools and port numbers and protocol that goes with them.
upvoted 3 times

  **Monyluv** 1 year, 10 months ago



Can anyone confirm that these are the correct steps? It does seem logical. Thanks!
upvoted 1 times

  **dbo98** 1 year, 10 months ago


I think the reasoning for 5GHz is because 802.11ac runs at 5GHz.
upvoted 5 times

  **Bogardinc** 1 year, 9 months ago



802.11ac also runs at 2.4GHz
upvoted 3 times

  **Fatneck** 3 months, 2 weeks ago

No, 802.11ac only works on the 5Ghz band
upvoted 1 times

  **BIZ2021** 2 months, 3 weeks ago

It is backward compatible to b/g/n which support 2.4GHz
upvoted 1 times

  **ciscoxo** 1 year, 10 months ago

Why 5ghz over 2.4?
upvoted 1 times

  **Thejphall** 1 year, 10 months ago

could be wrong or maybe it has something to do with the heat map if that's actually viewable in the real exam
upvoted 3 times

  **ciscoxo** 1 year, 10 months ago

I believe it should be 2.4 because of the distance of the iPad to the AP.
upvoted 7 times

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

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

Correct Answer: B

Antwon Highly Voted 1 year, 10 months ago

Selected Answer: B

The answer is B because we are discussing logging into a Linux SERVER (not a desktop). The best way to do that is via SSH.
upvoted 12 times

JMLorx Most Recent 3 weeks, 5 days ago

Selected Answer: B

Explanation below:

I had no idea but was out of SSH and VNC.

A quick Google search has told me the answer is SSH as this is primarily used and better for servers compared to VNC

VNC

Allows users to share a screen across multiple sessions, and is compatible with many devices and operating systems. VNC Connect encrypts all connections end-to-end, and remote computers can be protected by a password or system login credentials.

SSH

Sets up an encrypted connection between a user's device and a remote machine, often a server. SSH uses public and private key pairs for authentication, which is more secure than traditional password authentication.

upvoted 1 times

CPI 3 months, 2 weeks ago

Selected Answer: B

SecureShell is a good way to remote into a server via command line interface, rather than via GUI.

upvoted 1 times

vshaagar 4 months, 1 week ago

Selected Answer: B

B SSH. GUI is crashed. If GUI crashes how can he use VNC.

upvoted 1 times

088b925 5 months ago

Selected Answer: C

VNC allows remote access to a system's desktop environment, providing a graphical interface that allows for troubleshooting and diagnosis. Since the GUI fails when attempting to log in remotely, using VNC would allow the administrator to visually observe the server's desktop environment, identify errors or failures, and potentially troubleshoot the problem further.

upvoted 2 times

Ham_inclined 8 months, 3 weeks ago

Selected Answer: C

hmm, I guess its SSH. But I picked VNC cause we are trying to get into the GUI. I get that the GUI is crashing, but he was using RDP to remote into a linux server, so of course it wasn't working

upvoted 1 times

newbie176 8 months, 3 weeks ago

he tried to use remote desktop on linux server to fix it which would have been VNC. but since the gui is crashing he needs to use ssh (command line) to fix it. I think that ssh is best answer

upvoted 3 times

Raffaello 9 months ago

Selected Answer: B

SSH or Secure Shell is a network communication protocol that enables two computers to communicate (c.f http or hypertext transfer protocol, which is the protocol used to transfer hypertext such as web pages) and share data.

upvoted 2 times

  **Onero_1z** 10 months, 2 weeks ago

hghhgthgg

upvoted 3 times

  **Stanoh** 1 year ago

C. VNC (Virtual Network Computing).

VNC allows remote access to a graphical desktop environment, which will allow the administrator to view the server's GUI even when there are issues with the server's local display. This can help diagnose the cause of the crashing GUI and potentially resolve the issue.

upvoted 3 times

  **Paula77** 1 year, 1 month ago

Selected Answer: C

VNC is a remote desktop access protocol that allows users to view and interact with the graphical desktop environment of a remote computer. It provides a way for the administrator to access the Linux server's graphical interface remotely and investigate the GUI crash.

upvoted 1 times

  **Mehsotopes** 1 year, 1 month ago

Selected Answer: B

Uses a text based interface to give you access under CLI.

upvoted 1 times

  **Kristheitguru** 1 year, 5 months ago

Selected Answer: B

B

Because u can SSH using the RDP port and test if the port is open.

upvoted 1 times

  **Fuzm4n** 1 year, 10 months ago

Selected Answer: B

It's B. Linux server. Issue with the GUI. You still need to log into it. You can login with a CLI via SSH. Not sure how you guys are getting D.

upvoted 4 times

  **sioke** 1 year, 11 months ago

How to transfer data between linux and windows

Navigate and open File > Site Manager.

Click a New Site.

Set the Protocol to SFTP (SSH File Transfer Protocol).

Set the Hostname to the IP address of the Linux machine.

Set the Logon Type as Normal.

Add the username and password of the Linux machine.

Click on connect.

can this help to clarify the answer to be B

upvoted 1 times

  **glenpharmd** 1 year, 7 months ago

SFTP. You used this protocol as an example on how to transfer files between linux and windows. is that not one of the answers.

upvoted 1 times

  **CTE_Instructor** 1 year, 7 months ago

SFTP is SSH or Secure File Transfer Protocol and is not the correct answer to this question. This protocol is not used for logging in to a server, but does use SSH to transfer files between systems.

The correct answer is SSH which will allow you to log in via CLI in order to troubleshoot whatever problem this team is having.

upvoted 1 times

  **ATill** 1 year, 11 months ago

It's not remote desktop. It's Microsoft Remote Assistance that helps with remote issues. It's a Windows desktop remoting into a Linux server. So it would be MSRA

upvoted 2 times

  **simsbow1098** 1 year, 11 months ago

The answer is SSH. VNC is for MACos. MSRA is for Windows. SFTP is a SSH file transfer protocol. The question says Linux. Only remote access protocol on all major OS platforms.

upvoted 2 times

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

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



Correct Answer: C

  **Antwon** Highly Voted 1 year, 10 months ago

Selected Answer: C

The answer is C because both A and D will not accomplish wiping a hard drive, and subsequently a quick format will not sufficiently wipe information from a drive.

upvoted 5 times

  **cpaljhc** 1 year, 9 months ago

What about B

upvoted 1 times

  **StrawberryTechie** 1 year, 4 months ago

Quick formatting only erases the address of where to find the data on the drive. The data is still all there. So this is not a good option.

upvoted 1 times

  **user82** 1 year, 9 months ago

It asks what is the MOST secure method. C would be best

upvoted 1 times

  **[Removed]** 1 year, 9 months ago

B would install a file system on the drive but not wipe any information from it.

upvoted 1 times

  **er.garg2687** Most Recent 2 weeks, 3 days ago

Answer C is most accurate

upvoted 1 times

  **ITEXAMSLAB_COM_Comptia** 1 month ago

C. Using disk-wiping software

upvoted 1 times

  **GarbanzoBeans** 9 months ago

Selected Answer: D

CMD



list disk

select disk x (replace x with the disk number of your USB drive)

clean all

c'mon yall

upvoted 1 times

  **newbie176** 8 months, 3 weeks ago

but its not the most secure i think. You can still find data on it if u really tried. U gotta use disk wiping software

upvoted 2 times

  **Ham_inclined** 8 months, 3 weeks ago

Is there a way to Overwrite partitions from CMD instead of just deleting them? or maybe a powershell tool

upvoted 1 times

  **igorclapa** 5 months, 3 weeks ago

This is wrong.

upvoted 2 times

  **Chavozamiri** 9 months, 1 week ago

Selected Answer: C

C. Using disk-wiping software

upvoted 3 times

[Removed] 1 year, 5 months ago

Drilling it is the safest.

upvoted 1 times

[Removed] 1 year ago

It says to be reused. Doing this you cant reuse the hard drive.

upvoted 6 times

[Removed] 1 year, 9 months ago

Selected Answer: C

A, B, and C will not completely wipe the data from the drive.

upvoted 4 times

[Removed] 1 year, 9 months ago

Correction, D won't. C will.

upvoted 1 times

Question #4

Topic 1

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

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

Correct Answer: B

Antwon **Highly Voted** 1 year, 10 months ago

Selected Answer: B

The application in question is clearly malware, therefore it is best to remove it. A factory reset can remove malware, but doing something drastic like that is usually not a first step. Additionally, C and D won't help with removing malware.

upvoted 14 times

er.garg2687 **Most Recent** 2 weeks, 3 days ago

whenever application experience high utilization of bandwidth. It should be removed immediately

upvoted 1 times

Tswaka 1 year, 3 months ago

The answer is clear the application must be removed

upvoted 1 times

navvvarroooo 1 year, 8 months ago

She may actually have viruses. The software seems to be using more data. A poor program isnt always malware so we cannot assume this yet. As it asks what should you do FIRST.

upvoted 1 times

takomaki 1 year, 7 months ago

Yeah, but she is also receiving security warnings. What else could it be besides malware?

upvoted 2 times

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

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

Correct Answer: B

simslow1098 Highly Voted 1 year, 11 months ago

The change management phases are as follows:

Request forms, Purpose of change, Scope of the change, Date and Time of the change, Affective systems/ impact, risk analysis, change board approval, finally end user acceptance. With this the answer is end user acceptance.

upvoted 38 times

alexandrasexy Highly Voted 1 year, 9 months ago

Selected Answer: A

Final answer is A.

Order of change management phases:

1. Request forms
2. Purpose of change
3. Scope of the change
4. Date and Time of the change
5. Affective systems/ impact
6. Risk analysis
7. Change board approval
8. Finally end user acceptance.

upvoted 24 times

FALLY4 Most Recent 1 day, 14 hours ago

end user acceptance is done after or during the change implementation

upvoted 1 times

Philco 4 weeks ago

Selected Answer: B

Change Advisory Board only "approved change Request" , The did not approve the the Change in itself, Answer is B

upvoted 1 times

Dave93266 8 months, 3 weeks ago

Selected Answer: A

1. Request forms
2. Purpose of change
3. Scope of the change
4. Date and Time of the change
5. Affective systems/ impact
6. Risk analysis
7. Change board approval
8. End user acceptance.

upvoted 1 times

PatrickH 9 months ago

As Per Comptia Objectives: • Change management

- Request forms
- Purpose of the change
- Scope of the change
- Date and time of the change
- Affected systems/impact
- Risk analysis
- M Risk level
- Change board approvals
- End-user acceptance

Thats said no where does it explicitly state the actual order as in saying 1-8



upvoted 1 times

Chavozamiri 9 months, 2 weeks ago

Selected Answer: B

Is NOT A because A is the last step in the management phase, the most likely be the correct after a request approval is risk analysis. REQUEST FORM IS FIRST STEP Right Answer B!

upvoted 1 times

  **Chavozamiri** 9 months, 2 weeks ago

I'm wrong cause I just read again and the questions is about CHANGE BOARD REQUEST APROVAL , so the correct answer is A if is regarding Change board, if was about REQUEST FORM approval so Risk analysis...

upvoted 3 times

  **Yomijohnson** 1 year, 1 month ago

Good job guys

upvoted 1 times

  **WEREFox** 1 year, 2 months ago

Selected Answer: A

Mike Myers lists more steps, but "A. End user acceptance" is correct for these choices.

upvoted 1 times

  **Pras97** 1 year, 2 months ago

Nothing changes without the process

- Complete the request forms
- Determine the purpose of the change
- Identify the scope of the change
- Schedule a date and time of the change
- Determine affected systems and the impact
- Analyze the risk associated with the change
- Get approval from the change control board
- Get end-user acceptance after the change is complete

upvoted 3 times

  **jjwelch00** 1 year, 2 months ago

Selected Answer: C

C. Communicate to stakeholders: Once the change request is approved by the CAB, the next logical step is to communicate the approved change to the relevant stakeholders. This involves informing affected parties, such as end users, managers, and other teams, about the upcoming change, its impact, and any necessary actions or preparations they need to take. Clear and effective communication is crucial to ensure everyone is aware of the change and can plan accordingly.

upvoted 3 times

  **Thunder_Cat** 1 year, 4 months ago

Selected Answer: B

According to CompTIA CertMaster Learn for A+, the order for change request approval process is as follows: Change Board Approvals, Risk Analysis, Test and Implement the Change Plan, then End-user Acceptance.

upvoted 4 times

  **Thunder_Cat** 1 year, 4 months ago

Communicate to Stakeholders is a part of the Test and Implement the Change Plan.

upvoted 1 times

  **I_Know_Everything_KY** 1 year ago

This is absolutely incorrect.

its:

- Complete the request forms
- Determine the purpose of the change
- Identify the scope of the change
- Schedule a date and time of the change
- Determine affected systems and the impact
- Analyze the risk associated with the change
- Get approval from the change control board
- Get end-user acceptance.

upvoted 1 times

  **lordcheekklappur** 1 year, 4 months ago

Selected Answer: C

The other options are not the most likely next steps for the following reasons:

A. End user acceptance: End user acceptance typically occurs after the change has been implemented and tested to ensure that it meets the intended requirements and does not disrupt normal operations.

B. Perform risk analysis: Risk analysis is generally conducted before the change request is submitted to the CAB for approval. It helps to identify potential issues, evaluate the impact of the change, and determine if it is a viable solution.

D. Sandbox testing: Sandbox testing, which involves testing the change in an isolated environment, is usually performed before the CAB approval to ensure that the proposed change will not have any adverse effects on the production environment. It is part of the testing and validation process that precedes the CAB's decision.

upvoted 4 times


[-]  **SanaQayyum** 1 year, 5 months ago

Selected Answer: A

<https://www.professormesser.com/free-a-plus-training/220-1102/220-1102-video/change-management-220-1102/>

Please read last paragraphs

upvoted 4 times

[-]  **Pegi** 1 year, 4 months ago

Thank you for your guidance. I've just found it: "And one of the last steps of the change control process is having the end users confirm that the change was successful."

upvoted 2 times

[-]  **rah555** 1 year, 5 months ago

Selected Answer: C

The next step in the change process after a change advisory board approves a change request is to communicate to stakeholders. This is done to ensure that everyone who will be affected by the change is aware of it and can prepare accordingly. After communicating to stakeholders, the next step would be to perform risk analysis and sandbox testing before moving on to end user acceptance.

upvoted 2 times

[-]  **Kristheitguru** 1 year, 5 months ago

Selected Answer: D

The most likely next step in the change process after a change advisory board (CAB) approves a change request is to implement the change. Therefore, none of the options A, B, or C is the most likely next step.

Option D, "Sandbox testing," could be a possible next step before implementing the change in the production environment. This involves testing the change in a non-production environment, such as a sandbox or test environment, to identify and address any issues or conflicts that could affect the production environment.

upvoted 2 times

[-]  **[Removed]** 1 year, 6 months ago

Selected Answer: A

Refer to Professor Messer's videos.

upvoted 1 times

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

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

Correct Answer: C

Thejphall Highly Voted 1 year, 10 months ago

Selected Answer: C

After verifying the malware, quarantining would be the next step in malware removal process. Comptia Exam Objectives for malware removal.

1. Investigate and verify malware symptoms
2. Quarantine infected systems
3. Disable System Restore in Windows
4. Remediate infected systems
 - a. Update anti-malware software
 - b. Scanning and removal techniques (e.g., safe mode, preinstallation environment)
5. Schedule scans and run updates
6. Enable System Restore and create a restore point in Windows
7. Educate the end user

upvoted 10 times

Antwon Highly Voted 1 year, 10 months ago

Selected Answer: C

The answer is C because generally, quarantining a system is the first thing you do in malware removal. Then comes disabling system restore, then scan and remove the malware, and then schedule automated malware scans.

upvoted 7 times

er.garg2687 Most Recent 2 weeks, 3 days ago

Whenever system is suffering from Ransomware it should be isolated from network

upvoted 1 times

CPI 3 months, 2 weeks ago

Selected Answer: C

Always. Quarantine. First.

upvoted 1 times

Chavozamiri 9 months, 2 weeks ago

Selected Answer: C

Not great question but answer is C.

upvoted 1 times

CPAB 1 year, 3 months ago

Selected Answer: C

Quarantine the unit to not affect other users if the ransomware can affect the network. It was not recoverable even if you paid them and some ransomware keys were exposed online.

upvoted 2 times

Jcsimple 1 year, 6 months ago

Quarantine it guys, don't want it to spread like wildfire.

upvoted 2 times

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

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

Correct Answer: B

  **Antwon** Highly Voted  1 year, 10 months ago

Selected Answer: B

Remote wipe is the only one of these options that can truly keep your data from being stolen.
upvoted 10 times

  **GarethN** Most Recent  1 month ago

Selected Answer: D



A screen lock is the correct answer, remote wiping will only work if the phone is connected to the internet, if anyone steals a phone the first thing they are going to do is disable any internet connectivity ,but if a phone is stolen/lost with a screen lock one one will be able to access the data on the phone provided they don't know the password.
upvoted 1 times

  **goss_6087** 2 months, 2 weeks ago

If its company based, I would say they would use strict protocol, therefore answer is, B
Home user based, answer is, A
upvoted 1 times

  **Ok34** 6 months ago

answer is B
upvoted 1 times

  **hansie123** 6 months, 2 weeks ago

haha i wish i could wipe remotely
upvoted 1 times

  **Chavozamiri** 9 months, 2 weeks ago

Selected Answer: B

Answer B.
upvoted 1 times

  **mohdAj** 9 months, 3 weeks ago

Selected Answer: B

Remote wipe allows the company to remotely erase all data on the smartphone, preventing unauthorized access to sensitive information.
upvoted 1 times



  **exposure** 10 months, 2 weeks ago

Selected Answer: B

Simple
upvoted 1 times

  **BeautyBrainz** 11 months ago

According to CompTia they want to know what will keep someone from getting into the data so say there is already a screen lock on it, but someone finds a way to get into it. Once it is reported lost or stolen the company can find that phone and wipe the data clean. Remote wipe is the best answer
upvoted 1 times

  **ZioPier** 1 year, 3 months ago

Selected Answer: B



This question is quite vague, but there's few details that help us making a decision:

First of all the question doesn't say that the company wants to preserv the data on phone a s valuable, so wiring the data is a good option.

If option D was multifactor or biometric unlock, i would have considered it, but is just mentioning lockscreen, which is easily skippable, so not safe at all.

However, once an individual with malicious intention has your smartphone, he can easily access to all data without even turning it on, so remote wire is the best option

upvoted 4 times

  **Stonetales987** 1 year, 6 months ago

Selected Answer: B

B. Remote wipe.

upvoted 2 times

  **ninaanto** 1 year, 8 months ago

Selected Answer: B

Remote wipe enables you to remotely erase the data on the mobile device if the device is lost or stolen. If you enable the remote wipe feature on your mobile device, you can permanently delete data stored on your lost or stolen mobile device. You should make sure the erase feature completely erases the data

upvoted 2 times

  **Nick40** 1 year, 9 months ago

Selected Answer: D

Lock screen

upvoted 2 times

  **ImpactTek** 1 year, 9 months ago

Selected Answer: D

I go with screen lock because it says to "ensure data is secure". If we wipe the device then there is no data. To ensure security we need to encrypt it and put a pin on the device. Overallly the question is not complete and you can perceive either ways. It is a bad comptia question. I faced a similar question like this with a small change, in that question it was mentioned "without losing data" so the answer was pin. Here the question is not complete. If we don't overthink it the "remote wipe" make sense, if we overthink it the "pin" is the answer.

upvoted 1 times

  **Mojere** 1 year, 6 months ago

Data is secured if it follows the CIA triad, and the device is lost or stolen. The best option will be to remotely wipe the device if the device cannot be recovered to keep data secured. Definitely company data will always have some type of backup.

upvoted 1 times

  **Riderzz** 1 year, 9 months ago

I see where you are getting at, so when employers are issuing their employees smartphones having pin makes data more secure LOGICALLY though. If the lost device is found by a stranger, data can be stolen physically. It only takes a screwdriver and that data is far from secure.

upvoted 4 times

  **twobuckchuck** 1 year, 10 months ago

Selected Answer: D

Screen lock. If it gets stolen, nobody knows your password and can't access the data

upvoted 2 times

  **[Removed]** 1 year, 9 months ago

And if they steal the phone and take the hard drive in it? B is the answer.

upvoted 4 times

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

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

Correct Answer: B

  **Antwon** Highly Voted 1 year, 10 months ago

Selected Answer: B

The answer is B because the scenario being described is clearly adware. Therefore, the only way to truly mitigate the issue would be to run a full antivirus scan.

upvoted 18 times

  **WindySummer** 3 months, 1 week ago

****A****. The most effective solution for the technician to implement in this scenario is to disable the browser's capability to send notifications to the Windows 10 Action Center. By doing so, the unwanted advertisement notifications originating from the browser will no longer appear within the Action Center, providing relief to the user. This solution directly targets the source of the notifications, ensuring a focused resolution.

upvoted 2 times

  **max12553** 2 weeks, 4 days ago

That might work for us as normal people but not for CompTIA

upvoted 1 times

  **Riderzz** 1 year, 9 months ago

It's A.

The ad doesn't seem malicious and most certainly is not a virus. It is coming from the browser, running a scan may detect something but will not block it.

D could be correct but there is no specific site, A would be easier to block all browser notifications going into action centre.

upvoted 5 times

  **[Removed]** 1 year, 7 months ago



It said non-malicious

upvoted 10 times

  **[Removed]** 1 year ago

seemingly non-malicious

upvoted 13 times

  **vshaagar** 4 months, 1 week ago

But here it doesn't say if the USER is trained or not, so we have no idea. The best option is B. Running the antivirus scan.

upvoted 1 times

  **CTE_Instructor** 1 year, 7 months ago

Notifications from a web browser are not adware. Adware by definition is software designed to advertise. There is no software being installed, no performance issues related to the notifications, and the scenario clearly says it is not malicious.



If you had notifications from your browser appear on your notification center, sensibly the first thing you would do is disable the notifications.

upvoted 9 times

  **RoPsur** 1 year, 2 months ago

It also says "seemingly" before non-malicious. Therefore the BEST solution is to Run a full antivirus scan on the computer.

upvoted 2 times

  **IconGT** Highly Voted 1 year, 4 months ago

Selected Answer: B

B. Run a full antivirus scan on the computer would be the best solution for a technician to implement in this case. While the advertisements may not appear malicious, they could potentially be part of an adware or spyware program that is running on the computer. Running a full antivirus scan can help detect and remove any malicious software that may be causing the unwanted notifications. Disabling the browser from sending notifications, disabling all Action Center notifications, or moving specific site notifications from Allowed to Block may not address the underlying issue of a potential malware infection.

upvoted 11 times

  **MikeNY85** Most Recent 2 months, 4 weeks ago

The word 'RANDOM' gives the impression of Adware, all in all, running a virus scan is a first legit first step in this situation (my opinion).
upvoted 1 times

  **MikeNY85** 2 months, 4 weeks ago

all in all, running a virus scan is a first legit step in this situation (my opinion).
upvoted 1 times

  **Jay23AmMonsIV** 3 months ago

Selected Answer: A

This approach targets the root cause of the issue by preventing the web browser from sending any notifications to the Action Center. This will stop the random advertisement notifications without disabling other important notifications from the Action Center or having to identify and block specific sites individually. Running a full antivirus scan is also important for general security, but it may not directly address the specific issue of browser notifications.

upvoted 1 times

  **joeshmungus** 3 months, 4 weeks ago

Selected Answer: D

Dealt with this issue last week. The user had simply clicked "allow notifications" on a site they shouldn't have, so I followed option d to solve.

Adware is software designed to give you ads, your browser is not that. If the ads were pop up windows then it would be symptomatic, but the browser delivers any notification to your action centre. I chose D, as there is still a chance the user has browser notifications for legitimate sites.

(I gave a full scan to be safe, and nothing came up. Understandably these ad notifications do come from dodgy websites, but Comptia's step one to the process is "Investigate and verify malware symptoms" of which browser notifications are not.)


upvoted 3 times

  **igorclapa** 5 months, 3 weeks ago

Why are some of you selecting D???

Blocking notifications does not resolve the adware issue lol.

upvoted 1 times

  **joeshmungus** 3 months, 1 week ago

Adware is software designed to give you ads, your browser is not that. If the ads were pop up windows then it would be symptomatic, but the browser delivers any notification to your action centre. I chose D, as there is still a chance the user has browser notifications for legitimate sites.

upvoted 1 times

  **TemplarLord** 6 months, 2 weeks ago

Selected Answer: D

This is the best way.

upvoted 2 times

  **Iditenaxyigospoda** 7 months, 2 weeks ago

Selected Answer: D

Move specific site notifications from Allowed to Block.

upvoted 3 times

  **Raffaello** 9 months ago

Selected Answer: B



The BEST solution for a technician to implement is to run a full antivirus scan on the computer to detect and remove any potentially unwanted programs or malware that may be causing the unwanted advertisements in the Windows 10 Action Center

upvoted 1 times

  **IVHoltzmann** 9 months ago

This won't stop the notifications though. This issue occurs when a website has permissions to send notifications to Windows through the browser.

upvoted 1 times

  **Alizade** 9 months, 1 week ago

Selected Answer: D

D. Move specific site notifications from Allowed to Block.

upvoted 2 times

  **Chavozamiri** 9 months, 2 weeks ago

Selected Answer: B

ANSWER B clearly adware.

upvoted 1 times

  **Psyc00** 10 months, 1 week ago

Selected Answer: D

D. Move specific site notifications from Allowed to Block.

These notifications are likely coming from websites that the user has granted permission to show notifications. By moving specific site notifications from "Allowed" to "Block," the technician can prevent unwanted notifications from websites that the user does not wish to receive notifications

from. This solution addresses the issue at its source without affecting other Action Center notifications or disabling all notifications (Options A and C). Running a full antivirus scan (Option B) is a good practice but may not be directly related to this specific issue unless there is suspicion of malware

upvoted 2 times

  **Andylove** 11 months, 3 weeks ago

Selected Answer: D

Option D, on the other hand, addresses the problem directly. Many web browsers allow users to manage site notifications. By moving notifications from specific websites that are displaying unwanted advertisements from "Allowed" to "Block," you can prevent these sites from sending notifications to the Action Center, effectively stopping the unwanted advertisements without affecting other notifications or legitimate website notifications. This is a more precise and user-friendly approach to addressing the issue.

upvoted 3 times

  **Andylove** 11 months, 3 weeks ago

Selected Answer: D

Option D, on the other hand, addresses the problem directly. Many web browsers allow users to manage site notifications. By moving notifications from specific websites that are displaying unwanted advertisements from "Allowed" to "Block," you can prevent these sites from sending notifications to the Action Center, effectively stopping the unwanted advertisements without affecting other notifications or legitimate website notifications. This is a more precise and user-friendly approach to addressing the issue.

upvoted 2 times

  **ConqiD** 12 months ago

Selected Answer: D

Options A and C are more general approaches that may have unintended consequences, such as blocking notifications from all websites or disabling the Action Center notifications entirely, which may not be necessary and could impact the user's overall experience. Option B, running a full antivirus scan, is a good practice for overall system security but is less likely to address this specific issue, as these notifications are not necessarily indicative of a malware infection. Addressing the issue at the browser level (Option D) is a more targeted and appropriate solution in this context.

upvoted 1 times

  **Footieprogrammer** 1 year ago

Selected Answer: B

Run a scan

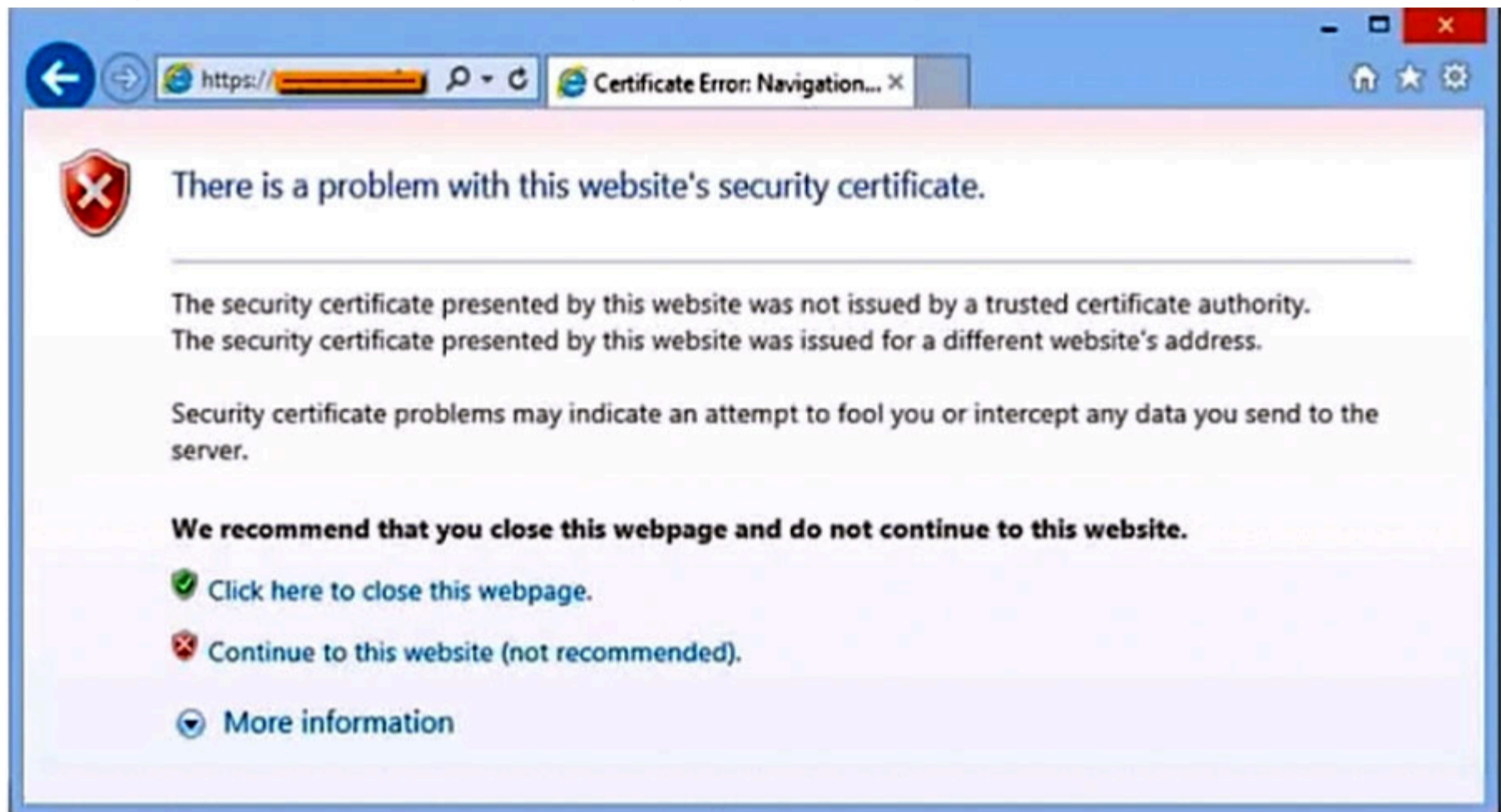
upvoted 1 times

  **I_Know_Everything_KY** 1 year ago

These ads are not malicious: they mostly come from users inadvertently allowing notifications from browsers. If you disable *all* notifications, then you lose this functionality. If one site is sending ads, then its most efficient to simply block that site in your browser settings.

upvoted 1 times

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



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

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

Correct Answer: A

techteacher Highly Voted 1 year, 10 months ago

Selected Answer: D

The use of the word "purportedly" makes me think this is a fraudulent website. At the very least, we aren't sure and the question asks what should the tech do FIRST. I would choose D.

upvoted 8 times

Sebatian20 Highly Voted 1 year, 3 months ago

D - Better to exit the website first and then investigate.

upvoted 7 times

jayblack1 Most Recent 7 months, 3 weeks ago

Selected Answer: D

The correct answer is D because the question asks what would be the first thing you should do. The link is from an e-mail. which could potentially be a phishing attack. And imagine this, you are the CFO which means you've been opening your organisations website many times in your browser without any problems. Then one day you get a link in your e-mail which seems to link to your org's bank but this time your browser flags it. Isn't that suspicious? The first thing to do would be to leave the site.

upvoted 2 times

PatrickH 9 months ago

Its D. Looks like an almost textbook example of Whaling

upvoted 1 times

Chavozamiri 9 months, 2 weeks ago

Selected Answer: D

After clicking on a link in an email ? Answer is probably D... if someone get this question on the exam can you please update here my comment pls

upvoted 1 times

Chavozamiri 9 months, 2 weeks ago

After clicking on a link in an email ? Answer is probably D... if someone get this question on the exam can you please update here my comment pls

upvoted 2 times

  **BeautyBrainz** 11 months ago

If there is a lock & a https:// address then it is a legitimate site & the certificates just need to be installed or updated.

upvoted 1 times

  **mgua83** 11 months, 1 week ago

I selected "D" for the reason it being a email with a link not a website that a Certificate was expired

upvoted 1 times

  **Footieprogrammer** 1 year ago

Selected Answer: D

D, no doubt.

upvoted 2 times

  **ZioPier** 1 year, 3 months ago

Is specified that the link is genuine. Happens often certificates get relocated due to many different issues. Updating the CRL will make the link certified again or make it fail in case is not genuine

upvoted 3 times

  **Chavozamiri** 9 months, 2 weeks ago

good point!

upvoted 1 times

  **Babi_12** 1 year, 4 months ago

Instructing CFO to exit the browser is the best option

upvoted 3 times

  **ronniehaang** 1 year, 6 months ago

Selected Answer: D

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

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

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

upvoted 6 times

  **ronniehaang** 1 year, 6 months ago

Filing a trouble ticket with the bank (Option B) or contacting the ISP to report the CFO's concern (Option C) may be useful in determining whether the link was legitimate or fraudulent, but these steps can also be taken after the immediate threat has been addressed.

In conclusion, the first and most important step the technician should take is to instruct the CFO to exit the browser immediately to prevent any potential harm.

upvoted 3 times

  **alexandrasexy** 1 year, 9 months ago

Selected Answer: D

Correct is D. Instruct the CFO to exit the browser.

upvoted 3 times



  **DonovanG** 1 year, 10 months ago

Selected Answer: D

CFO, bank, purportedly, problem with website's security certificate.

These info are enough

upvoted 4 times

  **Antwon** 1 year, 10 months ago

Selected Answer: A

CRL stands for Certificate Revocation List, and in this scenario probably needs to be updated so it can trust the website. (Certificates expire)

upvoted 4 times

  **twobuckchuck** 1 year, 10 months ago

Yea because you should do that FIRST totally

upvoted 2 times

  **RSMCT2011** 1 year, 10 months ago

the error message says the certificate is not issued by trusted CA, and the certificate was presented for other web server, so nothing to do with revoked certificated

upvoted 1 times

  **takomaki** 1 year, 7 months ago

RSMC is right. A revoked certificate would give a different error on internet explorer.

upvoted 1 times

  **Thejphall** 1 year, 10 months ago

Unless you access to the link address the CFO used wouldn't it be assumed based off the evidence presented that this was probably a phishing attempt and the site is fraudulent? The wording of the question made it seem that way at least. I would've probably gone with D.

upvoted 5 times

  **Thejphall** 1 year, 10 months ago



have* access

upvoted 1 times

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.

Correct Answer: B

  **Antwon** Highly Voted 1 year, 10 months ago

Selected Answer: C

It's a SOHO environment, meaning there are only a few machines. You can certainly manually check each one.
upvoted 21 times

  **twobuckchuck** 1 year, 10 months ago

Have you ever heard the phrase "Size doesn't matter"
upvoted 3 times

  **alexandrasexy** 1 year, 9 months ago

Actually, size does matter!
upvoted 15 times

  **techteacher** Highly Voted 1 year, 10 months ago

Selected Answer: C

I'm not sure how sending a sample to the vendor will help with checking other machines.
upvoted 8 times

  **rodwave** 1 year, 1 month ago

The network being a SOHO environment is important here because manually checking each machine wouldn't really be practical in a large network, since it would be time-consuming. Since an enterprise would likely deploy the same AV across a network, you could send a sample to an AV vendor where they could create detection signatures that the vendor can use to update the AV agents deployed across a network. Again, not really something a small network would find necessary.
upvoted 6 times

  **willyww** Most Recent 1 month, 3 weeks ago

they are asking MOST effective way to check other machines not how to remediate the unknow virus, The script seems like a good idea but the technician does not have a specific file, option b is ruled out because they are not asking how to remedy the virus, option d does not make much sense, I think the most logical is option c
upvoted 1 times

  **Jay23AmMonsIV** 3 months ago

Selected Answer: B

Here's why this is the best approach:


The antivirus vendor can analyze the unknown executable to determine if it is indeed a new or variant form of malware. They have the expertise and tools to thoroughly investigate the file.

If the file is confirmed to be malicious, the antivirus vendor can update their virus definitions to detect and remove the threat. This ensures that all machines protected by their antivirus software will be able to detect and handle the malware.

This approach not only protects the machines within the current network but also helps other users globally who might be exposed to the same threat.

While other options like running a startup script, manually checking each machine, or monitoring outbound network traffic can help in identifying or mitigating the issue, they are less comprehensive and may miss variations of the malware or fail to detect it completely. Providing a sample to the antivirus vendor ensures a thorough and expert analysis, leading to a more robust and effective solution.

upvoted 3 times

  **Tural038** 4 months, 3 weeks ago

Selected Answer: C

The answer is C
upvoted 2 times

  **bobby** 5 months, 3 weeks ago

I can't answer this question. C is good for RIGHT NOW. B is good for LONG TERM. How long before Antivirus will be updated? This is a serious question I do not know the answer. SOHO size may determine which i do first.

upvoted 1 times

  **yutface** 6 months ago

Selected Answer: B

Chat GPT by itself I often mistrust for these questions. But when Gemini suggests the same answer, I am more inclined to believe it. They both picked B:
Here's why:

Targeted approach: Submitting the unknown executable to the antivirus vendor allows them to analyze the file and potentially identify the threat. This targeted approach can lead to the creation of specific signatures that can accurately detect the threat on other machines.



Scalability: Compared to manually checking each machine (option C), submitting a sample is much more efficient, especially in a SOHO environment with multiple devices.

Future protection: If the vendor identifies the threat and creates a signature, it will not only help detect existing infections but also prevent future infections on all protected machines.

Here's why not C:

This is very time-consuming and impractical, even in a SOHO environment of up to 10 people. Additionally, manual searches might miss the threat if it's hiding or disguised.

upvoted 2 times

  **DBrega** 6 months, 3 weeks ago

Selected Answer: B

C would be feasible in a SOHO, but it is far from being the MOST EFFECTIVE way of dealing with viruses, unless you are a professional malware analyzer, and better than a whole team analyzing it, as it would be in a Antivirus vendor company. Spoiler, you aren't.

upvoted 1 times

  **Psyc00** 10 months, 1 week ago

Selected Answer: B

B. Provide a sample to the antivirus vendor.

Providing a sample of the unknown executable to the antivirus vendor is a prudent step to identify and address the potential threat. Antivirus vendors can analyze the sample, develop detection signatures, and provide updates to their antivirus software to detect and remove the threat from other machines on the network. This approach helps protect all machines in the network without having to manually check each one (Option C), which can be time-consuming and less effective. Monitoring outbound network traffic (Option D) may help identify suspicious activity but may not directly lead to the identification of the specific threat. Running a startup script to remove files by name (Option A) may not be effective if the threat has multiple variants with random string names.

upvoted 1 times

  **Onero_1z** 10 months, 2 weeks ago

Selected Answer: B

"the most effective way" so i think its B. CHATGPT also said is B

upvoted 1 times

  **Footieprogrammer** 1 year ago

Selected Answer: C

Easy to check SOHO network units manually, given that there are only a few units

upvoted 1 times

  **glenpharmd** 1 year ago

Given these options, B. Provide a sample to the antivirus vendor is the MOST effective way to check other machines on the network for this unknown threat. This way, once the vendor updates their definitions, all machines running the updated antivirus will be able to detect and potentially remove the threat

upvoted 1 times

  **Mehsotopes** 1 year, 1 month ago

Selected Answer: B

B makes sense for this answer, because it would be easier to consult the antivirus distributor to set an automated way to check codes inside of machine that has this rogue line and to add it to their definitions incase the attack/mistake is created again.

You can check each individually, but it's less inefficient and has less long term security.

upvoted 2 times

  **AdamRachel** 1 year, 4 months ago

Selected Answer: B

it is clearly stated that the virus is unknown to the technician. so the best way will be to send a sample to the vendor so they can send some useful information as they have a bigger base?

upvoted 2 times

  **Onero_1z** 1 year, 4 months ago

Selected Answer: C

the question made it clear stating "checking other machines" which makes c the right answer

upvoted 1 times

  **Phrank** 1 year, 5 months ago

The MOST effective way to check other machines on the network for the unknown threat would be option D: Monitor outbound network traffic.

By monitoring outbound network traffic, the technician can identify any network activity associated with the unknown executable. This can provide valuable information about the extent of the infection, including the number of machines affected, the nature of the traffic, and any communication with external servers.

upvoted 1 times

  **ronniehaang** 1 year, 6 months ago

The most effective way to check other machines on the network for the unknown threat is to manually check each machine. Option C is the correct answer.

Manually checking each machine on the network is the most effective way to identify whether any other machines are infected with the same unknown threat. This may involve running scans with various antivirus and anti-malware tools, reviewing system logs for suspicious activity, and inspecting system files for any anomalies. The technician should also interview users to see if they have experienced any unusual activity on their machines.

upvoted 1 times

  **ronniehaang** 1 year, 6 months ago

Running a startup script that removes files by name (Option A) may remove the file from infected machines, but it will not identify other machines that are infected with the same threat.

Providing a sample to the antivirus vendor (Option B) is a good step in detecting and preventing the spread of the threat, but it may take some time before the antivirus vendor can provide a detection and removal solution.

Monitoring outbound network traffic (Option D) may help identify whether any machines are communicating with known malicious servers, but it may not be effective in identifying this unknown threat.

In conclusion, manually checking each machine on the network is the most effective way to identify whether other machines are infected with the same unknown threat.

upvoted 2 times

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

- A. Keyboard
- B. Touch pad
- C. Ease of Access Center
- D. Display settings

Correct Answer: C

  **RJ4** Highly Voted  1 year, 11 months ago

Ease of Access settings configure input and output options to best suit each user. There are three main settings groups: Vision configures options for cursor indicators, high-contrast and color-filter modes, and the Magnifier zoom tool.
upvoted 9 times

  **JackyCIT** 1 year, 9 months ago

correct
upvoted 1 times

  **Antwon** Highly Voted  1 year, 10 months ago

Selected Answer: C

You can check this yourself if you have Windows 10. Go to settings, then ease of access, and there you will see on the sidebar "mouse pointer" where you can change the cursor color.
upvoted 5 times

  **Raffaello** Most Recent  9 months ago

Selected Answer: C

The Ease of Access Center provides a centralized location in the Control Panel where you can adjust accessibility settings and programs
upvoted 1 times

  **LibPekin** 10 months, 2 weeks ago

Selected Answer: C

Windows 10-11 users can verify this
upvoted 1 times

  **MrRoi** 11 months ago

It's C.. The Ease of Access setting is specifically catered to those with disabilities.
upvoted 1 times

  **Footieprogrammer** 1 year ago

Selected Answer: C

Ease of access center, you can try for yourself.
upvoted 1 times

  **rah555** 1 year, 5 months ago

Selected Answer: C

Ease of Access Center
upvoted 2 times

  **twobuckchuck** 1 year, 10 months ago

Selected Answer: B

I think its B
upvoted 2 times



  **JackyCIT** 1 year, 9 months ago



what a troll
upvoted 1 times

  **sinfulhymn** 1 year ago

can we collectively to report dumbasses and trolls please

too many stupid confident people giving out bad answers either on purpose or just because they're plain stupid
upvoted 3 times

  **CecilSaw** 1 year, 10 months ago
Ease of access center for accessibility options...
upvoted 3 times

  **JackyCIT** 1 year, 9 months ago
this dudes trolling
upvoted 2 times

Question #12

Topic 1

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

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

Correct Answer: D

  **Fuzm4n** Highly Voted  1 year, 10 months ago

Selected Answer: D

SSO with biometrics would do it. Nothing to remember and you would be logged into all your accounts.
upvoted 9 times

  **Tural038** Most Recent  4 months, 3 weeks ago

Selected Answer: D

D definitely
upvoted 1 times

  **Mr_Tension** 5 months, 1 week ago

it's D guys. source: Trust me
upvoted 1 times

  **AzadOB** 9 months ago

A
that will help with security and remembering the passwords.
upvoted 1 times

  **Footieprogrammer** 1 year ago

Selected Answer: D

Nothing to remember, easy login with biometrics
upvoted 2 times

  **Nick40** 1 year, 8 months ago

Selected Answer: D

its is D
upvoted 2 times

  **twobuckchuck** 1 year, 10 months ago

Selected Answer: C

Question specifically says what should he do to reduce helpdesk tickets. Doesn't say anything about without increasing security risk. Clear and obvious answer Comptia wants is C
upvoted 1 times

  **Thejphall** 1 year, 10 months ago

SSO with biometrics would still be simpler in this case as it removes the need to remember a password in the first place.
upvoted 9 times

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

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

Correct Answer: B

  **Fuzm4n** Highly Voted 1 year, 10 months ago

Selected Answer: C

BEST way to remove it completely is to reinstall the OS
upvoted 18 times

  **bigdaddyzaddy** Highly Voted 6 months, 3 weeks ago

Selected Answer: C

Professor Messer explained this thoroughly. Root kits can embed themselves within the kernel of the operating system itself turning it into a core piece of the os. Therefore, it's able to hide from other applications that may be running on top of the operating system. So even if you're running anti-malware software, that software would have no idea that a rootkit is installed on your system... There's no way B can be the right answer
upvoted 7 times

  **Philco** Most Recent 3 days, 3 hours ago

Selected Answer: C

Reinstall Windows
If the rootkit is deeply embedded, you might need to reinstall Windows using a clean install from an external media.
upvoted 1 times

  **SixGoddess** 1 month, 3 weeks ago



Selected Answer: C

THE ANSWER IS C
upvoted 1 times

  **Jay23AmMonsIV** 3 months ago

Selected Answer: C

Here's why this is the best approach:
Thorough Removal: Rootkits are designed to hide their presence and can be extremely difficult to detect and remove. They often operate at a low level in the system, making them resistant to many traditional anti-malware tools.
System Integrity: Reinstalling the operating system ensures that any rootkit, along with any other potential malware or system modifications, is completely removed. This restores the system to a known good state.
Prevention of Future Issues: A clean OS reinstallation eliminates any potential backdoors or malicious code that a rootkit might have installed, providing a fresh start and reducing the risk of re-infection.
While anti-malware software can be effective against many threats, rootkits are particularly insidious and may evade detection. Application updates and file restores do not address the root cause and may not be effective against rootkits. Therefore, an OS reinstallation is the most reliable method to ensure the rootkit is completely removed.
upvoted 2 times

  **igorclapa** 5 months, 3 weeks ago

Selected Answer: C


C.

If you suspect a rootkit on your device, it's so over. You have to reinstall your OS.
upvoted 1 times

  **yutface** 6 months ago

Selected Answer: C

Anti malware programs do not get rid of rootkits. IT 101. Reinstall OS everytime. I do it at work all the time.
upvoted 1 times

  **simjay93** 6 months, 3 weeks ago

a root kit should be removed by file restore ,the answer has to be D
upvoted 1 times

  **ScorpionNet** 8 months, 3 weeks ago

Selected Answer: C

Reinstalling the operating system will be more effective than the antivirus software because rootkits often bypass the antivirus scan making it difficult for the antivirus to remove it. To those that are getting into cybersecurity, these are referred as black hat hackers.

upvoted 4 times

  **Raffaello** 9 months ago

Selected Answer: C

A rootkit is software used by cybercriminals to gain control over a target computer or network. Rootkits can sometimes appear as a single piece of software but are often made up of a collection of tools that allow hackers administrator-level control over the target device

upvoted 1 times

  **Chavozamiri** 9 months, 1 week ago

Selected Answer: B

B. Anti-malware software I will go with this option because the question says SUSPECT so have a doubt and need make sure better install anti-malware to scan to make sure...

upvoted 2 times

  **mohdAj** 9 months, 3 weeks ago

Selected Answer: C

The BEST resolves the issue is C - OS reinstallation

upvoted 1 times

  **Psyc00** 10 months, 1 week ago

Selected Answer: B

B. Anti-malware software

Rootkits are a type of malware, and using reputable anti-malware software is the most effective way to detect and remove them. Anti-malware software is specifically designed to identify and eliminate malicious software, including rootkits. It's important to ensure that the anti-malware software is up to date and comes from a trusted source.

While application updates (Option A) and OS reinstallation (Option C) are important security practices, they may not be sufficient to remove a rootkit that has already infiltrated the system. Restoring files (Option D) is unlikely to resolve a rootkit issue because the rootkit typically infects the system at a deeper level.

upvoted 2 times

  **Paula77** 11 months, 3 weeks ago

Selected Answer: B

Rootkits are a type of malware that embeds itself deeply into the operating system, making them difficult to detect and remove. Specialized anti-malware software, often referred to as "anti-rootkit" tools, are designed to detect and remove rootkits from a system. These tools are specifically engineered to identify and eliminate the hidden and malicious components of rootkits.

While other measures like OS reinstallation or file restore might be necessary in severe cases, using anti-malware software is typically the first and most effective step to take when dealing with a suspected rootkit infection.

upvoted 7 times

  **willyww** 1 month, 3 weeks ago

please don't comment no sense answers that confuse the community, the answer is C "emekus" is right

upvoted 1 times

  **Emekus** 10 months, 1 week ago

A rootkit embeds itself in the....wait for it....root of the OS and it very likely to be undetected as the Antimalware runs after it has done its business. It takes control of the MBR/GPT so whatever scans you run, isn't going to find it. ALWAYS the answer to rootkits is OS reinstallation...ALWAYS.

23 years of dealing with rootkits here.

upvoted 8 times

  **TMFCJR** 11 months, 3 weeks ago

Selected Answer: C

If there is a rootkit, wouldn't the best option to be to reinstall the os, keeping files but adding new install of your device.

upvoted 2 times

  **ConqiD** 12 months ago

Selected Answer: B

What if I think I have a rootkit on my device?

Microsoft security software includes many technologies designed specifically to remove rootkits. If you think you have a rootkit, you might need an extra tool that helps you boot to a known trusted environment.

Microsoft Defender Offline can be launched from the Windows Security app and has the latest antimalware updates from Microsoft. It's designed to be used on devices that aren't working correctly because of a possible malware infection.

System Guard in Windows 10 protects against rootkits and threats that affect system integrity.

upvoted 1 times

  **[Removed]** 1 year ago

ANSWER C

On Windows, removal typically involves running a scan. If there is a deep infection, the only way to remove the rootkit is by reinstalling Windows. It

is better to do this via an external media device instead of using the built-in Windows installer. Some rootkits infect the BIOS, which will require a repair to fix. If you still have a rootkit after a repair, you may need to get a new PC.

upvoted 1 times

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

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

Correct Answer: A

  **Fuzm4n** Highly Voted  1 year, 10 months ago

Selected Answer: B

AES stronger than TKIP. It was definitely around 10 years ago.
upvoted 13 times

  **[Removed]** 1 year, 5 months ago



Yeah and there is also call firmware upgrade so everthing settles aes it is
upvoted 3 times

  **chattykathy241** Most Recent  4 months, 4 weeks ago

i think its tkip because again the router is older and wpa2 is probably the most recent the router can handle
upvoted 1 times

  **Mr_Tension** 5 months, 1 week ago

WPA2 with AES/TKIP encryption was introduced to the market in 2004. compare to AES and TKIP , AES is more secure. on the other side, WPA3 was officially introduced to the market in June 2018 which is not 10 years old yet. so correct answer is (B) WPA2 with AES
upvoted 1 times

  **igorclapa** 5 months, 3 weeks ago

Selected Answer: B

If the router is 10+ years old, very likely it doesn't support WPA3. Like others have said, AES is more secure than TKIP.
upvoted 1 times

  **Raffaello** 9 months ago

Selected Answer: B

The protocol used by WPA2, based on the Advanced Encryption Standard (AES) cipher along with strong message authenticity and integrity checking is significantly stronger in protection for both privacy and integrity than the RC4-based TKIP that is used by WPA.
upvoted 1 times

  **Chavozamiri** 9 months, 1 week ago

WPA was initially released in 2003. The Wi-Fi Alliance defined WPA as a response to serious weaknesses found in the WEP protocol. A more secure version, WPA2, was released in 2004.
upvoted 1 times

  **Chavozamiri** 9 months, 1 week ago

Selected Answer: B


WPA2 with AES
upvoted 1 times

  **mohdAj** 9 months, 3 weeks ago

Selected Answer: B

If the router is about ten years old, it may support WPA2 with AES. AES (Advanced Encryption Standard) is a common encryption method that was widely adopted even before the introduction of WPA3. Therefore, the answer would be:

B. WPA2 with AES
upvoted 1 times

  **edgaro482** 1 year ago

Selected Answer: A

In old soho routers, I dont think the AES was avaliale. So Im chose a A.
upvoted 1 times

  **Stanoh** 1 year ago

B. WPA2 with AES.

WPA2 (Wi-Fi Protected Access 2) with AES (Advanced Encryption Standard) is a secure option that was widely used during the time period when the router was manufactured. It offers a good balance between security and compatibility with older hardware.

WPA3 was introduced after 2013 and may not be supported by routers manufactured before that time. While WPA3 with AES-256 (option C) is the most secure option among those listed, it's unlikely to be compatible with a router of this age.

It's worth noting that WPA2 with TKIP (option A) should be avoided whenever possible, as TKIP is a less secure encryption method compared to AES.

upvoted 2 times

  **Jimbojkd** 1 year ago

C. WPA3 with AES-256

For the most secure wireless network possible, the technician should configure the router to use WPA3 encryption with AES-256 (option C). WPA3 is the latest and most advanced security protocol for wireless networks, offering enhanced protection compared to older standards like WPA2. AES-256 (Advanced Encryption Standard with a 256-bit key) is a strong encryption algorithm that provides a high level of security for data transmitted over the wireless network. This combination of WPA3 and AES-256 will help ensure that the wireless network is well-protected against various types of attacks.

upvoted 1 times

  **I_Know_Everything_KY** 1 year ago

You need to read questions more closely: the key part is "10 years ago" - thats why the answer is (B) - WPA with AES

upvoted 4 times

  **ZioPier** 1 year, 3 months ago

Selected Answer: A

Well... I think this is not a recent question. However, once a standard has come up, doesn't mean that is immediately covering every devices in production since then. Is likely that the Router would not support AES

upvoted 2 times

  **DonnieDuckoe** 1 year, 4 months ago

AES = Advanced Encryption Standard
TKIP = Temporal Key Integrity Protocol

upvoted 4 times

  **b33avix** 1 year, 4 months ago

depends when the question was written...

upvoted 4 times

  **Gridlin** 1 year, 7 months ago

Answer is B

upvoted 1 times

  **1Abel1** 1 year, 7 months ago

Surprisingly, D is the correct answer (WPA3 with AES-128). Kindly, do your research and you will be supper amaze. WPA 2 AES encryption is now considered old standard.

upvoted 1 times

  **[Removed]** 1 year, 7 months ago

It states the router is 10 years old. There would be compatibility issues with WPA3

upvoted 8 times

  **CTE_Instructor** 1 year, 7 months ago

"Kindly, do your research and you will be supper amaze. "

No comment other than... Do a search on the release date of WPA3, then re-read the question.

WPA2 with AES is the correct answer.

upvoted 20 times

  **Riderzz** 1 year, 7 months ago

WPA3 wasn't introduced till 2018, The question says that the router is 10 years old. WPA2 with AES was still around back then. Answer is B.

upvoted 7 times

  **Nick40** 1 year, 8 months ago

Selected Answer: B

AES was around in 2012. its wpa aes

upvoted 1 times

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

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

Correct Answer: D

  **Fuzm4n** Highly Voted 1 year, 10 months ago

Selected Answer: D

Since msconfig is really a thing anymore, it will tell you to go to the startup tab of the task manager.
upvoted 5 times

  **[Removed]** Highly Voted 1 year, 10 months ago

Selected Answer: D

I think the answer is D. There is no reason to go into the registry to disable programs on startup when all you have to do is disable the programs from the startup tab. I've done it before and it's quick and easy, and I've never had to use the registry for this task.
upvoted 5 times

  **Chavozamiri** Most Recent 9 months, 1 week ago

Selected Answer: D

Open the Startup tab and methodically disable items currently listed as enabled and reboot, checking for issue resolution at each startup.
upvoted 1 times

  **IconGT** 1 year, 4 months ago

Selected Answer: D

D. Open the Startup tab and methodically disable items currently listed as enabled and reboot, checking for issue resolution at each startup, would be the best solution for the technician to selectively prevent programs from loading at startup. This option allows the technician to easily see which programs are causing the excessive boot times and selectively disable them. Right-clicking the Windows button and entering shell:startup and moving items one by one to the Recycle Bin could be time-consuming and potentially cause issues if important system files are deleted. Remark out entries listed in the registry could be risky and may cause issues if the wrong entries are modified. Manually disabling all startup tasks currently listed as enabled and rebooting may not be efficient and could potentially disable important system processes.
upvoted 4 times

  **ronniehaang** 1 year, 6 months ago

Selected Answer: D

To selectively prevent programs from loading on startup in a Windows 10 machine, a technician should open the Startup tab and methodically disable items currently listed as enabled, and then reboot the machine, checking for issue resolution at each startup. Therefore, Option D is the correct answer.

The Startup tab can be accessed through the Task Manager by following these steps:

Right-click on the Taskbar and select Task Manager from the context menu.

Click on the Startup tab.

Methodically disable items currently listed as enabled by right-clicking on the item and selecting Disable from the context menu.

Reboot the machine and check for issue resolution at each startup.

By disabling items in the Startup tab, the technician can selectively prevent programs from loading on startup and check for issue resolution. The process of disabling each item one by one allows the technician to identify which program is causing the excessive boot times.

upvoted 4 times



  **ronniehaang** 1 year, 6 months ago

Option A is not the best choice as it involves manually moving items one by one to the Recycle Bin, which can be a time-consuming and inefficient process.

Option B is not the best choice as it involves modifying the Windows Registry, which can be risky if done incorrectly and should only be done by experienced technicians.

Option C is not the best choice as disabling all startup tasks currently listed as enabled may not help the technician to identify which program is causing the issue.

upvoted 4 times

  **Aerials** 1 year, 10 months ago



Selected Answer: D

D seems like the correct answer.
upvoted 4 times

  **PIEBENG** 1 year, 11 months ago

Selected Answer: B



The correct answer is B
upvoted 3 times

  **Antwon** 1 year, 10 months ago

Absolutely not. Why would you do that? You can simply disable which processes are activated at startup via task manager.
upvoted 5 times

  **BustaSkull3** 1 year, 10 months ago

Can you explain please?
upvoted 1 times

  **takomaki** 1 year, 7 months ago

Its not recommended to change the registry for a simple task like disabling a startup program. Editing the registry should be a last resort (aside from reinstalling windows that is)
upvoted 2 times

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.

Correct Answer: D



  **ArcticSkies** Highly Voted  1 year, 11 months ago

Selected Answer: C

The user is asking how to run an update, so tell them how to run an update.


If the company blocks normal users from manually running updates then you would inform them about the patch day update but that wasn't in the question. The question simply said that a user is asking how to run a Windows 10 update.

upvoted 17 times

  **Aerials** 1 year, 10 months ago

Users should not be changing or updating their own workstations.

upvoted 1 times

  **Antwon** 1 year, 10 months ago

Why not? There is no mention that the user is in an enterprise environment.

upvoted 11 times

  **CTE_Instructor** 1 year, 7 months ago

I'm just imaging some retired person living alone getting that response from a call center tech. "Sorry grandpa, you should not be changing or updating your own workstation".

Let the user know how to use his own device unless the question specifically mentions organizational policies.

upvoted 10 times

  **CodeOnTren** Most Recent  1 month, 1 week ago

Selected Answer: C

User asking how to update windows , even if an automatic patch is upcoming the user may have to do it manually , very rare cases if automatic updates are disabled .

upvoted 1 times

  **SecNoob27639** 1 month, 3 weeks ago

Selected Answer: C

CompTIA will be tricky with questions. They want you to try to pull in information that they didn't say. So, only take your decision making data from the question.

In this case, no where in the question does it mention that "your company sends out patches automatically every month," or even say that the technician is working for an "internal call center/help desk." Because CompTIA doesn't provide any information about what company policies might or might not be, go with the simplest answer. Tell the user how to check for updates.

Within my own org, our updates on our network don't go directly to the Microsoft update server. Our org is large enough that they run their own update server, on top of the software center that is normally used to manage updates and software. And yet, if someone called in to my desk asking how to check for updates, I would give them much the same directions as C.

upvoted 3 times

  **newbytechy** 6 months, 1 week ago

I think I get what the question is asking. Basically it's just stating "call center." Now this call center can just be a regular Windows call center, like Microsoft Support and the user is just a normal user asking how would they update windows on their computer. It doesn't say anything regarding a corporate environment or an employee calling in, it just says user. If that's the case it would be C.....a patch is usually released to address critical security vulnerabilities or other major issues after an update, if there are any issues found. So it would not be D because the user isn't calling in about any issues.

upvoted 1 times

  **d74ad00** 6 months, 2 weeks ago

Selected Answer: C

The only answer

upvoted 1 times

  **Hus1Saad** 8 months, 4 weeks ago

Selected Answer: C

The customer is asking how to run an update, and as a support person we should answer his enquiry.

Support center help the customer not instruct the customer what to do. However, if there is a company policy in the call center that advise this answer it will be just an advise and if the customer insisted on knowing how to update the agent must comply ...

I want to clarify, why D is the right answer? is that just the website option or it is confirmed that CompTIA will use answer D ?? because i may need to reconsider what courses I will be studying in the future

upvoted 2 times

Chavozamiri 9 months, 1 week ago

Selected Answer: D

D. Advise the user to wait for an upcoming, automatic patch

BECAUSE IS WINDOWS not a smartphone, why he wants to update windows before everybody else?

upvoted 2 times

mohdAj 9 months, 3 weeks ago

Selected Answer: C

his guides the user to access the Windows Update settings to manually check for updates. This is a standard procedure for users to initiate the update process on their Windows systems. The other options, such as suggesting an iPad, requesting the user to text their password, or advising to wait for an upcoming automatic patch, are not recommended or relevant to the user's request for updating Windows.

upvoted 1 times

solaWONDER 1 year, 2 months ago

the answer is C

upvoted 1 times

hmnna 1 year, 2 months ago

Selected Answer: C

I think the question is meant to test if you know how to quickly get to windows update. So no need to complicate it.

upvoted 3 times

thechief121 1 year, 3 months ago

The trick behind this one i think is not to think too corporate minded, it doesn't say what the user is that's calling, when they say call centre it could well be one of those tech support premium rate lines?. so i'm going to say C too on one.

upvoted 1 times

Gaurabdon 1 year, 4 months ago

Selected Answer: C

Without any other extra information on whether the client on an enterprise environment, the answer is without a doubt Option C.

upvoted 1 times

[Removed] 1 year, 7 months ago

D should be done if there is no available updates at the time, answer has to be C.

upvoted 1 times

alexandrasexy 1 year, 8 months ago

Selected Answer: C

C. Ask the user to click in the Search field, type Check for Updates, and then press the Enter key.

upvoted 1 times

Nick40 1 year, 8 months ago

Selected Answer: C

Tell the user how to update like he asked. there's no indication that this user is in a corporate setting. The answer is C

upvoted 3 times

cobbs 1 year, 9 months ago

Selected Answer: C

Inform the user. If it is blocked, then it will let them know. Normally updates in an organization come from an internal update server anyway.

upvoted 2 times

Rockrl 1 year, 9 months ago

Selected Answer: C

C is the best answer, read the question carefully, which states "The call Center Technician receives a call", this doesn't which indicates that this is just a regular user who wants to know how to update Windows

upvoted 2 times

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

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

Correct Answer: D

  **oatmealturkey** Highly Voted 1 year, 4 months ago

Selected Answer: C

This question was on my exam and I did not get anything wrong in this objective, so C is the right answer.
upvoted 11 times

  **Pookie717** 1 year, 4 months ago

You're positive about this?
upvoted 1 times

  **oatmealturkey** 1 year, 4 months ago

Yes. I only missed in a couple of objectives and this was definitely not one of them.
upvoted 2 times

  **Miloucha** 6 months ago

did you get some of these questions in your exam beside this one ? Thank you so much
upvoted 1 times

  **bconiglio** Highly Voted 1 year, 7 months ago

Selected Answer: C

Giving the user a ticket number, while helpful to them, would do nothing to correctly associate that ticket with the user in the system. The answer should be C, as it will actually associate the ticket in a formal way.
upvoted 11 times

  **Philco** Most Recent 6 days, 3 hours ago

Selected Answer: D

just a logic option
upvoted 1 times

  **JMLorx** 3 weeks, 5 days ago

Selected Answer: C

The key word here is "associated with".
If they gave them the ticket number they can check up on it yes but this would not help the problem being associated with that specific person
upvoted 1 times

  **CodeOnTren** 1 month, 1 week ago

Selected Answer: D

Unique ticket number should be the correct answer , is easier to find and helpful for future use
upvoted 1 times

  **SixGoddess** 1 month, 3 weeks ago

Selected Answer: C

ANSWER IS C
upvoted 1 times

  **d74ad00** 6 months, 2 weeks ago

Selected Answer: D


Both options C and D could effectively ensure that the ticket is associated with the correct user. However, option D specifically mentions providing the user with a unique ticket number for future reference, which may offer more clarity and ease of communication for both the user and the technician. Therefore, option D may be considered slightly more comprehensive in terms of ensuring accurate ticket association and facilitating subsequent communication. D
upvoted 2 times

  **MikeGeo** 5 months, 2 weeks ago

I see your perspective; but I disagree with your thought process. I believe that D is dependent on C being done.

I believe the answer is C because you can't do D without C being done first. You can't give a unique ticket ID to a customer without first generating the unique ticket ID.

upvoted 2 times

  **Hus1Saad** 8 months, 4 weeks ago

Selected Answer: D

D

unique ticket number not unique user number

unique ticket number will identify it as a new ticket. New ticket will have all the information (assumably)



This kind of silly questions with missing information is annoying

upvoted 3 times

  **Mango7** 11 months ago

so which answer do we have more vote on? C or D? and can someone plz explain, thank you so much.

upvoted 1 times

  **FT786** 11 months, 2 weeks ago

D. Provide the user with a unique ticket number that can be referenced on subsequent calls.

Providing the user with a unique ticket number allows for clear and unambiguous reference to the specific issue they reported. This ticket number can be used by both the technician and the user to track the progress of the issue, provide updates, and ensure that any follow-up calls or inquiries are related to the same problem. It also helps in maintaining a record of the issue for documentation and tracking purposes.


upvoted 2 times

  **Fannan** 1 year ago

Selected Answer: D

Every incident should have a ticket opened. The ticket is associated with the user who is having the issue.

upvoted 1 times

  **ZioPier** 1 year, 3 months ago

Selected Answer: D

I work in a factory. Alecerytime I need it assistance, I go on the portal and follow a process to raise my needs and a Request For Change.

Since there the It department will open a Ticket with a unique number. That is that simple. Nothing more. No number is assigned to me. Just tickets. The ticket will be open until my acceptance of problem solved.

upvoted 1 times

  **BigBrainLogic** 1 year, 4 months ago

Selected Answer: C

"One of the first things you're going to see is information about the user. When a user contacts the support desk, they may do that by phone, email, or chat, or by submitting a ticket through an online portal. In any of these cases that user has to be associated with that ticket, so they're going to be associated with a given user account or user record. This may be based on their phone number, their email, their first name, their last name, their employee ID, or some other piece of identifying information. Whenever a new ticket is created it's going to be tied back to that user, and that way you could see a history of everything that user has ever had issues with, so you can better support them."

-Jason Dion

The answer is C.

upvoted 7 times

  **IconGT** 1 year, 4 months ago

Selected Answer: C

C. Register the ticket with a unique user identifier would be the best practice for the technician to use to make sure the ticket is associated with the correct user. This unique user identifier could be the user's name, employee ID number, or other unique identifier that the organization uses.

Having the user provide a callback phone number could help with follow-up communication, but may not be enough to ensure that the ticket is associated with the correct user. Assigning the ticket to the department's power user or providing the user with a unique ticket number that can be referenced on subsequent calls may not be helpful in ensuring that the ticket is associated with the correct user.

upvoted 2 times

  **Gaurabdon** 1 year, 4 months ago

Selected Answer: D

Option C can be correct if the same user had multiple tickets beforehand we create a new ticket for her. However, it is not the case here (not explained). Unique ticket is automatically generated by the ticketing system unless you use 1900s ticketing system. To make sure that the ticket is associated with the correct user, you simply provide them with the ticket number generated and whichever technician deals with the client next time can simply ask for the ticket number and look at his/her details.

upvoted 5 times

  **StrawberryTechie** 1 year, 4 months ago

I think the answer is D. If it was C, there could be more than one ticket under that person's identifier. A support ticket number would take the support technician and customer straight to the problem being worked on.

upvoted 1 times

  **oatmealturkey** 1 year, 4 months ago

For the purposes of this question it doesn't matter if there is more than one ticket under a user identifier, it is simply asking how to associate a ticket with the correct user.

upvoted 2 times

  **nonzerocrowd** 1 year, 4 months ago

Selected Answer: D

C wouldn't be correct because you can already look up the user by email and phone number in a normal environment.

upvoted 1 times

  **oatmealturkey** 1 year, 4 months ago

Well exactly, a phone number or email address would count as a "unique user identifier". C is correct, it was on my exam and I know from my results that I couldn't have gotten it wrong.

upvoted 3 times

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

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

Correct Answer: D

  **Fuzm4n** Highly Voted 1 year, 10 months ago

Selected Answer: D

Too humid can make things sweat. Too dry can cause static.
upvoted 10 times

  **igorclapa** Most Recent 5 months, 3 weeks ago

Selected Answer: D

D.

Too dry = potential for static discharge, no bueno
Too wet = equipment gets damp/moist...also no bueno
upvoted 1 times

  **ScorpionNet** 1 year ago

Selected Answer: D

D is correct. Hot temperatures can cause corrosions and cold temperatures can cause (ESD) Electrostatic Discharge. It's very important especially as a network and systems administrator to make sure the minimum humidity levels stay at 45% to 50%. It doesn't only go for servers but also on network devices.
upvoted 1 times

  **IteratE** 1 year, 3 months ago

Selected Answer: D

Based on the answers from everyone which is D. I wonder how a tech considers what is the best temperature inside a data center?
upvoted 2 times

  **Banana8891** 1 year, 6 months ago

The question states environmental concern. So shouldn't that be considered when answering the question?
upvoted 1 times

  **Jcsimple** 1 year, 6 months ago

You should always consider temp in an office setting.
upvoted 1 times

  **yutface** 6 months ago

Temp isn't mentioned at all. Only humidity.
upvoted 1 times

  **Rafid51** 1 year, 6 months ago

Data centers generate a significant amount of heat
upvoted 1 times

  **Rafid51** 1 year, 6 months ago

Selected Answer: D

ta centers generate a significant amount of heat
upvoted 2 times

  **yutface** 6 months ago

People, humidity does not equal heat. Heat is not mentioned.
upvoted 1 times

  **Porygon** 1 year, 10 months ago

Selected Answer: D

explain please
upvoted 1 times

  **BigBilly** 1 year, 8 months ago

Too much or too little moisture in the air can damage computer components so humidity levels are a concern. Everything else is more of a luxury and not as necessary

upvoted 4 times




Question #19

Topic 1

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

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

Correct Answer: A

  **JollyGinger27** Highly Voted  1 year, 7 months ago

Selected Answer: A

A little Googling tells me the problem is to check the certificate.

upvoted 10 times

  **Raffaello** Most Recent  8 months, 4 weeks ago

Selected Answer: A

Expired digital certificates can cause a network outage or downtime incurring adverse effects on an organization's network and functionality. Digital certificates like TLS/SSL certificates play a crucial role in the smooth functioning of your website.

upvoted 2 times

  **Chavozamiri** 9 months, 1 week ago

Selected Answer: A

EAP-TLS requires the use of digital certificates

upvoted 3 times

  **rodwave** 1 year, 1 month ago

Selected Answer: A

EAP-TLS requires the use of digital certificates. Each user and device is issued a unique certificate that is used for authentication during the network login process. Since Digital certificates have an expiration date, the user's certificate likely expired during their extended leave so they can't login. So they just need a new certificate.

upvoted 4 times

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

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

Correct Answer: C

  **[Removed]** Highly Voted  1 year, 10 months ago

Selected Answer: D

This question is a little tricky, but also a little vague. For example, it says the USB drive will be used to transfer 20GB of data, but it doesn't say if that data is one file that is 20GB in size or 20 different files that are each 1GB in size.

However, if we assume that it is a single file that is 20GB then FAT32 is not an option because FAT32 only supports files up to 4GB in size. That rules out A.

If we were transferring data from Linux to Linux we could use ext4, but the question states the data is going from Linux to Windows, so ext4 is not an option because Windows does not support ext4. That is a Linux file system. That rules out B.

Theoretically, C and D could both be correct, as NTFS and exFAT are both supported by Windows and Linux and can be used on USB drives. However, the question is asking which is MOST likely. Since exFAT is the standard for USB Drives (while NTFS is the standard for hard drives) I'm going with D.

upvoted 69 times

  **BD773** Highly Voted  1 year, 10 months ago

C

Explanation:

Explanation:

Since Windows systems support FAT32 and NTFS "out of the box" and Linux supports a whole range of them including FAT32 and NTFS, it is highly recommended to format the partition or disk you want to share in either FAT32 or NTFS, but since FAT32 has a file size limit of 4.2 GB, if you happen to work with huge files, then it is better you use NTFS

upvoted 9 times

  **[Removed]** 1 year, 5 months ago

agreed, I tried that myself most of the movie I copy is 6 to 20 GB that's why I format mine to NTFS, but beware some television can't read NTFS.

upvoted 1 times

  **Philco** Most Recent  2 weeks, 1 day ago

C

you can use the NTFS file system on a USB drive. Here's how to format a USB drive to NTFS in Windows:

Right-click the USB drive

Select Format

In the File system drop-down menu, select NTFS

Click Start to begin formatting

If you chose the Better Performance policy, you'll need to use the Safely Remove Hardware notification to disconnect the device safely

upvoted 1 times

  **Philco** 2 weeks, 1 day ago

C--?

NTFS is compatible with Linux, but only for read/write support. NTFS is a proprietary file system developed by Microsoft and is primarily used on Windows-based systems. However, Linux and BSD can use NTFS read/write support with NTFS3 in Linux and NTFS-3G in BSD.

upvoted 1 times

  **SecNoob27639** 1 month, 3 weeks ago

Selected Answer: D

exFAT is the most "universally" compatible option of the 4.



exFAT covers all the bases. It supports single file sizes in a size range larger than the largest available consumer disk drives, let alone removeable media. In addition, it's generally compatible with Linux, due to being a fairly simple system overall.

FAT32 only supports file sizes up to 4 GB, which may or may not be acceptable for this transfer, as we don't know if it's a single 20 GB file or multiple 4GB or less files. Because it isn't stated, don't assume multiple files, go only with what is supplied. 20GB, so CompTIA probably wants to see that you know FAT32 doesn't work with files greater than 4GB.

ext4 would work with Linux, but I'll be honest, in over 5 years working in IT, I have never formatted a drive ext4 for desktop level use.



NTFS was developed as a primarily "Windows" file format, and while some version of Linux may work with it, there is the chance for compatibility issues.

upvoted 1 times

  **mankun** 3 months, 3 weeks ago

FAT32 is a variant of FAT that uses a 32-bit allocation table, nominally supporting volumes up to 2 TB. The maximum file size is 4 GB minus 1 byte. C

upvoted 1 times



  **jsmthy** 5 months, 2 weeks ago

Selected Answer: D

Write-enabled NTFS on Linux is a relatively recent innovation. The mount utility is far safer now, but most flavors of Linux mounts NTFS as read-only.

ExFAT, on the other hand, has been supported both ways for a much longer period of time.

upvoted 3 times

  **GOOF** 2 months, 1 week ago

I agree. The question asked which file system the technician is most likely to use. This begs for an answer that accommodates the most use-cases. "Most likely" style questions are asking for the average correct response, not the best response for a particular scenario.

upvoted 1 times

  **Alworth** 7 months ago



GUYS THE ANSWER IS NTFS ,C

upvoted 1 times

  **Ndebele_5** 8 months ago

exFAT is a file system introduced by microsoft in 2006 an optimized for flash drives such as USB flash drivesan sd cards .

upvoted 1 times

  **Waldem** 8 months, 2 weeks ago

To transfer data from a Linux computer to a Windows computer, you can use the exFAT file system. This file system is supported by both Linux and Windows operating systems and can handle files larger than 4 GB

upvoted 2 times

  **Raffaello** 9 months ago

Selected Answer: D

FAT32 - 32GB or smaller USB/SD card, used on Windows and, Mac, Android phones. NTFS - Windows disk partitions, transfer 4GB+ big files, gaming disk. exFAT - 64GB or bigger external hard drive or USB drives, used on Windows and Mac. EXT4 - Create a Linux partition for a specific environment

upvoted 1 times

  **Chavozamiri** 9 months, 1 week ago

Selected Answer: D

Since we are talking about USB, it is exFAT

upvoted 1 times

  **Psyc00** 10 months, 1 week ago

D. exFAT

exFAT (Extended File Allocation Table) is a filesystem that is compatible with both Windows and Linux and can handle large files and volumes, making it suitable for transferring 20GB of data. It's a good choice when you need a filesystem that works well on both operating systems and can handle large file sizes.

FAT32 (Option A) is an older filesystem that has limitations on file size and is not ideal for large files. ext4 (Option B) is a Linux-specific filesystem and may not be fully compatible with Windows. NTFS (Option C) is a Windows-specific filesystem and may not be the best choice for use with Linux.

upvoted 1 times

  **Nabilrrhmn** 1 year, 1 month ago

Selected Answer: D

NTFS: This is the default filesystem for Windows partitions that offers better performance, security, and reliability than FAT32. NTFS supports journaling, encryption, compression, long file names, access control, etc. However, NTFS is not very compatible with other operating systems and devices. Mac can read NTFS but needs third-party tools to write to it. Linux can also handle NTFS but may have some issues. Many other devices may not support NTFS at all

upvoted 2 times

  **RoPsur** 1 year, 2 months ago

Selected Answer: D

I voted D. The FAT series is compatible with both Linux and Windows. Fat32 supports up to 8TB partition size without having a file bigger than 4GB. The exFAT support 128 Petabytes of partition size, and files can be any size up to that point(128PB). NTFS is more for installing an OS than USB unless you will use it for other consoles. The ext4 file system is not compatible with Windows.

<https://www.howtogeek.com/235596/whats-the-difference-between-fat32-exfat-and-ntfs/>

upvoted 2 times

  **IconGT** 1 year, 4 months ago

Selected Answer: D

D. exFAT would be the most likely filesystem for the technician to use. While FAT32 and NTFS are supported by both Linux and Windows, FAT32 has a 4GB file size limit and NTFS is not natively supported by some Linux distributions. Ext4 is a Linux filesystem and is not natively supported by Windows. ExFAT is supported by both Linux and Windows and does not have the 4GB file size limit of FAT32, making it a good choice for transferring large files.

upvoted 3 times

DonnieDuckoe 1 year, 4 months ago

I have to say D on this one for sure. From Mike Meyers course on Udemy he goes over the different file systems and speaks about how exFAT is best for smaller storage devices like thumb drives because it doesn't have a Master File Table that takes up a bunch of space like on larger storage where you can afford to let that much storage go. ExFAT supports the same file sizes as NTFS and works on both operating systems here.

upvoted 3 times

Question #21

Topic 1

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

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

Correct Answer: C

Raffaello 9 months ago

Selected Answer: C

Why do I need a default app?

If you have more than one app that does the same thing, you can pick which app to use by default. For example, if you have multiple photo editing apps, you can choose which one to use to open a photo

upvoted 2 times

Chavozamiri 9 months, 1 week ago

Selected Answer: C

C. Default Apps

upvoted 2 times

ScorpionNet 1 year ago

Selected Answer: C

Default Apps is correct is just like thinking with the default web browser. We all know Windows uses Internet Explorer (formerly) by default, now it's Microsoft Edge in today's Windows Operating Systems. MacOS used Safari by default, and Linux used Firefox by default. In that case it would be done the same between Edge and Adobe reader.

upvoted 1 times

Guapo1 1 year, 5 months ago

Selected Answer: C

I do it all the time when I imaged a new computer.

upvoted 3 times

Jcsimple 1 year, 6 months ago

Default, plus it asks you to make PDF to Adobe default optional.

upvoted 3 times

alexandrasexy 1 year, 9 months ago

Selected Answer: C

Definitely Default Apps in Windows, correct answer is C.

upvoted 4 times

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

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

Correct Answer: A

CodeOnTren 1 month, 1 week ago

Selected Answer: B

it says windows 10 so i would assume is Indexing Options , in windows 11 i think they have changed this
upvoted 1 times

jade290 2 months ago

Selected Answer: A

I found the option to exclude folders under "Privacy & security" -> "Searching Windows" on my Windows 11 PC. Indexing does deal with searching but its seems more like search optimization from what I am reading: <https://support.microsoft.com/en-us/windows/search-indexing-in-windows-10-faq-da061c83-af6b-095c-0f7a-4dfecda4d15a>
upvoted 2 times

danishkayani11 2 months, 3 weeks ago

In Windows 10 there's an option "Privacy & Security>Searching Windows" but "indexing options" might be closely related to the question because its a complete name of the tool and its an old option
upvoted 1 times

newbytechy 6 months, 1 week ago

Answer is B. If you put in YT, How do you exclude an application from windows 10 search? It's a video that shows you the steps.
upvoted 2 times

Iditenaxyigospoda 7 months, 1 week ago

Selected Answer: B

Indexing Options
upvoted 1 times

Raffaello 9 months ago

Selected Answer: B

Using the Indexing Options
To do this, open the Start Menu and type "indexing options" in the search bar. When the Indexing Options window opens, click the "Modify" button. This will take you to the Indexed Locations window. Uncheck the check boxes for the locations you want to disable indexing for, then click "OK"
upvoted 2 times

Chavozamiri 9 months, 1 week ago

Selected Answer: B

"Indexing Options"
upvoted 1 times

mohdAj 9 months, 3 weeks ago

Selected Answer: B

To exclude an application folder from being catalogued by a Windows 10 search, you would typically use the "Indexing Options"
upvoted 2 times

Julirige 1 year ago

Selected Answer: A

If you check your privacy setting there is an option available to exclude folders from being searched.
upvoted 3 times

I_Know_Everything_KY 1 year ago

This is wrong. In windows 10, Privacy does not influence search indexing.



The correct answer is B.

upvoted 6 times

  **sinfulhymn** 1 year ago

Selected Answer: B

Who the hell is marking the answer like a dumbass on these questions. its indexing for christ sake
upvoted 4 times

  **AsapRocky241** 10 months, 3 weeks ago

Hahahaha
upvoted 2 times



  **DawBroSav2000** 1 year ago

I have been using this site for a bit. By not providing the correct answer/s to every question it has force me to open a browser to confirm therefore, gain more knowledge. Whether accident or on purpose. I find this format helpful for me to pass certifications.
upvoted 9 times

  **Mehsotopes** 1 year, 1 month ago



Selected Answer: B

This is definitely B, you modify your options under Indexing Options found in control panel. Check boxes of what you want shown, and uncheck boxes of what you don't want shown.
upvoted 2 times

  **tutita** 1 year, 5 months ago

Selected Answer: B

its B, you can hide or show the folders
upvoted 1 times

  **CryptX** 1 year, 9 months ago

Selected Answer: B

It's B
upvoted 1 times

  **cpaljhc** 1 year, 9 months ago

<https://www.groovypost.com/howto/hide-files-folders-from-search-windows-10/>
It says indexing options to hide files
upvoted 3 times

  **cooldude0901** 1 year, 10 months ago



Selected Answer: B

The answer is B
upvoted 4 times

  **simsbow1098** 1 year, 11 months ago

Selected Answer: B

Indexing Options
upvoted 4 times

  **RJ4** 1 year, 11 months ago

Privacy settings govern what usage data Windows is permitted to collect and what device functions are enabled and for which apps. There are multiple settings toggles to determine what data collection and app permissions are allowed:
Data collection allows Microsoft to process usage telemetry. It affects use of speech and input personalization, language settings, general diagnostics, and activity history.
App permissions allow or deny access to devices such as the location service, camera, and microphone and to user data such as contacts, calendar items, email, and files.
upvoted 3 times

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

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

Correct Answer: A


  **[Removed]** Highly Voted  1 year, 9 months ago

Selected Answer: A

Answer is A. Praise the Lord himself, Professor Messer.
https://youtu.be/d9bUZGvcTK8?list=PLG49S3nxzAnna96gzhJrzki4hH_mgW4b&t=225
 upvoted 12 times

  **Kristheitguru** 1 year, 5 months ago

In the video , you have screensaver and screen timeout as two different options so your not clicking screen saver to do this you will click screen-timeout
 upvoted 1 times

  **max12553** 2 weeks, 3 days ago

But the questions refers to sleep or inactivity. Sleep is from inactivity.
 upvoted 1 times

  **jt1623262727** Most Recent  5 months, 2 weeks ago

Selected Answer: A

Screen Timeout:

This is a power saving feature.
 After a set period of inactivity (like using the mouse or keyboard), the screen turns off entirely to conserve energy.
 It offers no security on its own. Anyone can walk up and see what was on your screen before it timed out.
 Screen Saver:

This can be both a visual treat and a security measure.
 After a set period of inactivity, it kicks in and displays images, animations, or even slideshows on your screen.
 Optionally, you can set a password for the screen saver, so it requires login to see what was on the screen before it activated.
 upvoted 1 times

  **Raffaello** 9 months ago

Selected Answer: A

A screensaver is a computer program that can be set to turn on after a period of user inactivity (when you leave your computer). It was first used to prevent damage to older monitors but is now used as a way to prevent viewing of desktop contents while the user is away.
 upvoted 1 times

  **Chavozamiri** 9 months, 1 week ago

Selected Answer: A

A. Use Settings to access Screensaver settings.
 upvoted 1 times



  **Mehsotopes** 1 year, 1 month ago

Selected Answer: A

Go to personalization, lock screen, and screen saver settings at the bottom of lock screen. In this dialog-box you will find a check-box that asks if on resume, you want to display the log in screen; if checked, this will lock your computer once screen saver is activated.
 upvoted 1 times

  **princedarcy** 1 year, 1 month ago

While this is accurate, the screen only locks after a period of inactivity and after not a period of sleep. That is done from Settings > Accounts > Sign-in options > scroll down to additional settings > If you've been away, when should Windows require you to sign in again? > the options being Never or When PC wakes up from sleep.
 upvoted 1 times

  **hmnna** 1 year, 2 months ago

Selected Answer: A

Answer should be A. I tried to set a screensaver password on my computer but failed. It does not show a logon screen.

upvoted 1 times

  **Babi_12** 1 year, 4 months ago

Answer is A

upvoted 1 times

  **Thejphall** 1 year, 10 months ago

I keep trying to lookup solid info for this question but the answers I find don't match any available choices. (Like I don't see the options here mentioned anywhere else that explains how you would go about doing something like what's mentioned in the question.)

If I had to guess I would assume it would be screen timeout settings but, personally I'm not seeing the specific options to configure when going to any of the available choices.

upvoted 4 times

  **OnA_Mule** 1 year, 10 months ago

You can try it yourself on a Windows host. Go to Settings and find Screen Saver Settings. On the Screen Saver page, there's a Check Box "On resume, display logon screen" which forces you to log in.

upvoted 4 times

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

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

Correct Answer: D

  **IconGT** Highly Voted 1 year, 4 months ago

Selected Answer: D

D. Enabling BitLocker To Go with a password that meets corporate requirements would be the best way to secure the current workflow. BitLocker To Go is a built-in encryption feature in Windows that can be used to encrypt removable storage devices such as USB drives. By enabling BitLocker To Go with a password, the data on the USB drive will be encrypted and can only be accessed with the correct password, which meets the compliance officer's requirement for media at rest to be encrypted. Deploying a secondary hard drive with encryption or requiring files to be individually password protected may not be as secure or practical for the company's workflow. Configuring a hardened SFTP portal for file transfers may be a good solution for future transfers, but may not be the best solution for the company's current use of USB drives.

upvoted 7 times

  **Chavozamiri** Most Recent 9 months, 1 week ago

Selected Answer: D

Enable BitLocker To Go with a password that meets corporate requirements.

upvoted 1 times

  **mohdAj** 9 months, 3 weeks ago

Selected Answer: D

BitLocker To Go is a Microsoft Windows feature that allows encryption of removable storage devices such as USB drives. By enabling BitLocker To Go and setting a password that meets corporate requirements.

upvoted 1 times

  **Nick40** 1 year, 8 months ago

Selected Answer: D

It's obviously D

upvoted 2 times

  **dimeater** 1 year, 9 months ago

Selected Answer: D

Company wants to stick with USB but also have encryption and security with the files.

upvoted 2 times

  **cooldude0901** 1 year, 10 months ago

Selected Answer: C

I think it's C

upvoted 1 times

  **[Removed]** 1 year, 9 months ago

That would be annoying and tedious because workers would have to enter a password for every protected file. The better option (and the correct answer) is D. They are using USB drives and are RESISTANT to change. BitLocker to Go is Microsoft's way of encrypting USB drives, and other answers would go against the corporation's preference of being resistant to change.

upvoted 9 times

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

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

Correct Answer: B

  **Paradox_Walnut** Highly Voted 1 year, 9 months ago

Selected Answer: B

The `cat` command on Linux concatenates files together. It's often used to concatenate one file to nothing to print the single file's contents to the terminal. This is a quick way to preview the contents of a text file without having to open the file in a large application

Source: <https://www.redhat.com/sysadmin/linux-bat-command#:~:text=The%20cat%20command%20on%20Linux,file%20in%20a%20large%20application.>
upvoted 9 times

  **Aggelos312** Highly Voted 1 year, 7 months ago

Selected Answer: B

The command "`cat`" displays the content of a file.
upvoted 8 times

  **Raffaello** Most Recent 9 months ago

Selected Answer: B

The `cat` command is mostly used in Linux and other operating systems. The `cat` command is called `cat` as it is used to concatenate files. For example, to display the contents of a file, use `cat filename.txt`, to view the large file, use `cat filename.txt | more`
upvoted 1 times

  **Chavozamiri** 9 months, 1 week ago

Selected Answer: B

B. The contents of the text `comptia.txt` would be displayed.
upvoted 1 times

  **ScorpionNet** 1 year, 4 months ago

Selected Answer: B

The answer is B. TestOut has the lab that has you create a file on Linux. The `cat` command will display the given text by the file name. It will display what you entered in the file using the `vi` command.
upvoted 1 times

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

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

Correct Answer: B



  **007madmonk** Highly Voted 1 year, 8 months ago

Selected Answer: B

It's B

<https://www.professormesser.com/free-a-plus-training/220-1102/220-1102-video/privacy-licensing-and-policies-220-1102/>

upvoted 12 times

  **Pegi** 1 year, 2 months ago



Thanks for the reference. B is absolutely the correct answer

upvoted 3 times

  **HUSBULLA** Highly Voted 1 year, 5 months ago



husbulla the goat

upvoted 8 times

  **6e49f75** 7 months ago

HUSBULLA! Hope everyone passes their core 1 and 2 exams! Passed my core 1 and currently studying for core 2. Going to take it tomorrow!!

upvoted 4 times

  **Doveta1ls** 6 months, 3 weeks ago

6e49f75 how did it go! I have mine in two days!

(Also B)

upvoted 2 times

  **Chavozamiri** Most Recent 9 months, 1 week ago

Selected Answer: B

bit-for-bit copy or a byte-for-byte copy(CLONE) will preserve the evidence.

upvoted 1 times

  **mohdAj** 9 months, 3 weeks ago

Selected Answer: B

B. Clone any impacted hard drives

upvoted 1 times

  **paobro** 1 year, 4 months ago

B

And as the first responder, you may be responsible for collecting any evidence and ensuring that no evidence is destroyed during this process. It's very common when collecting this evidence to get a copy of any storage drives. When taking this evidence, we're not simply copying the files, we're copying every single bit of information from that storage drive. You'll sometimes hear this referred to as a bit-for-bit copy or a byte-for-byte copy.

That means you're not only collecting all of the files, you're also collecting anything else that might be on that storage device. We'll sometimes perform this drive copy by physically removing the drive from the device. We will then connect it to a hardware write blocker that would prevent anything from changing the data that's on that storage drive. We can then make a copy of that drive by using a hardware copying device or by using software imaging tools that can create the copy for us

Professor "GOD" Messer

upvoted 5 times

  **CruzBruzzz** 1 year, 8 months ago

Selected Answer: B

B because you can't tamper with evidence. Cloning is the only option.

upvoted 4 times

  **CruzBruzzz** 1 year, 8 months ago

I stand corrected, after research on this question I believe A is the correct answer. That is because he is trying to preserve the files. How else would you preserve it? You can encrypt the file to protect anyone getting into the files. Maybe also provide a hash to to verify any changes of

the file. I believe A is the correct option. B wouldn't make sense because even if you clone the files you just made copies and those copies can easily be modified (not preserved). I would go with A.

upvoted 4 times

  **Paradox_Walnut** 1 year, 9 months ago

Selected Answer: A

Wouldn't the answer be "A"? Since the incident handler would want to "preserve the evidence"?

upvoted 4 times

  **cmarks05** 1 year, 8 months ago

By encrypting the files you altered the evidence

upvoted 10 times

  **Paula77** 11 months, 3 weeks ago

By encrypting the files you are protecting not preserving the files. The question is asking what is the best way of "preserving" which is cloning.

upvoted 1 times

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

- A. Full
- B. Differential
- C. Off-site
- D. Grandfather-father-son

Correct Answer: B

  **TKW36** Highly Voted  1 year, 10 months ago

Selected Answer: B

I think it is B because it specifically states "storage space is a concern" and GFS is storage heavy. Also only a few files are modified frequently, so differential is the best for that.

upvoted 9 times

  **takomaki** Highly Voted  1 year, 7 months ago

Selected Answer: C

Its Offsite and here's why. Yes storage space is a concern. However, offsite backups generally dont mean you get another data center and use it for backups. In most cases, offsite refers to the cloud. For a ransomware target, its getting more common for them to infect the whole network, and its likely backups will be affected as well. Cloud storage is also very cheap if you only need to backup a few files. GFS has offsite backups, but at least some are on site, and that's more prone to ransomware and uses more storage (Otherwise whats the point of the generations?) Differential backups and full backups dont protect against ransomware in any particular way, so they dont address all the concerns, especially since they arent backup methods, but instead types of backups.

upvoted 8 times

  **MikeGeo** Most Recent  5 months, 2 weeks ago

I disagree with the majority. I think the answer is C



The question has two concerns: Ransomware attacks & File size.

The question does state they they only back up a few files; but they still specifically stated that storage space is a concern. If it were incremental instead of differential I would be more inclined to think that was the answer, but I think differential doesn't meet the concern of minimizing file size. Also, GFS is very file heavy so that's out.

In regard to Ransomware attacks, I think that B, C, and D cover that issue adequately.

So we're left with B or C; and I still think that C addresses the file size concern, where B does not.

upvoted 2 times

  **Lance711** 7 months ago

Selected Answer: C

I'm going with offsite. There is another option that would clear this up, but CompTIA likes have 2 answers this close. A good answer is Differential. A better answer is Offsiet. The BEST answer is Offsite Differential. Therefore, I believe it's offsite.

upvoted 2 times

  **Raffaello** 9 months ago

Selected Answer: B

Differential backups only backup files that have been modified or added since the last full backup. This method reduces the storage space used and offers protection against ransomware attacks, as it allows for full system restoration without the need to access recent versions of potentially infected files

upvoted 1 times

  **Chavozamiri** 9 months, 1 week ago

Selected Answer: B

Differential backups are a good choice for mitigating ransomware attacks and addressing the specified concerns because they only back up the files that have changed since the last full backup. This means that they are efficient in terms of storage space as they do not require the storage of duplicate data. In the event of a ransomware attack, you can restore to the last full backup and then apply the most recent differential backup to recover the changed files.

upvoted 1 times

  **Psyc00** 10 months, 1 week ago

Selected Answer: B

B. Differential

Differential backups are a good choice for mitigating ransomware attacks and addressing the specified concerns because they only back up the

files that have changed since the last full backup. This means that they are efficient in terms of storage space as they do not require the storage of duplicate data. In the event of a ransomware attack, you can restore to the last full backup and then apply the most recent differential backup to recover the changed files.

Full backups (Option A) store all the data, which can consume a lot of storage space over time. Off-site backups (Option C) are important for disaster recovery but do not specifically address the concerns related to ransomware mitigation. Grandfather-father-son (Option D) is a retention policy for managing multiple backup sets over time but doesn't inherently mitigate ransomware attacks.

upvoted 2 times

  **BigBrainLogic** 1 year, 4 months ago

I disagree with the majority of people here, I think it's off-site, because the best backup solution for ransomware is stored off-site.

upvoted 6 times

  **IconGT** 1 year, 4 months ago

Selected Answer: B

B. Differential backup method would be the best backup method that would best address these concerns. Differential backups only back up files that have been modified since the last full backup, which means only a few files that are regularly modified will be backed up. This minimizes the backup size and storage space needed, while still ensuring that recent modifications are backed up in the event of a ransomware attack. Additionally, differential backups can help mitigate the risk of data loss from ransomware attacks because they only backup modified files, reducing the chances of backing up encrypted files. Full backups would be too large for the amount of data being regularly modified, while off-site and grandfather-father-son backup methods do not address the specific concerns about backup size and ransomware mitigation.

upvoted 1 times

  **BigBrainLogic** 1 year, 4 months ago

Selected Answer: B

A differential backup backs up all the files that have been modified since the last full backup. This method saves storage space compared to full backups, as it only backs up the changes made. This option provides a balance between storage space usage and protection against ransomware attacks. Off-site backup refers to the physical location of the backup storage, not the backup method itself. While it's a good practice to store backups off-site to protect against disasters, it doesn't directly address the storage space concern mentioned in the scenario. Grandfather-father-son is a backup rotation scheme rather than a backup method

upvoted 1 times

  **ronniehaang** 1 year, 6 months ago

Selected Answer: B

A differential backup method would be the BEST option in this scenario. Differential backup takes a full backup of the system initially and then backs up only the changes that have been made since the last full backup. This method saves both time and storage space compared to a full backup. Additionally, differential backups provide an advantage in the event of a ransomware attack as only the changes made after the last full backup will be affected, making it easier to restore the unencrypted data. Off-site and grandfather-father-son backup methods refer to the storage location and backup rotation schedule, respectively, and are not directly related to mitigating ransomware attacks.

upvoted 4 times

  **Rafid51** 1 year, 6 months ago

Selected Answer: B

differential backup will be smaller than a full backup of the entire system, as it only captures changes and not the entire system.

upvoted 1 times

  **LeLouch7** 1 year, 7 months ago

there are only three types..full, incremental & differential

upvoted 1 times

  **wepaid** 1 year, 7 months ago



B is incorrect. The differential backups will contain an increasing amount of data which may exhaust the storage space. Grandfather-father-son backup method would be a more efficient solution in this scenario because it uses a rolling window of backups, allowing only a certain number of backups to be kept at any given time, which can help with storage space concerns. Therefore answer is D.

upvoted 1 times

  **1Abel1** 1 year, 7 months ago

D is correct "Grandfather-father-son" because it can mitigate ransomware attacks based on the fact that a copy "Grandfather" can be saved offsite.

upvoted 2 times

  **examtopics11** 1 year, 9 months ago

Selected Answer: B

GFS is a backup strategy similar to 3-2-1, not a method of backup.

upvoted 3 times

  **CritterForDinner** 1 year, 10 months ago

I don't think GFS is the correct answer because it will take up much storage space. Differential would be more conducive to conserving space.

upvoted 3 times

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

Correct Answer: A

  **Porygon** Highly Voted  1 year, 10 months ago

Selected Answer: A

The reasoning is as follows: The question states that while the technician is troubleshooting a customer's PC, the technician receives a phone call [most likely not from the customer]. This can either be assumed or not, but should not change the outcome. The main issue is what follows. The technician sets the phone to silent, and continues with working. THIS is what the question is asking for. CompTIA wants to know what the technician did.

The technician silenced the phone to avoid distractions while troubleshooting.

B and C are both very similar, but unless the technician is receiving a video call while troubleshooting customer's personal data, they [B and C] do not apply.

And D is not applicable because we cannot assume that a timeline was ever set or needs to be met. Because there is not enough info, and/or the question is only asking for an explanation of what the technician did by silencing the phone.

Therefore the answer is A. Avoid distractions.

upvoted 6 times

  **Raffaello** Most Recent  9 months ago

Selected Answer: A

Unlike the airplane mode, the silent mode still allows the device to receive and send calls and messages. This quiet option may be useful in meetings, speeches, libraries, museums, or places of worship. In some places it is mandatory to use the silent mode or to switch off the device.

upvoted 1 times

  **mohdAj** 9 months, 3 weeks ago

Selected Answer: A

A. Avoid distractions

By not taking the phone call and setting the phone to silent while troubleshooting a customer's PC, the technician is demonstrating an effort to avoid distractions and maintain focus on the task at hand. This is important for providing efficient and effective technical support.

upvoted 1 times

  **ScorpionNet** 1 year ago

Selected Answer: A

A is correct. The technician avoided any kinds of distractions while troubleshooting a customer's computer. The phone call could be from a friend or a scammer. It's best to take it when you are on break or off work hours. Taking the call while on the job is a red flag as it will reduce productivity.

The technician did the right thing to silence the phone to avoid getting distracted from helping out the customer.

upvoted 2 times

  **IconGT** 1 year, 4 months ago

Selected Answer: A

A. Avoid distractions would be the best description of the technician's actions. By setting the phone to silent and not taking the call, the technician is minimizing distractions and maintaining focus on the task at hand, which is troubleshooting the customer's PC. While dealing appropriately with customer's confidential material, adhering to user privacy policy, and setting and meeting timelines are all important aspects of a technician's job, they are not directly related to the action of setting a phone to silent to avoid distractions.

upvoted 1 times

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

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

Correct Answer: D

  **ronniehaang** Highly Voted  1 year, 6 months ago

Selected Answer: D

The tool that can be used to transfer a large number of files over an unreliable connection and resume the process if the connection is interrupted is "robocopy."

Robocopy, which stands for "Robust File Copy," is a built-in command-line tool in Windows that is used to copy files and folders from one location to another. It provides various options that can be used to customize the copying process, including the ability to resume file transfers if they are interrupted.

upvoted 13 times

  **ronniehaang** 1 year, 6 months ago

To transfer files using robocopy, the technician can open a Command Prompt window and use the robocopy command with the appropriate parameters. For example, the following command can be used to copy files from the source directory to the destination directory and resume the copying process if it is interrupted:

```
robocopy source destination /Z /S /W:5 /R:2
/Z: Copy files in restartable mode (resumes if interrupted)
/S: Copy subdirectories, but not empty ones
/W:5: Wait 5 seconds between retries
/R:2: Retry twice if the transfer fails
```

upvoted 6 times

  **Raffaello** Most Recent  9 months ago

Selected Answer: D

Robocopy is a powerful command-line tool for Windows that allows users to synchronize files and folders from one location to another

upvoted 1 times

  **mohdAj** 9 months, 3 weeks ago

Selected Answer: D

Robocopy (Robust File Copy) is a command-line utility in Windows that is well-suited for copying large amounts of data with options for resuming in case of interruptions and handling unreliable connections.

upvoted 1 times

  **Mehsotopes** 1 year, 1 month ago

Selected Answer: D

Robocopy allows you to copy data between networks, or using long NTFS file names. The modifiers allow you to choose what data you want to transfer, and set automation with archive attributes.

upvoted 1 times

  **alexandrsexy** 1 year, 9 months ago

Selected Answer: D

Robocopy is the best way to copy large amounts of files even over unreliable connections.
The correct answer is D. robocopy

upvoted 1 times



  **CritterForDinner** 1 year, 10 months ago

Robocopy is noted for capabilities above and beyond the built-in Windows copy and xcopy commands, including the following, some requiring appropriate command-line options:

-Ability to tolerate network interruptions and resume copy

<https://en.wikipedia.org/wiki/Robocopy>

upvoted 1 times

  **Aerials** 1 year, 10 months ago

Robocopy, for "Robust File Copy", is a command-line directory and/or file replication command for Microsoft Windows. Robocopy functionally replaces Xcopy, with more options.

upvoted 3 times

Question #30

Topic 1

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

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

Correct Answer: A

  **musicartspeaks** 1 year, 1 month ago

Selected Answer: A

Needs to get the bigger files transferred and backed up first.



upvoted 1 times

  **[Removed]** 1 year, 9 months ago

Selected Answer: A

The answer is A. Not only is it common sense (backup all of your data first in case you lose data with other backup methods), but it is also initially required for the other backup methods listed to be implemented properly.

upvoted 4 times

  **Aerials** 1 year, 10 months ago

A full backup takes the most time and resources, but should be completed first, in case the faster and less reliable ones fail.

upvoted 4 times

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

Correct Answer: C

  **Kristheitguru** Highly Voted 1 year, 5 months ago

Its not always ChatGPT has the correct Answer, i have tried that for my Core 1 exam half weren't right it.
upvoted 24 times

  **RyeBread** 7 months ago

Agreed. Not sure why people are relying on ChatGPT. Input the question with the answers and see how ChatGPT answers. Then submit the same question with the answers and you may notice ChatGPT will apologize and give another answer. Keep doing it and it will just go back and forth. I recommend not relying on ChatGPT for studying for this reason.
upvoted 6 times

  **doctordoom** Highly Voted 1 year, 7 months ago

Selected Answer: D

D. Firewall

I've been using ChatGPT to verify some of these answers on this site and i highly recommended trying it out. I trust it a lot more than random peoples opinions on the internet. I fed it the full question and possible answers.

A firewall is a security feature that monitors and controls network traffic and can be used to block or allow communication between an application and the internet. By configuring a firewall on the user's smartphone, the user will be alerted when an application attempts to communicate with the internet and can take action accordingly.

A firewall can be set to notify the user when an app tries to access the internet, allowing the user to review the app's request and decide if they want to allow or block it.

Option A and B are not addressing the user's concern, as operating system updates and remote wipe are not related to monitoring and controlling the internet access of the application. Option C is related to security but it's mainly focused on detecting and removing malware and it doesn't have the ability to monitor and control network traffic as a firewall does.

upvoted 15 times

  **amityGanoofib** 5 months, 4 weeks ago

just wanted to say, ChatGPT composes its answers from a mix of articles and random peoples opinions on the internet, so it can be hit or miss.
upvoted 1 times

  **CodeOnTren** Most Recent 1 month, 1 week ago

Selected Answer: D

I choose D too , but since the question is about "Smartphone" the correct answer would be C is a tricky one and is exactly what CompTIA wants
upvoted 1 times

  **GOOF** 2 months, 1 week ago

D. Firewall:

The purpose of a firewall is to allow/deny/log/notify network traffic. The purpose of antivirus is to allow/deny/log/notify code execution or file access. Antivirus which include network protection is just a fancy way of saying it includes a signature-based firewall. Not all antivirus possess this whereas all firewalls do.

upvoted 1 times

  **Jayysaystgis** 3 months ago

Answer is D. Compare the functions between a Firewall and Antivirus on Google
upvoted 1 times

  **Mr_Tension** 5 months, 1 week ago

mate, read the question. it's saying (user would like to be alerted). Antivirus won't alert you if an application goes to communicate with internet. you can set these rule only with firewall

upvoted 2 times

  **jsmthy** 5 months, 2 weeks ago

Selected Answer: D

Both antivirus and firewall are able to view the network traffic of a device.

However, a firewall fundamentally runs on a lower level than an antivirus and will catch hidden data usage outside of the user jail.

upvoted 2 times

Alpha_Secure 5 months, 3 weeks ago

I believe D is correct and examtopics.com purposely selects the wrong answer to make it more controversial and make us interact.

upvoted 3 times

Poppy16 5 months, 4 weeks ago

Can someone explain if the correct answer is the the most voted one? Or if it's what is listed as the correct answer

upvoted 3 times

MikeGeo 5 months, 3 weeks ago

I believe the answer is D [Firewall].

I think this because the question asks for an alert when an app attempts to contact the internet. This would be something that a Firewall would do; monitor apps and notify when an app is trying to reach the internet.

Now, I think that the app (which is trying to reach the internet) would have some sort of virus or similar in it, and an antivirus would be the course of action to remove the virus; but even if that's what is happening, that's not what the question is asking for.

Unless I'm wrong about a Firewall being able to monitor when an app reaches out to the internet... but this is my thought process regardless.

upvoted 1 times

jmcd2 6 months ago

Selected Answer: C

The answer is C chapGPT stinks and isnt the answer to everything

<https://quizlet.com/735337169/220-1102-flash-cards/>

upvoted 1 times

jmcd2 6 months ago

Also what phone has a firewall?

upvoted 1 times

yutface 6 months ago

Selected Answer: D

Messer:

ery rarely would an application need to have inbound access to one of our mobile phones or tablets. That's one of the reasons why running a firewall on a phone or tablet is not the default, and usually a firewall is not included with those operating systems. However, you may be able to find a firewall available in your favorite App Store. Most of these are available on the Android operating system, but none of them seem to be widely used across the board.

upvoted 1 times

newbytechy 6 months, 1 week ago

D.

Explanation: A firewall acts as a barrier to block unauthorized access to and from a NETWORK (<--keyword in question) or system, while antivirus software detects and removes malicious software (malware) on a device.

upvoted 1 times

Iditenaxyigospoda 7 months, 1 week ago

Selected Answer: D

Antivirus software is important for protecting a device from malware, some antivirus solutions might offer insights into app behavior. They are generally not focused on monitoring or controlling internet access for individual apps like a firewall would.

On smartphones, some firewall applications can alert the user when an app tries to connect to the internet. This would directly address the user's concern by providing real-time information about which apps are attempting to transmit data.

upvoted 1 times

Raffaello 9 months ago

Selected Answer: D

An Android smartphone may be configured with a firewall software programme to track and manage incoming and outgoing network traffic. In addition, by regulating internet access for individual apps and protecting against cyber threats, firewalls can provide an additional layer of security for Android devices

upvoted 2 times

Chavozamiri 9 months, 1 week ago

Selected Answer: C

I believe Mobile phones don't have firewall, al antivirus have firewall built -in

upvoted 1 times

Psyc00 10 months, 1 week ago

Selected Answer: D

D. Firewall

A firewall allows the user to monitor and control network traffic, including communication between applications and the internet. By setting up firewall rules and notifications, the user can be alerted when an application tries to access the internet, giving them control over which apps are allowed to transmit data.

While operating system updates (Option A) are important for overall device security, they may not provide the real-time monitoring and control needed in this case. Remote wipe (Option B) is a feature that allows you to erase the data on a lost or stolen device but doesn't address the issue of monitoring app data usage. Antivirus (Option C) focuses on malware detection and removal but may not provide the specific feature of alerting the user about application data usage. A firewall is the most suitable solution for this specific concern.

upvoted 1 times

  **INEEDTOSTUDYMORE** 10 months, 3 weeks ago

it is firewall. just read it in the comptia a+ study guide book page 1261

upvoted 1 times

Question #32

Topic 1

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

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

Correct Answer: D

  **Newfy123** Highly Voted  1 year, 7 months ago

Selected Answer: D

-it mentions "in case of theft" so not data in transit (that would be data moving during a transaction)
-It says its a workstation, so no USB drive involved most likely a regular HDD
-why only encrypt certain files when you can encrypt the whole drive and deny access to everything in case of theft.

upvoted 16 times

  **willyww** Most Recent  1 month, 3 weeks ago

Selected Answer: D

D is the most logical



upvoted 1 times

  **ibn_e_nazir** 6 months ago

Selected Answer: D

It is a point of sale transaction system but all the transactions are saved on the local HDD for day to day reports generations, so it means sensitive data is still there on the hard drive with credit card and other sensitive information. in case of theft, this data can be retrieved and used illegally. Full disk encryption can avoid this possibility.

upvoted 1 times

  **JermQ** 1 year, 7 months ago

Can someone explain why it is D?

upvoted 1 times

  **Joelashu** 1 year, 5 months ago

because we securing the whole workstation in case of thief simple.....

upvoted 8 times

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

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

Correct Answer: AF

  **PatrickH** Highly Voted  1 year, 8 months ago

Its absoluly A and F. You shouldnt block the ads, you should remove them. Its almost certainly a proxy redirect so resteeing browser and running antivirus best solution.

upvoted 20 times

  **dbo98** Highly Voted  1 year, 10 months ago

Selected Answer: CF

I don't see how A would be an option because of, "The user thought the company-provided antivirus software would prevent this issue." So what would running the anti-virus software do? Plus it states that it is a Pop-up as soon as they open the browser.

upvoted 11 times

  **StrawberryTechie** 1 year, 4 months ago

Pop ups can be adware. And adware is still considered malware.

upvoted 3 times

  **ropea** 11 months, 4 weeks ago

It didn't catch the malware in real time (active scan). but that doesn't mean a full system scan wouldn't find it.

upvoted 3 times

  **glenpharmd** 1 year, 1 month ago

He thought the company provided anti - virus software. Therefore, does not know for sure if they have it or used it. So run an anti- virus software

upvoted 2 times

  **a87d6a4** Most Recent  3 weeks, 5 days ago

Selected Answer: CF

Question is asked what is most likely to RESOLVE the issue. F remains a top recommendation because it directly targets the root cause (browser hijacking or unwanted extensions that are causing the pop-ups.).

C might be more immediately effective than scanning with the current antivirus software, given the scenario. This would prevent the pop-ups from appearing in the first place, especially if they're caused by malicious ads or scripts.

These steps directly address the issue and are likely to prevent further occurrences. Scanning with antivirus software is still valuable but might be secondary in resolving the immediate problem of pop-ups.

upvoted 1 times

  **CodeOnTren** 1 month, 1 week ago

Selected Answer: AF

its A and F , the reason why the antivirus didnt work is because is a false alarm luring the person into paying the ad so as long as the antivirus is aware the computer is not effected is a simple AD pop up

upvoted 1 times

  **Dat_Oyin** 1 month, 1 week ago

AC screen for virus then block AD

upvoted 1 times

  **goss_6087** 2 months, 2 weeks ago

Companies have strict protocols, therefore A-F would be a no brainer

upvoted 1 times

MikeNY85 2 months, 3 weeks ago

A pop-up blocker would prevent pop-ups from appearing, but it won't remove the adware or malware causing this. I think the most appropriate action here is to A and F, since C won't remove the adware (it'll just prevent the pop-ups from showing).

upvoted 2 times

Jay23AmMonsIV 3 months ago

Selected Answer: AC

While resetting the web browser can sometimes resolve issues related to browser settings or extensions, it may not address the underlying cause of the pop-up messages, which is likely malware or adware.

Therefore, scanning the computer with the antivirus software and deploying an ad-blocking extension to the browser are the most appropriate steps to take in resolving the issue.

upvoted 1 times

Ryan_0323 5 months ago

Selected Answer: AF

I was originally CF but im changing my answer to AF because i feel like its common sense to always run the anti virus software in a situation like this.

upvoted 1 times

amityGanoofib 5 months ago

Selected Answer: AF

i dont usually vote but i gotta for this one, you gotta run that antivirus, i wasnt sure whether c or f would be better for the second answer but i think resetting the browser after running the antivirus might do a bit better than using an ad blocker.

upvoted 1 times

Avengers_inc 5 months, 2 weeks ago

Selected Answer: AC

I just want to honestly understand why resetting the browser is even on your mind????

upvoted 3 times

jsmthy 5 months, 2 weeks ago

Selected Answer: AF

If the browser is infected, always check with a malware scan because a separate program (often marked on antivirus programs as a PUP) may be injecting the browser with the adware.

An ad-blocking program only targets the current site meaning it won't help against a PUP or a messed up browser config.

upvoted 1 times

bdemps98 5 months, 3 weeks ago

Selected Answer: AF

I believe the next steps would be A and F, but C would come after those are completed.

upvoted 1 times

taco_security 7 months, 1 week ago

Selected Answer: AF

A and F. You scan as a best practice but the issue is notifications being pushed from web browsers.

upvoted 1 times

za_ck 7 months, 2 weeks ago

Selected Answer: AC

To resolve the issue of pop-ups on a company workstation, the following steps should be taken:

1. Scan the computer with the company-provided antivirus software to detect and remove any malware or viruses that may be present on the system. This is the first step in resolving any security-related issues on a computer.

2. Deploy an ad-blocking extension to the browser to prevent pop-ups from appearing when browsing the web. Ad-blocking extensions can help prevent unwanted ads and pop-ups from appearing on a user's screen, which can help reduce the risk of malware infections.

upvoted 1 times

Gerty2119 7 months, 3 weeks ago

Selected Answer: CF

The question asks which options will most likely RESOLVE the issue. Scanning the system doesn't resolve the issue. Blocking the ads and resetting the web browser actually resolves the issue, whether it's efficient or not doesn't matter in this case.

upvoted 2 times

Raffaello 9 months ago

Selected Answer: AF

Open your Windows Security settings. Select Virus & threat protection > Scan options. Select Windows Defender Offline scan, and then select Scan now

Persistent web page issues may be resolved by clearing your web browser's cache and cookies. If the issue continues, or you have other browser issues, you could also try resetting your browser to its default settings

upvoted 1 times

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

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

Correct Answer: D

  **Raffaello** 9 months ago

Selected Answer: D

On Macs, installer files usually have the extension . pkg (not to be confused with application packages, which usually have the extension . app). Installers are executable files that you can launch by double-clicking on their icon (which may look like a little package).

upvoted 1 times

  **b377us19** 1 year, 3 months ago

A+ Directive 1.10 The wording in the question is a bit misleading but since the install process has already started it would be recognised as an .app file. Before the file is installed it would show as a .pkg file. See Professor Messor Comptia A+ 220-1102 Training Course.

upvoted 3 times



  **jambreaker** 1 year, 5 months ago

The file type that a technician is most likely to use when installing new software on a macOS computer is D. .app.

An .app file is a type of file that contains a packaged application that can be installed on a macOS computer. It contains all of the necessary files and resources that are needed to run the application, and it is designed to be easy to install and use.

On the other hand, .deb is a file format used by the Debian Linux distribution to distribute and install software packages. .vbs is a file extension for VBScript files, which are scripts written in the Visual Basic Scripting language, and .exe is a file extension for executable files in Windows operating systems. These file types are not typically used for installing software on a macOS computer.

upvoted 2 times

  **JollyGinger27** 1 year, 7 months ago

Selected Answer: D

A is used in Linux, B and C are used in Windows, and D is used in MacOS for installed apps. It's D, everyone.

upvoted 3 times

  **007madmonk** 1 year, 8 months ago

Selected Answer: D

It's D


<https://www.file-extensions.org/mac-os-x-file-extensions>

upvoted 2 times

  **alexandrasexy** 1 year, 9 months ago

Actually, none of the provided options is a valid answer.

upvoted 3 times

  **minx98** 1 year, 6 months ago

for real, but D the only one that makes sense

upvoted 1 times

A technician is investigating an employee's smartphone that has the following symptoms:

- ☞ The device is hot, even when it is not in use.
- ☞ Applications crash, especially when others are launched.
- ☞ Certain applications, such as GPS, are in portrait mode when they should be in landscape mode.

Which of the following can the technician do to MOST likely resolve these issues with minimal impact? (Choose two.)

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

Correct Answer: DE

🗳️ 👤 **simsbow1098** Highly Voted 1 year, 11 months ago

Selected Answer: AC

E and F makes the most logical sense for this question because that would be the end all be all solution for this question. However, the question states "minimal impact" making me believe the answers would be A and C.

upvoted 16 times

🗳️ 👤 **Jcsimple** 1 year, 6 months ago

Why would I reinstall an app that is on default settings?

upvoted 2 times

🗳️ 👤 **PathPINGLE** Highly Voted 1 year, 11 months ago

Selected Answer: AC

The question asks for minimal impact so closing unnecessary apps would make sense. None of the other answers would fix the landscape/portrait problem with the phone other than option A.

upvoted 10 times

🗳️ 👤 **CodeOnTren** Most Recent 1 month, 1 week ago

Selected Answer: AC

Minimal impact

upvoted 1 times

🗳️ 👤 **Iditenaxyigospoda** 7 months, 1 week ago

Selected Answer: CE

Close unnecessary applications.

Update the device's operating system.

upvoted 1 times

🗳️ 👤 **Chavozamiri** 9 months, 1 week ago

Selected Answer: AC

I think who answer that was not able to see the word Minimal impact :)

upvoted 2 times

🗳️ 👤 **JBSecurity101** 10 months, 3 weeks ago

Selected Answer: AC

Minimal impact on the device/end-user is the key here.

upvoted 1 times

🗳️ 👤 **KingM007** 1 year ago

Selected Answer: CE

These two answer choices (CE) are going to help you out with 100% of the problem you are facing. Only while answer choice A is going to help you out with 1 of the 3 problems.

upvoted 1 times

🗳️ 👤 **Walide0** 1 year ago

Selected Answer: AC

Turn on autorotate, close any unwanted apps according to minimal impact

upvoted 3 times

  **JBSecurity101** 1 year ago

A & C illicit minimal impact to the user.

upvoted 1 times

  **Fannan** 1 year ago

Selected Answer: AC

Minimal impact: enable autorotation and closing apps would cause the least impact.

upvoted 1 times

  **TungstonTim** 1 year ago

Selected Answer: CE

C. Close unnecessary applications: Closing unnecessary applications can help free up system resources and potentially resolve performance and crashing issues. Background applications can contribute to the device becoming hot and unstable.

E. Update the device's operating system: Outdated operating systems can sometimes lead to performance issues, crashes, and compatibility problems. Updating the operating system can help fix bugs and improve overall stability.

The key phrase in the question is "minimal impact". That is why 'D' is not correct since it would result with the loss of all data.

upvoted 4 times

  **rodwave** 1 year, 1 month ago

Funny how no one can really agree on the answer because the question is honestly just bad and confusing. Classic comptia

upvoted 4 times

  **1T_wizard** 1 year, 1 month ago

Selected Answer: CE

C. Close unnecessary applications: Closing unnecessary applications can help free up system resources, which may cause the device to overheat and lead to application crashes.

E. Update the device's operating system: Updating the operating system can address potential bugs and compatibility issues that may be causing the GPS app to malfunction in portrait mode when it should be in landscape mode. It can also manage other software-related issues that could be contributing to the problems.

upvoted 2 times

  **solaWONDER** 1 year, 2 months ago

the answer is C and E.

upvoted 1 times

  **Delawasp** 1 year, 3 months ago

Selected Answer: CE

The symptoms suggest that the employee's smartphone is experiencing performance issues. Closing unnecessary applications can help free up resources and reduce the strain on the phone's hardware, which can help alleviate the overheating and crashing issues. Updating the device's operating system can also address potential software bugs and security vulnerabilities that could be contributing to the symptoms.

Activating airplane mode would disable all wireless communications on the device, which might not be an ideal solution if the employee needs to use the phone for work purposes. Performing a factory reset would wipe all data and settings on the device, which is a drastic action that should only be taken as a last resort. Reinstalling the specific applications that have crashed may help resolve the issue with those apps, but it may not address the root cause of the overall performance issues. Finally, turning on autorotation may be a minor fix for the portrait/landscape mode issue, but it is unlikely to resolve the other symptoms.

upvoted 1 times

  **IconGT** 1 year, 4 months ago

Selected Answer: CE

C. Close unnecessary applications and E. Update the device's operating system would be the best steps the technician can take to most likely resolve these issues with minimal impact. Closing unnecessary applications can help free up resources on the smartphone, which may be causing the device to become hot and causing applications to crash. Updating the device's operating system can help fix any known issues or vulnerabilities that may be causing the symptoms. Turning on autorotation, activating airplane mode, performing a factory reset, and reinstalling the applications that have crashed may not necessarily address the underlying issue and may even cause additional issues or data loss.

upvoted 1 times

  **I_Know_Everything_KY** 1 year ago

How does updating the OS address the screen orientation issue? You have only dealt with 50% of the problem.

Turning on autorotation would ABSOLUTELY "address the underlying issue".

upvoted 1 times

  **orsopdx** 1 year, 5 months ago

Selected Answer: AC

Definitely A&C. Fix autorotation on apps. It says "especially when other apps are running", implying the user just has too many apps open at once, making the phone run hot and crashing other apps. It specifies minimal impact.

upvoted 3 times

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

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

Correct Answer: C

  **bconiglio** Highly Voted  1 year, 7 months ago

Selected Answer: B

Rolling back patches seems fairly intensive for a first step. A quick hardware check would take a few minutes at most and eliminate some causes of a sudden reboot. I vote B.

upvoted 9 times

  **Rixon** 2 weeks, 4 days ago

Full hardware check takes 10 times longer than rollback. Did you ever try running Memory check on a PC? It can take HOURS.

upvoted 1 times

  **SammsLovesJesus** Most Recent  5 days, 7 hours ago

Selected Answer: C

Windows must have updated and restarted. Therefore patches must have been installed

upvoted 1 times

  **Rixon** 2 weeks, 4 days ago

Selected Answer: C

"after a reboot occurred in the middle of the night." < This is a 100% indicator that the update is the problem here. Everything was working before the update, an update occurred, now it doesn't work. And you guys are voting for Hardware problems? Use your brain.

upvoted 1 times

  **saraperales** 1 month, 1 week ago

Selected Answer: B

It's b

upvoted 1 times

  **stinkle** 1 month, 3 weeks ago

B all the waaaay

upvoted 1 times

  **tthaiana** 2 months, 1 week ago

Selected Answer: B

first step would be to check if everything its alright...

upvoted 1 times

  **GOOF** 2 months, 1 week ago

Windows updates management/troubleshooting are relevant parts of this exam's testing goals. This question specifically states a restart occurred overnight, which is most commonly associated with Windows update performing its work while the computer is most likely to be idle.



upvoted 1 times

  **Alzahrani** 4 months, 3 weeks ago

Selected Answer: C

Sudden restart coming from an updated implementation. So option C is the correct answer for this question.

upvoted 1 times

  **jsmthy** 5 months, 2 weeks ago

Selected Answer: B

Gather information first. Hubris has, can, and will break a good technician.

Assumptions can lead you to reinstall those patches after you realize your hard drive is throwing SMART predictive failure errors.



upvoted 1 times

  **amityGanoofib** 5 months, 3 weeks ago

Selected Answer: B

i would say B cause the first step should involve gathering information not immediately making changes. yes C has you gathering a bit of info but then quickly assuming what the problem is and starting to make changes.



upvoted 1 times

  **keems** 6 months, 1 week ago

Selected Answer: B

this is worded rather peculiar. from my comprehension, the question is asking what the first step of the troubleshooting process is; not to troubleshoot the actual issue. If we were trying to troubleshoot the actual issue, I would say C since we can see that it is obviously software related. HOWEVER, that is not the question therefore my answer is B.

upvoted 1 times

  **DBrega** 6 months, 3 weeks ago

Selected Answer: C

Taking in account the context (reboot at night), the problem is probably software/config related, not hardware.



upvoted 1 times

  **Iditenaxyigospoda** 7 months, 1 week ago

Selected Answer: C

Check for any installed patches and roll them back one at a time until the issue is resolved.

upvoted 1 times

  **nedeajob12** 9 months ago

Selected Answer: B

at first i thought it was C, but being a helpdesk tech for a few years, i def think B is the way to go as a FIRST step. if all hardware seems good, then go ahead and roll back updates

upvoted 1 times

  **JBSecurity101** 10 months, 3 weeks ago

Selected Answer: B

Rolling back windows update patches one at a time is much more intensive and performing a simple CPU/RAM check.

upvoted 1 times

  **Lalauta** 11 months, 1 week ago

B. Run both CPU and memory tests to ensure that all hardware functionality is normal.

When troubleshooting a computer issue, especially one related to performance and application loading problems, it's essential to start with hardware diagnostics to rule out any potential hardware problems. Running CPU and memory tests can help identify if there are underlying issues with the computer's components that may be causing the application loading problems.

upvoted 2 times

  **TungstonTim** 1 year ago

Selected Answer: C

C. Check for any installed patches and roll them back one at a time until the issue is resolved.

The first step in troubleshooting the reported issue with applications not loading properly after an unexpected reboot is to check for any installed patches or updates that might have caused compatibility issues. Rolling back patches one at a time can help identify if any recent update is causing the problem. This approach focuses on the software aspect of the issue, which is likely to be the cause, given that the problem occurred after the reboot.

upvoted 4 times

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

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

Correct Answer: C

  **JollyGinger27** Highly Voted  1 year, 7 months ago



Selected Answer: C

A geofence, alarm system, and motion sensor are all virtually implemented. The badge reader prevents physical access to a building without one.
upvoted 6 times

  **Raffaello** Most Recent  8 months, 4 weeks ago

Selected Answer: B

Video surveillance is employed to monitor physical access to the datacenter and information system. The video surveillance system is linked to the building alarm monitoring system to support physical access monitoring of alarm points
upvoted 1 times

  **Abe_Santi** 8 months, 3 weeks ago

REALLY????! How does video surveillance make any sense to being a solution of preventing physical access to any part of a building? Video will only allow you to monitor access points, not keep people from accessing. The only legit answer to prevent physical access is a badge reader as it is a physical locking mechanism that will not allow the door to be opened without approved access card. And if you're trying to say that someone who is monitoring the cameras are able to allow physical access to people by seeing who they are and can approve it, the person monitoring the screens will still need to push a button of some sort to allow the lock to open to permit access. So again, that still means it's not the video surveillance that is allowing access.
upvoted 3 times

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

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

Correct Answer: AF

  **JBSecurity101** 10 months, 3 weeks ago

Selected Answer: AF

Brute force attack attempts require a password lock-out after a specified number of attempts to mitigate the threat. MFA would provide an extra-layer of security/authentication while mitigating the potential success of a brute-force attack and/or dictionary attack.

upvoted 2 times

  **Xaraa** 1 year ago



Why can't it be A and E. A (multi-factor authentication) would provide extra protection, whereas, E (password manager) will help enable a stronger and more complex password, hence extra security. F (lockout after five bad passwords) makes me wonder what if the password is deciphered on the fourth attempt?

upvoted 1 times

  **CodeOnTren** 1 month, 1 week ago

Well i agree , but if there were no lockout in place , the attacker can try unlimited times

upvoted 1 times

  **tsjr63** 11 months, 2 weeks ago

Because we want to prevent a brute force attack as described in the example.A password manager would be insufficient



upvoted 2 times

  **Mehsotopes** 1 year, 1 month ago

Selected Answer: AF

Only allowing five password attempts disallows an attacker from brute forcing their way into a network/computer system, unless they had a good dictionary attack. Multifactor is always recommended for extra security, whether that extra step is a biometric access (Sometimes considered intrusive), or by a physical control access key, i.e. card badge reader. If both of those answers did not satisfy then having location factor security is a good third option, but attacker would just have to be in the right place.



upvoted 1 times

  **JollyGinger27** 1 year, 7 months ago

Selected Answer: AF

Although B sounds like a sound answer, it won't prevent brute-force attacks from happening anyway and D doesn't replace the remote-access tool entirely, so A and F are the best answers.

upvoted 1 times

  **JollyGinger27** 1 year, 7 months ago

Edit: D doesn't guarantee that a different tool will have better brute-forcing security, too.



upvoted 1 times

  **bconiglio** 1 year, 7 months ago

Selected Answer: AF

I think A and F are correct. While limiting the support tool may help, A and F definitely would, so they're better answers.

upvoted 3 times

  **lilbuu** 1 year, 8 months ago

I thought it was A and F. limit the amount of attempts to gain access and add security measure for authentication

upvoted 2 times

  **victorburst** 1 year, 9 months ago

A and B

upvoted 1 times

 **[Removed]** 1 year, 9 months ago

B is definitely not the answer because now that limits the use of the software inside the corporate network. The question mentions "brute force," which is just repeatedly guessing the password(s) of accounts. So requiring MFA (password + something else) and having account lockouts (e.g., the account is locked out after 5 bad password attempts) would prevent brute force attacks.

upvoted 4 times

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

Correct Answer: D

Aerials Highly Voted 1 year, 10 months ago

Out of these choices, resource monitor will be the most useful in pinpointing which resource is being hogged and what is hogging it.
upvoted 12 times

JBSecurity101 Most Recent 10 months, 3 weeks ago

Selected Answer: D

Resource monitor would provide the technician with the necessary statistics to determine the cause of the slowdown.
upvoted 1 times

TungstonTim 1 year ago

Selected Answer: D

'D' is the correct answer since the question asks how you would go about figuring out the problem. Choosing 'A' is more toward attempting to solve the problem.
upvoted 1 times

HQvRusss 1 year ago

Selected Answer: D

D. Resource Monitor
upvoted 1 times

Nabilrrhmn 1 year, 1 month ago

Selected Answer: D

D. Resource Monitor. This will help the technician monitor and analyze the performance of the computer's CPU, memory, disk, and network in real time.
upvoted 1 times

malek505 1 year, 3 months ago

the question said 'Identity', so as a technician you should investigate the issue by monitoring the resource
upvoted 4 times

ciola89 1 year, 3 months ago

Selected Answer: A

Disk Cleanup is a Microsoft software utility first introduced with Windows 98 and included in all subsequent releases of Windows. It allows users to remove files that are no longer needed or that can be safely deleted. Removing unnecessary files, including temporary files, helps speed up and improve the performance of the hard drive and computer. Running Disk Cleanup at least once a month is an excellent maintenance task and frequency.
upvoted 1 times

[Removed] 1 year, 1 month ago

Its saying to identify not resolve
upvoted 5 times

LePecador 1 year, 3 months ago

Yes, it can help the disk if it's running out of storage or improve performance, but the question is asking to IDENTIFY the cause of WHY the computer is running slow. In that case, D) Resource Manager would help better
upvoted 6 times

Jcsimple 1 year, 6 months ago

A very interesting feature from Win10.
upvoted 1 times

[Removed] 1 year, 5 months ago

Yeah a bunch of useful metrics, just like what you see in aws cloudwatch dashboard.
upvoted 1 times



Upon downloading a new ISO, an administrator is presented with the following string:

59d15a16ce90c8ee97fa7c211b7673a8

Which of the following BEST describes the purpose of this string?

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


Correct Answer: C

[-]  **Aerials** Highly Voted  1 year, 10 months ago
Hashes can be used to compare file integrity
upvoted 8 times

[-]  **mohdAj** Most Recent  9 months, 3 weeks ago

Selected Answer: C

In the context of downloading an ISO file, this string is likely a hash value generated using a hashing algorithm (such as MD5, SHA-256, etc.).
upvoted 2 times

[-]  **JollyGinger27** 1 year, 7 months ago

Selected Answer: C

Hashes are used to verify that the program is legit and from the proper source and not tampered with things like malware.
upvoted 2 times

[-]  **takomaki** 1 year, 7 months ago

Selected Answer: C

Thought it was digital signature for a second because those are used for nonrepudiation, but no, the checksums to verify file integrity generally use SHA hashes, I checked the VirtualBox site.
upvoted 4 times

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

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

Correct Answer: AF

  **trungH** Highly Voted 1 year, 11 months ago

Selected Answer: AE

I would go with A & E. I don't see how GPS spoofing will prevent this
upvoted 19 times

  **Manzer** Highly Voted 1 year, 11 months ago

Selected Answer: AE

Block the 3rd party apps.
upvoted 12 times

  **Jay23AmMonsIV** Most Recent 3 months ago

Selected Answer: AE

A. Prevent a device root: Rooted devices are more vulnerable to malicious applications and potential security threats. By preventing the device from being rooted, the administrator can enhance security and prevent unauthorized access to system resources.



E. Block third-party application installation: Third-party applications pose a significant risk, as they may contain malware or other security vulnerabilities. By blocking third-party application installation, the administrator can ensure that only trusted and vetted applications from official app stores are installed on the device, reducing the risk of malicious software.

Options B, C, D, and F are not directly related to securing the device against the described threat
upvoted 2 times



  **groovynerd** 3 months, 1 week ago

Selected Answer: AE

Blocking the way to go
upvoted 1 times

  **LeoZ456** 6 months, 3 weeks ago

There is one problem with A, the question did not mention whether is an IOS system device or an Android system device. Device root is a term that only works for Android but the question never mentions it. So C E would be a better choice for this question.
upvoted 2 times

  **Lance711** 7 months ago

Selected Answer: AE

A and E. Read the question. The main concern is 3rd party apps and malware that have already been found on the phone. So it's evident that the user is adding 3rd party apps. Again, adding a pin that the user knows and giving him access to install 3rd party apps will on replicate the problem.
upvoted 2 times

  **Iditenaxyigospoda** 7 months, 1 week ago

Selected Answer: AE

A. Prevent a device root.
E. Block third-party application installation.
upvoted 1 times

  **Raffaello** 9 months ago

Selected Answer: AE

Root detection is a security feature to identify whether the restrictions imposed by manufacturers of Android devices have been bypassed and block the 3rd party apps
upvoted 2 times

[-] **Chavozamiri** 9 months, 1 week ago

Selected Answer: AE

I don't see how GPS spoofing will prevent this
Phone uses MDM that means that is company phone probably so A and C
upvoted 3 times

[-] **Grzesiekfrk** 9 months, 3 weeks ago

I have one question to everyone who chose answer A. How exactly are you going to prevent root? I'm curious because I can't find anything about it on Google
upvoted 2 times

[-] **JBSecurity101** 10 months, 3 weeks ago

Selected Answer: AE

GPS spoofing has nothing to do with the issue after the device was reset.
upvoted 2 times

[-] **Ohnononon** 1 year, 4 months ago

zot fou zot. Ena sois pagla, sois latet perdi. Merci
upvoted 1 times

[-] **glenpharmd** 1 year, 2 months ago

write in English
upvoted 7 times

[-] **IconGT** 1 year, 4 months ago

Selected Answer: AC

A. Prevent a device root and C. Require a PIN on the unlock screen would be the best steps the administrator can take to help secure the device against this threat in the future. Preventing a device root can help prevent unauthorized changes to the device's operating system or file system, which can be used to install malicious applications. Requiring a PIN on the unlock screen can help prevent unauthorized access to the device if it is lost or stolen. Disabling biometric authentication, enabling developer mode, and preventing GPS spoofing may not necessarily address the specific threat of malicious applications. Blocking third-party application installation may also be an option, but it may not be practical for some users who need to install legitimate third-party applications.
upvoted 3 times

[-] **Delawasp** 1 year, 3 months ago

This is correct
upvoted 2 times

[-] **8809cb9** 7 months, 3 weeks ago

No it is not. Requiring a PIN does not prevent the user from downloading malicious applications from third party sources, and most certainly would not stop a threat from accessing the device. 3rd party applications not approved and reviewed by the Google Play Store is one of the main components in malicious software gaining access to a device.
upvoted 3 times

[-] **DonnieDuckoe** 1 year, 4 months ago

Can someone please tell me what Device Root is in their own words?
upvoted 2 times

[-] **Besxp** 1 year, 3 months ago

Basically just admin mode on phone.
upvoted 2 times

[-] **ropea** 11 months, 4 weeks ago

and allows the user to install 3rd party apps. It makes it more susceptible to exploits.

In iPhones I believe it's called jailbreaking. and I remember one practice test says that attackers try to find jailbroken phones.
upvoted 2 times

[-] **phanton** 1 year, 4 months ago

The two actions the administrator should take to help secure the device against this threat in the future are:

A. Prevent a device root: Rooting a device can bypass the security measures put in place by the manufacturer or MDM software, making the device vulnerable to attacks.

C. Require a PIN on the unlock screen: This can help prevent unauthorized access to the device in case it gets lost or stolen.

Therefore, options A and C are the correct answers.

Disabling biometric authentication (option B) can make the device less secure as biometric authentication is often more secure than a PIN or password. Enabling developer mode (option D) can also make the device more vulnerable as it can allow unrestricted access to the device's software and settings. Preventing GPS spoofing (option F) is not directly related to securing the device against malicious applications. Option E, blocking third-party application installation, is also a good security measure, but it's not mentioned that the malicious applications were installed from third-party sources.

upvoted 4 times

[-] **8809cb9** 7 months, 3 weeks ago

This is wrong. A is correct but E is the second correct answer. The question is asking about how to prevent the issue of malicious software being added to the device, not about physical unrestricted access to the device. A pin wouldn't stop malware from coming onto a device if it's ran by the user.

upvoted 2 times

  **[Removed]** 1 year, 5 months ago

Selected Answer: AE

sure this

upvoted 2 times

  **[Removed]** 1 year, 5 months ago

Selected Answer: AE

As a previous Mobile Technician, most of the MDM device I work on you can't install third party application, and also can't flash anything on it answer is a and e

upvoted 2 times

  **[Removed]** 1 year, 5 months ago

You can't install thirparty application because they disable developer settings and you can't turn it on.

upvoted 1 times

Question #42

Topic 1

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

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

Correct Answer: B

  **mcneel5** **Highly Voted**  1 year, 7 months ago

Noticed on the 220-1102 test back in January 2023

upvoted 7 times

  **Jay23AmMonsIV** **Most Recent**  3 months ago

Selected Answer: B

Windows 10 Home edition does not support joining a domain. Domain joining capability is a feature typically found in Windows 10 Professional, Enterprise, and Education editions. Therefore, if the laptop has Windows 10 Home installed, it will not be able to join a domain.

Options A, C, and D are less likely to be the cause of the issue

upvoted 1 times

  **Raffaello** 9 months ago

Selected Answer: B

To join a domain on Windows 10, Windows 11, and earlier, you'll need to have the Pro, Education, or Enterprise edition version of the operating system. On a Mac, you can join a domain using the Directory Utility tool.

upvoted 1 times

  **JollyGinger27** 1 year, 7 months ago

Selected Answer: B

According to this Microsoft forum post, you need to upgrade to Windows 10 Pro in order to join a domain:

<https://answers.microsoft.com/en-us/windows/forum/all/how-to-add-windows-10-home-edition-to-a-domain/ec15d3c4-75bb-487b-a58f-9c3135580bed>

upvoted 4 times

  **Jcsimple** 1 year, 6 months ago

And WIn10 Home does not have the join domain or BitLocker.

upvoted 2 times

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

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

Correct Answer: B

  **Jay23AmMonsIV** 3 months ago

Selected Answer: B

Chrome OS is designed by Google and is specifically optimized for lightweight, web-centric computing. It provides a simple and user-friendly interface primarily centered around the Google Chrome web browser. Chrome OS devices, such as Chromebooks, are known for their fast boot times, low system resource requirements, and seamless integration with web-based applications and services.

Options A, C, and D are less suitable for workstations needing a lightweight, browser-based interface
upvoted 1 times

  **Raffaello** 9 months ago



Selected Answer: B

ChromeOS, sometimes styled as chromeOS and formerly styled as Chrome OS, is a Linux-based operating system developed and designed by Google. It is derived from the open-source ChromiumOS and uses the Google Chrome web browser as its principal user interface.
upvoted 1 times

  **Rafid51** 1 year, 6 months ago

Selected Answer: B

Chrome OS is a lightweight operating system that provides a browser-based interface.
upvoted 2 times

  **JollyGinger27** 1 year, 7 months ago

Selected Answer: B



I'm tempted to say A but it's based on Linux (harder to use) and it doesn't come with a browser. The other 2 (C and D) are not lightweight compared to ChromeOS. B is the best answer even if it doesn't sound like it's for workstations.
upvoted 2 times



A user has requested help setting up the fingerprint reader on a Windows 10 laptop. The laptop is equipped with a fingerprint reader and is joined to a domain.



Group Policy enables Windows Hello on all computers in the environment. Which of the following options describes how to set up Windows Hello Fingerprint for the user?

- A. Navigate to the Control Panel utility, select the Security and Maintenance submenu, select Change Security and Maintenance settings, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete.
- B. Navigate to the Windows 10 Settings menu, select the Accounts submenu, select Sign-in options, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete.
- C. Navigate to the Windows 10 Settings menu, select the Update & Security submenu, select Windows Security, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete.
- D. Navigate to the Control Panel utility, select the Administrative Tools submenu, select the user account in the list, select Windows Hello Fingerprint, and have the user place a fingerprint on the fingerprint reader repeatedly until Windows indicates setup is complete.

Correct Answer: B

  **goss_6087** 2 months, 2 weeks ago
Cuz I cheated. Test it yourself - BBBB BBBB
upvoted 1 times

  **JollyGinger27** 1 year, 7 months ago
Selected Answer: B
Like that other comment, just verify it yourself and you will see that it is indeed B.
upvoted 4 times

  **alexandrasexy** 1 year, 9 months ago
Selected Answer: B
Indeed B is the correct answer. Just follow the steps on a Windows 10 pc!
upvoted 4 times

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

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

Correct Answer: C

Antwon Highly Voted 1 year, 10 months ago

Selected Answer: C

Since utilizing the cloud is mentioned here, that does require a good connection and can use a lot of bandwidth
upvoted 7 times

Jay23AmMonsIV Most Recent 3 months ago

Selected Answer: C

toring CAD files on the cloud server will involve uploading and downloading large files over the network. CAD files are typically large in size, and if every file modification triggers a backup to the cloud server, it will result in a significant increase in network utilization. This increased network traffic can potentially lead to slower network performance, congestion, and potential bottlenecks, especially if the firm's network infrastructure is not adequately prepared to handle the additional load.

Options A, B, and D are less likely to be of concern in this scenario
upvoted 1 times

simjay93 6 months, 3 weeks ago

Selected Answer: B

the key word here is manager.
Here are the IT manager roles listed :

1. Strategic Planning
2. Budgeting and Resource Allocation
3. Team Leadership
4. Project Management
5. Vendor Management
6. IT Infrastructure Management
7. Security and Compliance
8. Technology Evaluation and Adoption
9. User Support and Customer Service
10. IT Governance and Risk Management

The answer that is mainly in line with management when there is extra work to be done is B, take consideration of the extra costs and time the technician will have to incur
upvoted 2 times

Raffaello 9 months ago

Selected Answer: C

"Utilization" is the percentage of a network's bandwidth that is currently being consumed by network traffic. Consistently high (>40%) utilization indicates points of network slowdown (or failure) and a need for changes or upgrades in your network infrastructure.
upvoted 1 times

Andy1001 10 months, 1 week ago

The answer is B. He's the manager and he is managing costs and budgets. Please don't hate me for this I think C is the better answer too but that was marked a wrong on my mock test.
upvoted 2 times

JBSecurity101 10 months, 3 weeks ago

Selected Answer: C

Network utilization will be higher as CAD files are very large and will use a lot of network resources.
upvoted 1 times

IconGT 1 year, 4 months ago

Selected Answer: C

C. Network utilization will be significantly increased due to the size of CAD files is most likely to be of concern to the IT manager. The newest version of the CAD software that forces storage of backups of all CAD files on the software's cloud server will likely result in a significant increase in network traffic as the size of CAD files can be very large. This can potentially impact the performance of the network and other applications that rely on it. While all updated software should be tested with all system types and accessories, extra technician hours should be budgeted during

installation of updates, and large update and installation files may overload the local hard drives, these concerns are not directly related to the issue of network utilization caused by the storage of backups of all CAD files on the software's cloud server.

upvoted 2 times

  **lordcheekklappur** 1 year, 5 months ago

Selected Answer: C

its asking what is most likely to be of CONCERN to the IT manager, Not what action to take.

C is the Concern and A is an action they would be taking but it did not say what the IT manager should do.

upvoted 2 times

  **rah555** 1 year, 5 months ago

Selected Answer: C

Network utilization will be significantly increased due to the size of CAD files.

upvoted 2 times

  **1337Minty** 1 year, 5 months ago

Why would it be A??? Look at the question carefully,

"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?"

Makes no sense for the testing to be the most concern if there's already backups on hand, they can rollback if need be. This is a business setting. The network utilization is the MOST concern, there is a business that's running with other users utilizing the network.

upvoted 1 times

  **JJReddic** 1 year, 5 months ago

Selected Answer: A

Why is the answer C for this one? Not too sure but should we test in this situation first before anything?

upvoted 1 times

  **Xzahmed1990** 1 year, 5 months ago

Selected Answer: A

A looks good

upvoted 1 times

  **[Removed]** 1 year, 6 months ago

Selected Answer: A

I have reason to believe that it is A, aren't we supposed to be testing the change before we rollout the upgrades?

upvoted 1 times

  **minx98** 1 year, 6 months ago

Selected Answer: A

Think it's A but can't confirm. C and D are both good but A is the best method

upvoted 1 times

  **minx98** 1 year, 6 months ago

A is most logical

upvoted 1 times

  **minx98** 1 year, 6 months ago

Update: don't know what I was smoking it is definitely C

upvoted 10 times

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

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

Correct Answer: C

  **JollyGinger27** Highly Voted 1 year, 7 months ago

Selected Answer: C

Phishing over the phone is called Vishing according to Professor Messer in one of his videos.
upvoted 12 times

  **mohdAj** Most Recent 9 months, 3 weeks ago

Selected Answer: C

Vishing is a type of social engineering attack where attackers use voice communication, typically over the phone, to trick individuals into providing sensitive information or taking fraudulent actions. In this case, the fraudulent caller is using a pretext to pretend to be from a reputable bank, attempting to deceive the company employee.
upvoted 2 times

  **Sihtrik** 1 year, 1 month ago

Selected Answer: C

Vishing - Voice Phishing (Phishing done over a call)
upvoted 2 times

  **NadirM_18** 1 year, 3 months ago

Answer here is C. Vishing = Voice Phishing (Phishing done over a call)
upvoted 1 times

  **Marioadmin** 1 year, 4 months ago

Selected Answer: A

Is not this Pretexting?
According to google:
What is pretexting? Pretexting is use of a fabricated story, or pretext, to gain a victim's trust and trick or manipulate them into sharing sensitive information, downloading malware, sending money to criminals, or otherwise harming themselves or the organization they work for.
upvoted 1 times

  **Kyle25** 1 year, 4 months ago

Vishing is more specific to this situation -
the fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as bank details and credit card numbers.
upvoted 6 times

  **Marioadmin** 1 year, 4 months ago

You are right.
upvoted 3 times

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

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

Correct Answer: B

  **Rafid51** Highly Voted  1 year, 6 months ago

Selected Answer: B

An account lockout policy sets a limit on the number of incorrect login attempts
upvoted 7 times

  **Philco** Most Recent  3 days, 1 hour ago



Selected Answer: B

An 'Account Lockout' is a critical security feature that disables an account after a defined number of failed login attempts with an incorrect password, aiming to prevent brute-force password guessing attacks.
upvoted 1 times

  **mohdAj** 9 months, 3 weeks ago

Selected Answer: B

B: Account lockout is the best choice for mitigating the threat of a dictionary attack.
upvoted 1 times

  **JollyGinger27** 1 year, 7 months ago

Selected Answer: B

Any better encryption method won't help since a brute-force attack can still guess the password, so A is not the answer. C is not the answer because it has to do with the orientation of the screen. D is not the answer because antiviruses don't have anything to do with brute-force attacks. Therefore, B is the best answer.
upvoted 3 times

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

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

Correct Answer: C

  **wepaid** Highly Voted  1 year, 7 months ago

dfrgui.exe is a built-in tool in Windows that can be used to defragment a hard drive. Defragmenting a hard drive can improve its performance by rearranging the data on the hard drive so that files are stored in contiguous blocks, which can improve the speed at which the data can be read from the drive. When a hard drive is badly fragmented, it can cause the PC to run slowly as the computer has to work harder to access the scattered data. Therefore final answer is C.

upvoted 11 times

  **JollyGinger27** Highly Voted  1 year, 7 months ago

Selected Answer: C

Like the other comment said, the de-fragmentation tool used in Windows runs through dfrgui.exe

Therefore, the answer is C

upvoted 9 times

  **IDTENT** Most Recent  10 months, 4 weeks ago

This one bothers me in that the tech SUSPECTS fragmentation and has therefore completed step 2 of the troubleshooting theory. RESMON feels like a nod to step 3 (test the theory) where running defrag feels like step 4 (Implement the solution)

upvoted 1 times

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

- A. Drilling
- B. Degaussing
- C. Low-level formatting
- D. Erasing/wiping

Correct Answer: B

  **Paradox_Walnut** Highly Voted 1 year, 9 months ago

Selected Answer: B

What is Degaussing? Degaussing is a method of permanently erasing data from working and non-working hard drives, tape, and floppy disks. Degaussing completely sanitizes the media of data in seconds by delivering a powerful magnetic pulse that instantly destroys all magnetic domains on the disk platters.

Source: <https:// GarnerProducts.com/what-is-degaussing#:~:text=What%20is%20Degaussing%3F,domains%20on%20the%20disk%20platters.>
upvoted 11 times

  **No5172685** 1 year, 7 months ago

Degaussing destroys the drive preventing them from being refreshed.
upvoted 3 times

  **Sebatian20** 1 year, 3 months ago

I don't know man, i though drilling be pretty safe as well.
upvoted 2 times

  **IVHoltzmann** 8 months, 3 weeks ago

The data on the parts of the platter that were not drilled is still capable of being read by certain tools. Degaussing is the most secure method of these options.
upvoted 2 times

  **Jayysaystgis** Most Recent 2 months, 2 weeks ago

I wanted to say D. There is the definition of *Resfreshing* on Google In computing, the term "refresh" has multiple meanings:
Reinstalling an operating system
Reinstalling a computer's operating system and updating applications, drivers, and settings can restore a computer's performance and stability. So why use degaussing on a hard drive.it would render it useless.
upvoted 1 times

  **Jay23AmMonsIV** 3 months ago

Selected Answer: D

Erasing or wiping the hard drives involves securely deleting all data stored on the drives using specialized software or tools designed for this purpose. This process ensures that all PII and other sensitive information is effectively removed from the drives, making it unrecoverable by standard data recovery methods.

Drilling: Physically drilling holes into the hard drives can destroy them, but it may not completely ensure that the data is irrecoverable. Skilled individuals or specialized equipment could potentially still recover data from the damaged drives, especially if the drilling is not thorough or if some parts of the disk remain intact.

Degaussing: Degaussing involves using a powerful magnet to disrupt the magnetic fields on the hard drive, effectively erasing the data. While degaussing can be effective for certain types of magnetic media, such as magnetic tapes, it may not work reliably for modern hard drives, which use more complex magnetic storage methods.

upvoted 1 times

  **Arya001** 5 months, 1 week ago

D. Erasing/wiping.

Erasing or wiping the hard drives ensures that the data stored on them is completely removed and cannot be recovered. This process is essential for protecting sensitive information, such as PII, from falling into the wrong hands. Drilling, degaussing, and low-level formatting might not completely destroy the data or could be less reliable methods for ensuring data destruction compared to a thorough erasing or wiping process.

upvoted 2 times

  **Avengers_inc** 5 months, 2 weeks ago

Selected Answer: A



In as much as y'all are saying deguassing, you do realize that option is absolutely useless against SSDs yeah? DRILLING HAS TO BE THE ANSWER!!! It's PII fgs!!! thats extremely sensitive data!

upvoted 1 times

  **axel.chayra** 5 months, 1 week ago

Yeah, good thing the question specifically stated they are HDDs and not SSDs.

upvoted 2 times

  **Ryan_0323** 5 months ago

sometimes they screw with us on the wording but i dont think they would do that in this scenario

upvoted 1 times

  **dangerousDub** 10 months, 3 weeks ago

I think it is honestly, B

Degaussing, since the question Ask how to Dispose of it instead of reusing it.

Degaussing will make it unusable, while Erasing/Wiping the hard drive will still be usable.



upvoted 2 times

  **JBSecurity101** 10 months, 3 weeks ago

Selected Answer: B

Degaussing is the correct method of erasure. Question specifically states the devices in question are hard drives NOT SSDs.

upvoted 1 times

  **Kunjar** 1 year, 3 months ago

Its either A or B definetly not D.

upvoted 1 times

  **ZioPier** 1 year, 3 months ago

Selected Answer: B

Any lessons from any professor I saw about the subject is:

" for HDD the best method for disposal is degassing. This will make any data completely unrecoverable".

One of them said that he personally prefer drilling as it physically destroy and misshape the disk, but the correct answer will always be degassing.

Wiping is only in case the hard disk is meant to be reused

upvoted 1 times

  **Babi_12** 1 year, 4 months ago

what about both. Wiping, degaussing and drilling at the same time to make sure

upvoted 1 times

  **IconGT** 1 year, 4 months ago

Selected Answer: D

D. Erasing/wiping is the best method to dispose of the drives that contain PII. Erasing or wiping the hard drives involves overwriting all data on the drives, making it more difficult or impossible for anyone to recover the data. This method is recommended by most data destruction standards, including NIST 800-88, which is widely recognized in the industry. Drilling or physically destroying the drives is also a viable option, but it may not be practical or cost-effective for a large number of drives, and it may not be environmentally friendly. Degaussing and low-level formatting are not recommended for the disposal of drives that contain PII because they may not completely remove all data and may leave residual magnetic fields that can cause data recovery issues.

upvoted 3 times

  **Kristheitguru** 1 year, 5 months ago

Selected Answer: D

D is the Answer because theres possiblities of recovery on the other three options

upvoted 2 times

  **DandyAndy** 1 year, 5 months ago

Its has to be D. =D haha

upvoted 1 times

  **mcgirthus** 1 year, 4 months ago

It doesn't ask for the method that provides possibility of recovery, I don't understand why people on this website assume information that is not in the question.

The question asks for the BEST method to DISPOSE of the drive, which indicates it's not being re-used; the answer is B, Degaussing.

Degaussing is the most effective method of ensure a disk can never be used or recovered, even after drilling a drive data could technically still be recovered in some cases.

upvoted 2 times

  **hiddenkillz** 11 months ago

You can definitely recover data from an SSD that's been "degaussed". I don't understand why people on this website assume information that is not in the question. The question said "Drives" not "Hard drives" SSDs are not vulnerable to magnets. I think C would really be the correct method here because it will flip every single bit on each drive thus destroying all of the data.

upvoted 1 times

  **LayinCable** 1 year, 5 months ago

You're absolutely trolling.

upvoted 1 times

  **examreviewer** 1 year, 6 months ago

Selected Answer: D

Drilling and degaussing are also methods of disposing of hard drives, but they may not be as secure as erasing/wiping. Drilling involves physically destroying the drive by drilling holes through it, but it may still be possible to recover some data from the remaining pieces of the drive. Degaussing involves using a strong magnetic field to erase the data on the drive, but it may not be effective on modern hard drives that use magnetic shielding to protect data.

upvoted 1 times

  **LayinCable** 1 year, 5 months ago

Even after a drive has been "wiped" or "erased," the drive could still have its data or some of it pulled if someone has the right equipment and/or level of know how to extract said data. Which would leave drilling or degaussing as one of the possible answers.

upvoted 1 times

  **IDTENT** 1 year, 4 months ago

Drilling certainly isn't the answer here: As per CompTIA textbook: A disk can also be destroyed using drill or hammer hand tools—do be sure to wear protective goggles. While safe for most cases, this method is not appropriate for the most highly confidential data as there is at least some risk of leaving fragments that could be analyzed using specialist tools.

upvoted 2 times

  **ronniehaang** 1 year, 6 months ago

Selected Answer: A

Physical destruction is ALWAYS the best method before recycling or repurposing to minimize the risk of leaving persistent data remnants.

upvoted 2 times

  **max319** 1 year, 6 months ago

Just so you are aware, CompTIA defines degaussing as a physical method of destruction. Regardless, degaussing would be the correct answer because with drilling it is technically possible to recover some data from a drilled hard disk with the correct resources. Whereas degaussing makes the drive completely cease to function by delivering a powerful magnetic pulse, eliminating all magnetic domains on the disk platters (they're destroyed).

CompTIA's definition of Physical Destruction (pg. 12)

[https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-\(3-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1102-exam-objectives-(3-0))

Degaussing vs. Drilling



<https://guarddocs.com/resource/hdd-degaussing-vs-shredding/>

upvoted 4 times

  **hiddenkillz** 11 months ago

SSD's are not affected by degaussing, and this question did not specify what kind of drives are used, therefore Degaussing cant be assumed to be the correct answer.

upvoted 1 times

  **JollyGinger27** 1 year, 7 months ago

Selected Answer: B

Since we're talking about hard drives and not SSDs here, the best way to dispose of them would be through Degaussing. B is the answer

upvoted 3 times

  **takomaki** 1 year, 7 months ago

Wouldn't it make more sense to drill? Degaussing doesn't work on SSDs.

upvoted 2 times

  **LayinCable** 1 year, 5 months ago

It also doesn't state that the drives are SSD's, but from where the question says desktop, we could probably safely assume that they are HDD's instead. I know a desktop could have an SSD but for CompTIA purposes, I would go with HDD's.

upvoted 1 times

  **minx98** 1 year, 6 months ago


drilling can still leave fragments which may be recoverable with the correct tools. If you drill a hole in something, it won't work but that doesn't mean its indistinguishable

upvoted 1 times

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

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

Correct Answer: D

  **RoPsur** 1 year, 2 months ago

Selected Answer: D

Though Windows Home costs less, it's RDP version only acts as a client that connects to; not a server that can receive connections from.
upvoted 3 times



  **JollyGinger27** 1 year, 7 months ago

Selected Answer: D

Based on Professors Messer's videos in the first section, Windows 10 Pro has Remote Desktop but Windows 10 Home doesn't, so the most economical solution would be to use Windows 10 Pro. D is the answer
upvoted 4 times

  **Kelvinquan** 1 year, 8 months ago

Well. Pro is correct. But home also uses a kind of remote access.
upvoted 2 times

  **lilbuu** 1 year, 7 months ago

You can use Remote Desktop to connect to Windows 10 Pro and Enterprise, Windows 8.1 and 8 Enterprise and Pro, Windows 7 Professional, Enterprise, and Ultimate, and Windows Server versions newer than Windows Server 2008. You can't connect to computers running a Home edition (like Windows 10 Home).
upvoted 2 times

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

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

Correct Answer: C

  **Paradox_Walnut** Highly Voted  1 year, 9 months ago

To hide files, go to File Explorer, open the File's Properties, and select the "Hidden" box within "Attributes".

File Explorer > File > Properties > General Tab > Attributes > Hidden > Apply

upvoted 7 times

  **JollyGinger27** Highly Voted  1 year, 7 months ago

Selected Answer: C

I just confirmed what the other guy said about looking at File Explorer to hide the file. Therefore, C is the answer.

upvoted 6 times

  **JMLorx** Most Recent  3 weeks, 5 days ago

Selected Answer: C

Just confirmed from the other guys confirmation about looking at File Explorer to hide the file. Therefore, C is the answer.

upvoted 1 times

  **b7cd4aa** 6 months, 4 weeks ago

Selected Answer: C

Just confirmed from the other guys confirmation about looking at File Explorer to hide the file. Therefore, C is the answer.

upvoted 3 times

  **Raffaello** 9 months ago

Selected Answer: C

How to hide files and folders in Windows 10 using File Explorer

Navigate to the file or folder you want to hide. ...

Right-click and choose Properties. ...

Choose Hidden and press OK. ...

Confirm Attribute Changes. ...

The selected file is marked as hidden and its icon grayed out.

upvoted 2 times

  **cpaljhc** 1 year, 9 months ago

Why not indexing options?

upvoted 1 times

  **[Removed]** 1 year, 9 months ago

Indexing options speeds up the search process for File Explorer, but it does not hide any folders. To hide folders, you have to go to File Explorer options, so it is C.

upvoted 8 times

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

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



Correct Answer: C

  **juicyb00ty** 1 year, 6 months ago

Selected Answer: C

Whenever you get a new router, the first thing you should do is change the password immediately. Changing the SSID doesn't mean better security, it just changes the name but the password still stays the same, that's why you gotta change that password ASAP. Otherwise any one can try and guess the default password.



upvoted 4 times

  **JollyGinger27** 1 year, 7 months ago

Selected Answer: C

I'm confirming what the other guy said. You have to secure your network first before doing anything else. C would be the answer

upvoted 4 times

  **Aggelos312** 1 year, 7 months ago

shouldn't the answer be D?

upvoted 1 times

  **takomaki** 1 year, 7 months ago

Changing SSID doesn't help security very much, if at all. You want to focus on securing your network first. If the SOHO router has been bought by the user, the default password is easily guessed. If it was provided by the ISP, the password is shown on the device, so anyone who sees the device will know the password.

upvoted 4 times

A technician has spent hours trying to resolve a computer issue for the company's Chief Executive Officer (CEO). The CEO needs the device returned as soon as possible. Which of the following step should the technician take NEXT?

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

Correct Answer: D

  **Porygon** Highly Voted  1 year, 10 months ago

Selected Answer: D


The answer is D, however, if I didn't like my job, I'd probably pick C. Just to let the boss know who is in charge.

upvoted 34 times

  **Michcat** 1 year, 1 month ago

dam right !

upvoted 4 times

  **sigidy** 1 year, 7 months ago

yeah, that's right!

upvoted 3 times

  **Wade18** 1 year, 7 months ago

W ansewr

upvoted 2 times

  **Jay23AmMonsIV** Most Recent  3 months ago

Selected Answer: A

Change management processes typically involve notifying stakeholders, such as owners or managers responsible for the affected systems or services, about planned changes. By following the change management process, owners can be informed about the reinstalling of the security software, allowing them to monitor the process and assess any potential impact on system performance or security. While options B, C, and D are also considerations in change management processes, they are not as directly relevant to the specific scenario described

Having a rollback plan is an important aspect of change management to mitigate risks associated with changes. However, in this scenario, the primary concern is reinstalling the security software rather than anticipating potential negative impacts on applications.

Therefore, ensuring that owners are notified about the change and can monitor its performance impact is the most relevant reason to follow the change management process in this scenario.



upvoted 1 times

  **Avengers_inc** 5 months, 2 weeks ago

Selected Answer: D

Dont let your ego take the better part of you, plus you probably wont even be enough to die on that ticket.. escalate that s**t pronto!

upvoted 1 times

  **Raffaello** 8 months, 4 weeks ago

Selected Answer: D

Ticket escalation is the process by which a customer issue (support ticket) is passed on to a senior customer service manager or supervisor for a quick and effective resolution. Ticket escalation happens when support agents are unable to resolve a customer query effectively in a timely manner

upvoted 1 times

  **mohdAj** 9 months, 3 weeks ago

Selected Answer: D

the technician has already spent hours trying to resolve the issue , Thats mean B Wrong answer

Continuing to spend more time without resolution might not be the most efficient use of resources, especially when dealing with a critical issue for a high-profile user like the CEO. Escalating the ticket ensures that the problem is addressed by individuals with more expertise or resources to expedite the resolution process.

upvoted 1 times



  **TungstonTim** 1 year ago

Selected Answer: B

When facing a complex computer issue that has taken a significant amount of time and effort to troubleshoot, it's often a good idea to return to the basics and repeat the iterative processes. This involves checking the work that has already been done, verifying assumptions, and re-evaluating the troubleshooting steps taken. Sometimes, stepping back and reviewing the issue with a fresh perspective can lead to new insights or solutions.

Continuing to research the issue (Option A) might lead to more time spent without guaranteed results. Informing the CEO that the repair will take a couple of weeks (Option C) is not an ideal solution, as it's essential to address their needs promptly. Escalating the ticket (Option D) might be necessary in some cases, but it's generally a good practice to exhaust all reasonable troubleshooting steps before escalating to higher levels of support.

upvoted 1 times

  **mohdAj** 9 months, 3 weeks ago

"A technician has spent hours trying to resolve a computer issue"

upvoted 2 times

  **Kristheitguru** 1 year, 5 months ago

Selected Answer: B

B. Repeat the iterative processes would be the next step the technician should take. This involves going back through the troubleshooting steps that have already been taken to ensure that nothing was missed or overlooked. It's possible that the issue may have been caused by a simple oversight or an incorrect assumption, and repeating the process could help the technician identify and resolve the problem. If the issue still cannot be resolved after repeating the iterative process, then the technician may need to escalate the ticket or seek additional assistance. However, it's important to keep the CEO informed of the progress and expected timeline for the resolution.

upvoted 1 times

Question #54

Topic 1

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

Correct Answer: B

  **Delawasp** **Highly Voted**  1 year, 3 months ago

Selected Answer: B

B. Chain of custody must be maintained throughout the forensic evidence life cycle when dealing with a piece of evidence. The chain of custody refers to the chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of physical or electronic evidence. It is crucial to maintain a clear and complete chain of custody to ensure that the evidence is admissible in court and that its integrity and authenticity are not compromised. While acceptable use, security policy, and information management are also important considerations in forensic investigations, they do not specifically refer to the maintenance of the chain of custody.

upvoted 10 times

  **Michcat** 1 year, 1 month ago

Thanks ~~

upvoted 1 times

  **MikeGeo** **Most Recent**  6 months, 3 weeks ago

Was not expecting my time on the police force to aid in a tech based exam, but here we are



upvoted 1 times

  **Porygon** 1 year, 10 months ago

Selected Answer: B

Answer is correct

upvoted 3 times

  **imtiaziL** 1 year, 10 months ago

answer is correct

[https://www.google.co.za/url?](https://www.google.co.za/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiD4sTX2f_6AhVKQEEAHbXcCp0QFnoECA4QAw&url=https%3A%2F%2Fwww.unodc.org%2Fen%2Fcybercrime%2Fmodule-6%2Fkey-issues%2Fhandling-of-digital-evidence.html%23%3A~%3Atext%3DTo%2520demonstrate%2520this%252C%2520a%2520chain%2Clife%2520cycle%2520of%2520a%2520case.&u sg=AOvVaw2OoKXHja_nQmIUgAi4wauN)

[sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiD4sTX2f_6AhVKQEEAHbXcCp0QFnoECA4QAw&url=https%3A%2F%2Fwww.unodc.org%2Fen%2Fcybercrime%2Fmodule-6%2Fkey-issues%2Fhandling-of-digital-evidence.html%23%3A~%3Atext%3DTo%2520demonstrate%2520this%252C%2520a%2520chain%2Clife%2520cycle%2520of%2520a%2520case.&u sg=AOvVaw2OoKXHja_nQmIUgAi4wauN](https://www.unodc.org/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html#text=To%20demonstrate%20this%2C%20a%20chain%2Clife%20cycle%20of%20a%20case.&u sg=AOvVaw2OoKXHja_nQmIUgAi4wauN)

upvoted 3 times

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

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

Correct Answer: A

  **Jay23AmMonsIV** 3 months ago

Change management processes typically involve notifying stakeholders, such as owners or managers responsible for the affected systems or services, about planned changes. By following the change management process, owners can be informed about the reinstalling of the security software, allowing them to monitor the process and assess any potential impact on system performance or security. While options B, C, and D are also considerations in change management processes, they are not as directly relevant to the specific scenario described.

Having a rollback plan is an important aspect of change management to mitigate risks associated with changes. However, in this scenario, the primary concern is reinstalling the security software rather than anticipating potential negative impacts on applications.

Therefore, ensuring that owners are notified about the change and can monitor its performance impact is the most relevant reason to follow the change management process in this scenario.

upvoted 1 times

  **[Removed]** 1 year, 6 months ago



Selected Answer: A

I asked ChatGPT this question and this is the result

If static IP addresses are not allowed, then the technician can use DHCP reservation to ensure that the server maintains the same IP address at all times.

DHCP reservation is a feature available in most SOHO devices and it allows the technician to assign a fixed IP address to a specific device on the network. The device's MAC address is used to identify the device, and the DHCP server assigns the same IP address to that device every time it requests an IP address.

upvoted 2 times

  **JollyGinger27** 1 year, 7 months ago

Selected Answer: A

The answer appears correct based on this Google article I found:

<https://support.google.com/googlenest/answer/6274660?hl=en>

upvoted 2 times

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

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

Correct Answer: A

  **Vin0126** Highly Voted  1 year, 10 months ago

Selected Answer: A

The software was already installed previously it just accidentally uninstalled. Therefore no need for the rollback. It just need to re-install and monitor for the performance.

upvoted 20 times

  **Kristheitguru** 1 year, 5 months ago

answer is D because you will always need a backup plan in IT even if it worked before. What if something happens mid installation?.

upvoted 1 times

  **LayinCable** 1 year, 5 months ago

Just for this answer, it says in case it breaks an application and not anything to do with the downloading process. I do agree that a rollback plan should be in place but from where it's the exact same software, they would have probably known by now if this software breaks applications. So I do agree with A

upvoted 2 times

  **Porygon** Highly Voted  1 year, 10 months ago

Selected Answer: A

D is not the answer, the 2 saying D are incorrect.

The only really decent answers for this would be A or C; and though A could use wording adjustment, it's a better answer than C.

There is no need for a rollback, and risk assessment has already been calculated.

The assumption would be that re-installing the security software (which MUST be on those servers), could cause the servers to go offline possibly for the installation; so you had best notify your users of the possible downtime and to expect either slow traffic, or non-existent connection until the reinstallation is completed.



upvoted 8 times

  **Rixon** Most Recent  2 weeks, 4 days ago

Selected Answer: D

D is the most appropriate answer because it addresses the core aspect of change management—risk management through a rollback plan—ensuring that any potential negative impact from the change can be mitigated.

upvoted 1 times

  **Tural038** 4 months, 2 weeks ago

Selected Answer: A

correct

upvoted 1 times

  **Mr_Tension** 5 months, 1 week ago

whoever is saying D, mate isn't there a rollback plan already when they install the app for the first time? also he is going to install the app which was uninstalled by mistakenly. So that means he already have a rollback plan to install this app. so in this scenario , he just need to inform the owner. so from my opinion Answer is A

upvoted 1 times

  **bobby** 5 months, 3 weeks ago

I can't answer this question.... My Comptia book can't answer this question. Messer hasn't answered this question. The vote basically 50/50 done by people whom are all studying for this. Only conclusion I can come up with is this is an intentional bad question.


upvoted 2 times

  **BabaBoer** 7 months ago

Selected Answer: D

Answer is D


upvoted 1 times

[-]  **Pisces225** 8 months, 3 weeks ago

Selected Answer: D

D - the thing throwing everyone off is that it's the same version. Even the same version is a concern because volume and directory exceptions along with other options may have been previously configured and will have been lost. A default install needs to be treated like any other and it's obvious from the question that the requirement is a matter of company policy and having a rollback option is part of any proper change management process which can't be selectively ignored because there's 'a good reason'. As implied by the question, the technician even received a responses from the change management approver compliance with the policy is required regardless of the component having been previously part of the environment.

upvoted 2 times

[-]  **Alizade** 9 months, 1 week ago

Selected Answer: D

D. A rollback plan can be implemented in case the software breaks an application.


upvoted 1 times

[-]  **LeagoMorena** 9 months, 1 week ago

Selected Answer: D

Strongly believe its D

upvoted 1 times

[-]  **Mozzy83** 10 months ago

Selected Answer: D

I believe the correct answer is D. It is expected that installing the same software wouldn't cause any complications, but rollbacks are for the unexpected.

upvoted 2 times

[-]  **Paula77** 11 months, 3 weeks ago

Selected Answer: D

Change management processes typically include the creation of a rollback plan as part of change planning. In this case, if the reinstallation of the security software were to cause unexpected issues or conflicts with applications, having a rollback plan would allow for a smooth and quick recovery to the previous state. This minimizes the potential impact on operations and ensures that the environment can be reverted to a stable state if necessary.

upvoted 2 times

[-]  **TonxhiPatonxhi** 11 months, 3 weeks ago

Selected Answer: D

It's D

upvoted 2 times

[-]  **glenpharmd** 1 year ago

A rollback plan can be implemented in case the software breaks an application.

The reason this is the best choice is that reinstalling the security software on all servers in the environment can introduce unexpected complications, including potential conflicts with other applications. A rollback plan ensures that if something does go wrong, there's a structured approach to revert the changes and restore the servers to their previous state. This helps in maintaining the integrity, availability, and functionality of systems and applications in the environment.

upvoted 1 times

[-]  **Nabilrrhmn** 1 year, 1 month ago

Selected Answer: D

According to the CompTIA Security+ certification exam objectives, the BEST reason to follow the change management process in this scenario is D. A rollback plan can be implemented in case the software breaks an application. This will ensure that the change can be reversed or undone if it causes any negative consequences or unexpected outcomes.

upvoted 4 times

[-]  **solaWONDER** 1 year, 2 months ago

THE ANSWER IS D

upvoted 3 times

[-]  **Delawasp** 1 year, 3 months ago

Selected Answer: D

D. A rollback plan can be implemented in case the software breaks an application. Following the change management process in this scenario is important because it ensures that a rollback plan is in place in case the software breaks an application. This can help minimize downtime and reduce the impact on business operations. Additionally, going through the change management process can provide an opportunity to assess the impact of the change, involve stakeholders, and ensure that the change is tested and approved before implementation.

upvoted 2 times

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

- A. Install and run Linux and the required application in a PaaS cloud environment.
- B. Install and run Linux and the required application as a virtual machine installed under the Windows OS.
- C. Use a swappable drive bay for the boot drive and install each OS with applications on its own drive. Swap the drives as needed.
- D. Set up a dual boot system by selecting the option to install Linux alongside Windows.

Correct Answer: B

  **JBSecurity101** 10 months, 3 weeks ago

Selected Answer: B

Limited bandwidth negates any cloud environment solution; therefore, the answer is B.
upvoted 2 times

  **LayinCable** 1 year, 5 months ago

Im actually kind of confused by this because it says he has limited bandwidth and running a VM takes some resources, so how could this be a viable answer?
upvoted 1 times

  **BinMcGrin** 1 year, 5 months ago

I think the limited bandwidth has to do with the user's internet connection, therefore making answer A unviable.
upvoted 2 times

  **HubrisTheExalted** 1 year, 5 months ago

I wish that there was an answer for making a docker application that way there wouldn't need to be any resources allocated to running an entire VM on the same computer
upvoted 1 times

  **[Removed]** 1 year, 9 months ago

Selected Answer: B

It's B. This question aligns more with Domain 4 of the 220-1101 exam (cross-platform virtualization), so it's quite weird to see it in the 220-1102 exam.
upvoted 4 times

  **Porygon** 1 year, 10 months ago

Selected Answer: B

B. However, I don't really like the word "under" in regards to how the Linux virtual box is installed. I would have used maybe: "in", "on", or "embedded", even though embedded isn't really the best way to describe it.

Sounds like good ole CompTIA asking weird questions.
upvoted 3 times

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



- A. Within the Power Options of the Control Panel utility, click the Change Plan Settings button for the enabled power plan and select Put the Computer to Sleep under the Plugged In category to Never.
- B. Within the Power Options of the Control Panel utility, click the Change Plan Settings button for the enabled power plan and select Put the Computer to Sleep under the On Battery category to Never.
- C. Within the Power Options of the Control Panel utility, select the option Choose When to Turn Off the Display and select Turn Off the Display under the Plugged In category to Never.
- D. Within the Power Options of the Control Panel utility, select the option Choose What Closing the Lid Does and select When I Close the Lid under the Plugged In category to Do Nothing.

Correct Answer: D

  **CodeOnTren** 1 month, 1 week ago



Selected Answer: D

Really obvious is D , he literally wants to close his laptop so it can only mean one thing
upvoted 1 times

  **igorclapa** 5 months, 3 weeks ago

Selected Answer: D

How could we possibly know the answers without the chatgpt anons???
upvoted 2 times

  **ph12** 1 year, 3 months ago

100% D is the correct answer
upvoted 4 times

  **StrawberryTechie** 1 year, 4 months ago

Selected Answer: D

I followed the instructions in D on my laptop and it worked. The answer is D.
upvoted 2 times

  **navvvarroooo** 1 year, 8 months ago

Selected Answer: D

Wait no in windows 10 it would be D
upvoted 2 times

  **navvvarroooo** 1 year, 8 months ago

The answer is C because thats the only path
upvoted 1 times

  **Abz1999** 1 year, 6 months ago

Stop confusing people
upvoted 5 times

  **Paradox_Walnut** 1 year, 9 months ago

Selected Answer: D

If you have a laptop, please try these settings/options yourself. It will be D.
upvoted 3 times

  **Porygon** 1 year, 10 months ago

Selected Answer: D


The answer is D.
That is THE ONLY ANSWER that makes sense given the context. You need to change 'what happens when I close the lid' on the laptop, and D is the only way to reach that option, and accomplish the question.

C is NOT correct.

Source, look it up on google, or check the Microsoft website FAQ or guides.

C'mon.

upvoted 2 times

[-]  **NerdyW** 1 year, 10 months ago

Selected Answer: D

The answer D is correct. The laptop has an additional option under power and sleep settings that desktops do not have. Switching to do nothing prevents the screen from turning off when closed.

upvoted 3 times

[-]  **[Removed]** 1 year, 11 months ago

Directly from Microsoft Website: If you're using only a laptop, select Choose what closing the lid does. Next to When I close the lid, select Sleep, and then select Save changes.


upvoted 1 times

[-]  **simsbow1098** 1 year, 11 months ago

Selected Answer: C


C is the only path in the control panel that exists. Open up your control panel, click on power options, choose when to turn off the display then select put computer to sleep to never. In windows there is an option to change when the computer sleeps but that isn't one of the answers.

upvoted 1 times

[-]  **Anicka456** 1 year, 11 months ago

you must be very persistent to tick this answer i will for D .. as the settings are in power options.

upvoted 1 times

[-]  **Aerials** 1 year, 10 months ago

The answer is NOT C, because C refers to the screen settings only. Not the Sleep settings. They are different.

upvoted 1 times

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

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

Correct Answer: C

  **IconGT** Highly Voted 1 year, 4 months ago

Selected Answer: C

C. Ransomware has infected the computer. Ransomware is a type of malware that encrypts files on a victim's computer, making them inaccessible, and demands a ransom in exchange for the decryption key. When a user receives a message stating that files are encrypted and cannot be accessed, it is likely that ransomware has infected the computer. Cryptominers are malware that use a victim's computing resources to mine cryptocurrency. Phishing is a social engineering attack that tricks victims into providing sensitive information. Keyloggers are malware that record a user's keystrokes to steal login credentials or other sensitive information. While these types of malware can cause issues on a computer, they would not likely result in a message stating that files are encrypted and inaccessible.

upvoted 5 times

  **Mr_Tension** Most Recent 5 months, 1 week ago

Do crypto miner encrypt your file? phishing encrypt your file? Keylogger encrypt your file? then what's the point of arguing you guys with option C? bro it's just a common sense. Black hat hacker might run a ransomware attack and ask for money but if they are hacktivist , of course they will never ask for money. all they want to stop running the business. So again , stop arguing here and try to use your brain.

upvoted 3 times

  **[Removed]** 1 year, 4 months ago

Ransomware encrypts files and asks for payment. It didn't explicitly state that it asked for payment, but the gist here is that they are locking you out of your own files.

upvoted 2 times

  **StrawberryTechie** 1 year, 4 months ago

Selected Answer: C


Although it doesn't state that anyone is asking for a fee to unlock the files, C is still the closest answer.

upvoted 3 times

  **LayinCable** 1 year, 5 months ago

C makes no sense as the question says absolutely nothing about him being prompted to pay a fee of some kind to access the data he once had access to. Maybe it is CompTIA's way of getting people to get it wrong but I don't think they would just leave out big details like that in a question. They're more on the rewording things to make them sound different, rather than withholding pertinent info.



upvoted 2 times

  **minx98** 1 year, 6 months ago

Selected Answer: A

I don't think it's C. Ransomware is when a user is demanded to pay for something and the question doesn't say anything about this. Cryptomining however would temporarily disable a feature, such as the files being encrypted for the user not being able to access. Therefore I would go with A

upvoted 2 times

  **minx98** 1 year, 6 months ago


On second thought, it is most likely Crypto-ransomware. The question should have stated this to be honest but there goes compitia trying to falsely catch people out

upvoted 1 times

  **StaticK9** 11 months, 3 weeks ago

Ransomware is a kind of malware that encrypts a victim's data and holds the decryption key for ransom.

upvoted 1 times

  **Rafid51** 1 year, 6 months ago

Selected Answer: C

Ransomware is a type of malicious software that encrypts the user's files and demands payment in order to use the file.

upvoted 3 times

  **JollyGinger27** 1 year, 7 months ago

Selected Answer: C

It's C. Know your malware stuff, you guys.

upvoted 3 times

A technician is replacing the processor in a desktop computer. Prior to opening the computer, the technician wants to ensure the internal components are protected. Which of the following safety procedures would BEST protect the components in the PC? (Choose two.)

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

Correct Answer: AB

  **JollyGinger27** Highly Voted 1 year, 7 months ago

Selected Answer: AB

The CPU is not a hot-swappable component, so you would need to remove the power first. Then, just use an ESD strap to protect the equipment from Electrostatic discharge. Therefore, A and B are the best answers.

upvoted 10 times

  **minx98** 1 year, 6 months ago

no way. It is C and E

upvoted 1 times

  **CodeOnTren** 1 month, 1 week ago

bruh fr

upvoted 1 times

  **beefwellington** 1 year, 6 months ago

I think they key here is "prior to opening the computer". placing the psu in an antistatic bag would require opening the PC.

upvoted 5 times

  **minx98** 1 year, 6 months ago

Yes you are correct actually, A and B

upvoted 4 times

  **LayinCable** 1 year, 5 months ago

Hahaha ive seen your comments a few times in some of these questions and they crack me up with how you realize things. They're correct and informational, but they just make me laugh

upvoted 6 times

  **Jay23AmMonsIV** Most Recent 3 months ago



Selected Answer: AF

An Electrostatic Discharge (ESD) strap helps to prevent static electricity from building up on the technician's body and potentially damaging sensitive electronic components inside the computer. Using an ESD strap ensures that any static charge is safely discharged to ground, protecting the internal components from electrostatic damage.

Grounding equipment, including the computer and work surface, helps to dissipate any static electricity and prevents electrostatic discharge from damaging internal components. Ensuring that the equipment is properly grounded provides an additional layer of protection against ESD during the component replacement process.

Utilizing an ESD strap (option A) and ensuring equipment is grounded (option F) are the best safety procedures to protect internal components during the processor replacement process.

upvoted 1 times

  **igorclapa** 5 months, 3 weeks ago

Selected Answer: AB

Use an ESD strap & unplug the computer from power? I don't know....better go ask chatgpt, he'll know what to do.

upvoted 2 times

  **DBrega** 6 months, 3 weeks ago

Selected Answer: AF


You'll need to protect computer from ESD. Computer must be grounded!

upvoted 1 times

  **MHendricks** 1 year ago

Would it not be A & F? The question is asking to protect the components in the computer. So if the components are grounded and using ESD strap, it will prevent the components from being damaged? Correct me if I am wrong please.

upvoted 3 times

  **IconGT** 1 year, 4 months ago

Selected Answer: AC

A. Utilizing an ESD strap and C. Placing the PSU in an antistatic bag are the best safety procedures to protect the internal components in the PC.

An ESD (Electrostatic Discharge) strap helps to prevent damage to sensitive electronic components by grounding the technician, thereby preventing any static electricity discharge. Placing the Power Supply Unit (PSU) in an antistatic bag can also protect it from electrostatic discharge during the replacement process.



Disconnecting the computer from the power source is also important to prevent electrical shocks, but it will not protect the internal components from ESD. Ensuring proper ventilation and removing dust from the ventilation fans are important for maintaining the computer's cooling system but do not protect the internal components during a processor replacement. Ensuring equipment is grounded is also important but may not be sufficient to protect against ESD.

upvoted 2 times

  **Kordrakka** 1 year, 4 months ago

"Prior to opening the computer" is the key phrase here. You can't put a PSU in the antistatic bag prior to opening the computer.

upvoted 5 times

  **minx98** 1 year, 6 months ago

Selected Answer: CE

These are the two which can damage the computer parts if not done

upvoted 1 times

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



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

Correct Answer: A

  **takomaki** Highly Voted 1 year, 7 months ago



Selected Answer: D

Guys, its Ease of Access. I use Win10 21H2, and it literally says "Turn on speech recognition". Language simply lets you set up your mic for speech recognition, and if you try to do it, all it does is open up a troubleshooter. It simply tells you if your mic supports speech recognition. Even if its not just the mic, the goal is to enable it, which is necessary in order for the setup to even work properly. If Windows 11 has it too, its definitely D.
upvoted 16 times

  **Gwcan** 11 months, 2 weeks ago

The question says the user wants to "set up" speech recognition. The Language tool in settings has an option that says "set up your mic for speech recognition", whereas ease of access just has a toggle that allows you to turn speech recognition on and off. It's a tricky question but it seems like the answer is A.

upvoted 2 times

  **Big_Q** 10 months, 3 weeks ago

The key phrase is "Windows Settings tools." Ease of Access is a Control Panel applet. To choose Speech Recognition go to Start > Settings > Time & Language > Language > Speech > Speech Language

upvoted 3 times

  **SammsLovesJesus** Most Recent 3 days, 10 hours ago

Selected Answer: D

The answer her is D
upvoted 1 times

  **Philco** 2 weeks ago

Although the Answer is A
it seems to be a Bad Answer choice-----It should says---- Control Panel>Speech Recognition> Start Speech Recognition
There is no Such thing as a Language option on Control Panel-----using Win 10 version 22H2

upvoted 1 times

  **CodeOnTren** 1 month, 1 week ago

Selected Answer: D

I feel like this is the right answer
upvoted 1 times

  **jade290** 2 months ago



Selected Answer: D

I literally just found it here on my PC:
Control Panel\Ease of Access\Speech Recognition
upvoted 1 times

  **Alzahrani** 4 months, 3 weeks ago


Selected Answer: D

I checked this on my personal computer and found speech recognition in Ease of Access.
upvoted 1 times

  **yutface** 5 months, 2 weeks ago


Selected Answer: D

Open Control Panel.
Click on Ease of Access.
Select Speech Recognition.
Click the Start Speech Recognition link.
In the Set up Speech Recognition page, click Next.
Choose the type of microphone you'll be using.
upvoted 2 times

  **Cyberpleb** 5 months, 2 weeks ago

In Control Panel, select Ease of Access > Speech Recognition > Train your computer to better understand you. Select Next. Follow the instructions on your screen to set up speech recognition.

upvoted 1 times

  **MikeGeo** 5 months, 3 weeks ago

Option A is for determining if it's english, spanish, etc.
Option D allows for using the vocal input in lieu of typing.

upvoted 1 times

  **yutface** 6 months ago

Stupid, filler question. You can literally just hit the windows key and type "speech recognition" and hit enter. Questions like this do not show your knowledge of windows, but show what "Facts" you have memorized.

upvoted 1 times

  **Jay210** 7 months, 1 week ago



I asked my instructor he said D

upvoted 1 times

  **Hus1Saad** 8 months ago

it is amazing how they make these questions and not allow us to have a clear answer, why not window+Ctrl+S or something ...

upvoted 1 times

  **Raffaello** 8 months, 4 weeks ago

Selected Answer: D

In Control Panel, select Ease of Access > Speech Recognition > Train your computer to better understand you. Select Next. Follow the instructions on your screen to set up speech recognition

upvoted 2 times

  **DeckardCain** 11 months, 1 week ago

Select Start > Setting> Ease of access> Speech> Turn on Speech Recognition

upvoted 2 times

  **StaticK9** 11 months, 3 weeks ago

Selected Answer: D

D. Ease of Access

upvoted 1 times

  **JBSecurity101** 1 year ago

Selected Answer: D

Ease of Access.

upvoted 1 times

  **GL1494** 1 year, 1 month ago

Selected Answer: D

D is correct after I look around everything came to that answer. Language is more for OS or applications used in your language.

upvoted 1 times

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

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

Correct Answer: C

  **Manzer** Highly Voted 1 year, 11 months ago

Selected Answer: B

The tech doesn't recognize the interface. So don't use it.
upvoted 25 times

  **LayinCable** Highly Voted 1 year, 5 months ago

Selected Answer: B

Some of these questions are answered wrong on purpose so that Exam topics could avoid copyright issues with these tests. But its also good that we have discussion boxes to mitigate these kinds of things, so no, if it quacks like a duck and walks like a duck, then its probably a virus and you shouldn't click on it. The answer is B.
upvoted 21 times

  **IDTENT** 10 months, 4 weeks ago

More likely the original answer is wrong as the pdf they came from held that answer. That is what makes examtopics stand out; intelligent discussion around the question.
upvoted 3 times

  **goss_6087** Most Recent 2 months, 2 weeks ago

Would "A" be likened to quarantining the affected system?
upvoted 2 times

  **Christycent** 4 months, 1 week ago

Selected Answer: B

categorically B, why would you use an interface you dont recognize?
upvoted 1 times

  **mohdAj** 9 months, 3 weeks ago

Selected Answer: B

It's important for the technician to understand the nature of the interface and what triggered it to appear.
upvoted 1 times

  **JBSecurity101** 1 year ago

Selected Answer: B



Obvious answer. It's a fake anti-virus software.
upvoted 2 times

  **[Removed]** 1 year, 5 months ago

Seems like C is the answers every indian call center scammer wants.
upvoted 9 times



  **Sebatian20** 1 year, 3 months ago

20B Indians cant be wrong.
upvoted 4 times

  **tutita** 1 year, 5 months ago

Selected Answer: B

makes the most sense... why would you use an interface you dont recognize? it can be a pop up ad virus
upvoted 4 times

  **Rafid51** 1 year, 6 months ago

Selected Answer: B

The technician must first determine whether it is legitimate or a potential scam. Therefore, he needs to (B) Investigate what the interface is and what triggered it to pop up.

upvoted 2 times

  **bconiglio** 1 year, 7 months ago

Selected Answer: B

If the interface is unfamiliar or suspicious, definitely don't use it. B is the only answer that presents a troubleshooting step and doesn't fall for the malware.

upvoted 2 times

  **PatrickH** 1 year, 8 months ago

C is literally the worst possible answer. Use the scammers own software to remove the virus! Wont end well. B is correct

upvoted 2 times

  **alexandrsexy** 1 year, 9 months ago

Selected Answer: B



No doubt about this one: B. Investigate what the interface is and what triggered it to pop up.

upvoted 2 times

  **TiaAnizia** 1 year, 9 months ago

The answer is B

upvoted 1 times

  **sioke** 1 year, 10 months ago

Step 1 - Identify malware symptoms, Step 2 - Quarantine infected systems, Step 3 - Disable System Restore, Step 4 - Remediate infected systems, Step 5 - Schedule scans and run updates, Step 6 - Enable System Restore and create restore point, Step 7 - Educate user,

So I think the answer is B identify the symptom



upvoted 5 times

  **ryanzou** 1 year, 11 months ago

Selected Answer: B

B makes more sense



upvoted 3 times

  **enoyl** 1 year, 11 months ago

Selected Answer: B

tech is rookie



upvoted 3 times

  **trungH** 1 year, 11 months ago

Selected Answer: A

C makes no sense why would you use an unrecognized interface to perform a virus scan?

upvoted 2 times

  **andrizo** 1 year, 11 months ago

I agree, but I wouldn't go with A as this does not solve the issue.

upvoted 4 times

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

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

Correct Answer: D

  **alexandrasexy** Highly Voted  1 year, 9 months ago

Selected Answer: D

D. AUP = Acceptable Use Policy
upvoted 7 times

  **Raffaello** Most Recent  8 months, 4 weeks ago

Selected Answer: D

An acceptable use policy (AUP), acceptable usage policy or fair use policy is a set of rules applied by the owner, creator or administrator of a computer network, website, or service that restricts the ways in which the network, website or system may be used and sets guidelines as to how it should be used.
upvoted 2 times

  **JBSecurity101** 1 year ago

Selected Answer: D

Acceptable Use Policy.
upvoted 2 times

  **Paradox_Walnut** 1 year, 9 months ago

AUP = Acceptable Use Policy
upvoted 4 times

  **imtiazL** 1 year, 10 months ago

correct answer

reason - [https://www.google.co.za/url?](https://www.google.co.za/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwilwee92_6AhVcS0EAHSM4AQwQFnoECA8QAQ&url=https%3A%2F%2Fwww.techtarget.com%2Fwhatis%2Fdefinition%2Facceptable-use-policy-AUP&usg=AOvVaw3q8pNJOckx2YCvM35uhUNb)

https://www.google.co.za/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwilwee92_6AhVcS0EAHSM4AQwQFnoECA8QAQ&url=https%3A%2F%2Fwww.techtarget.com%2Fwhatis%2Fdefinition%2Facceptable-use-policy-AUP&usg=AOvVaw3q8pNJOckx2YCvM35uhUNb

upvoted 2 times

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

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

Correct Answer: B

  **Bogardinc** Highly Voted 1 year, 8 months ago

Took 1102 today and this question was on the exam but VNC was replaced with MSRA (Microsoft Remote Access)
upvoted 16 times

  **Wade18** 1 year, 7 months ago

did you pass my boi?
upvoted 15 times

  **[Removed]** 1 year, 7 months ago

So it's RDP
upvoted 4 times

  **CTE_Instructor** 1 year, 6 months ago

MSRA is Microsoft Remote Assistance, which would satisfy the prompt of the question to assist a user remotely. This allows multiple connections for troubleshooting / guidance purposes.

In the options in this specific question, VNC allows screen sharing which would also allow the technician to assist the user by seeing what is on their screen.

RDP is primarily used if you *were* the user attempted to connect to a remote workstation. It's primarily a single user connection.
upvoted 10 times

  **Rixon** Most Recent 2 weeks, 4 days ago

Why does CompTIA give more than 1 correct answer as an option?
upvoted 1 times

  **mohdAj** 9 months, 3 weeks ago

Selected Answer: B

VNC / MSRA
"allow a technician to see the issue along with the user"
upvoted 4 times

  **mohdAj** 9 months, 3 weeks ago

Selected Answer: B

VNC (Virtual Network Computing) is a technology that allows a technician to see and control a remote user's desktop.
upvoted 2 times

  **Mehsotopes** 1 year, 1 month ago

Selected Answer: B

Being a centralized support function, VNC would make sense being that it is assigned for thin clients connecting to a central host server.
upvoted 1 times

  **[Removed]** 1 year, 1 month ago

Yeah i agree, it also says to see the issue with the user which RDP does not allow you to do
upvoted 1 times

  **[Removed]** 1 year, 4 months ago

VNC and MSRA both allow screen sharing.
upvoted 2 times

  **Kristheitguru** 1 year, 5 months ago

Selected Answer: B



RDP will block the Users screen while the technician works on the device.
upvoted 3 times

  **Paradox_Walnut** 1 year, 9 months ago

Selected Answer: B



It's VNC

upvoted 3 times

  **enoyl** 1 year, 11 months ago

VNC is essentially a screen-sharing protocol and is ideal for collaboration sessions which include presentations and training, as well as remote technical support functions. Each logged-in client can view and interact within the same session. RDP on the other hand does not allow concurrent logins and a new login will automatically force a previous session to log off.



upvoted 2 times

  **RJ4** 1 year, 11 months ago

There are alternatives to using RDP for remote access. For example, in macOS, you can use the Screen Sharing feature for remote desktop functionality. Screen Sharing is based on the Virtual Network Computing (VNC) protocol. You can use any VNC client to connect to a Screen Sharing server.



VNC itself is a freeware product with similar functionality to RDP. It works over TCP port 5900. Not all versions of VNC support connection security. macOS Screen Sharing is encrypted.

upvoted 1 times

  **enoyl** 1 year, 11 months ago

If VNC is an alternative for RDP, why not choose RDP for the answer?

upvoted 3 times

  **GlixRox** 1 year, 11 months ago

End of the question states "allow a technician to see the issue along with the user" - that's the key. RDP logs you in, but force logs off the current user. And they get a blank lock screen on their end so they can't see what you're doing. VNC allows screen sharing - use it all the time at work as desktop support.

upvoted 22 times

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

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

Correct Answer: AB

  **alexandrsexy** Highly Voted  1 year, 8 months ago

Selected Answer: AB

A & B because F. Access control vestibule is when you enter the actual Data center itself not in the server rooms, all other answers except video surveillance are incorrect!

upvoted 15 times

  **CecilSaw** Highly Voted  1 year, 9 months ago

Selected Answer: AB

IMO access control vestibule wouldn't make sense in this situation. A man trap to access the server room? A and B seem to be the only logical answers. Note it does say to the server room, not the servers themselves.

upvoted 9 times

  **sinfulhymn** 1 year ago

Youve never seen security for a server room. eat shit honestly

It says Best way to secure physical access.

For one a control vestibule allows one person, biometrics makes sure credential apply to only one person as opposed to badge readers that can be stolen or replicated.

upvoted 1 times

  **max12553** 2 weeks, 2 days ago

So you agree with him? but still tell him to eat shit. You probably failed Core 1 huh?

upvoted 1 times

  **Dat_Oyin** Most Recent  1 month, 1 week ago

A and B because they said physical access meaning ID you will bring with you.

upvoted 1 times

  **Avengers_inc** 5 months, 2 weeks ago

Selected Answer: BF

I honestly feel B and F is the appropriate answers. Chances of getting access denied for a badge reader is kinda lower than that of biometrics (you might have to wipe the sensor and your fingers before it works) then as for Access Control Vestibule, i mean the question specifically said PHYSICAL access... only makes sense that this should be part of the answers. It is specifically deisgned for this purpose... Physical Access

upvoted 2 times

  **yutface** 6 months ago

Selected Answer: AF

A badge can be easily stolen. Man trap is clearly the most secure of them all. And you can't fake biometric scan.

upvoted 2 times

  **phanton** 1 year, 4 months ago

A. Biometric lock - Biometric locks use unique physical characteristics, such as fingerprints or facial recognition, to grant access to a secure area. This provides a high level of security and ensures that only authorized individuals can enter the server room.

B. Access control vestibule - An access control vestibule is a small room or enclosure that is located between two doors. The individual must enter the vestibule, and then be authenticated before being granted access to the server room. This provides an additional layer of security and helps to prevent unauthorized access.

Therefore, the correct answers are A and E (Locking rack).

Badge readers and USB tokens can also provide some level of security, but they are not as effective as biometric locks, access control vestibules, and locking racks. Video surveillance can help to monitor activity in the server room, but it does not prevent unauthorized access.

upvoted 1 times

[-] **StrawberryTechie** 1 year, 4 months ago

Selected Answer: AF

A makes sense because only you have those traits associated to access. F also makes the most sense before a badge reader because that could be stolen. F only allows one person in at a time making sure that the person has access.

upvoted 2 times

[-] **wepaid** 1 year, 7 months ago

AF is the best answer. In simple terms, it's a smoother way of 2-way security. Passing through an Access Control vestibule can already almost guarantee access was given. Then there is the second option which is a biometric lock. This is a very unique way of security.

upvoted 1 times

[-] **imtiazL** 1 year, 10 months ago

A and F is the best option

upvoted 1 times

[-] **enoyl** 1 year, 11 months ago

Selected Answer: EF

E-F is the best physical security in the options.

upvoted 3 times

[-] **will305** 1 year, 11 months ago

I would say A & F. Badges can be lost/stolen. A locking rack is hardly an issue to break into. And the other answers don't make sense. Using biometrics, which is something a person cannot lose/is difficult to clone alongside an access control vestibule seems to be the most secure option for keeping out unwanted persons.

upvoted 8 times

[-] **ciscoxo** 1 year, 10 months ago

I believe the answer is A and B because the question is specifically asking about the server room and not the rack itself. a locking rack is not used to get into the room itself.

upvoted 6 times

Question #66

Topic 1

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

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

Correct Answer: A

[-] **obsidian_fields** **Highly Voted** 1 year, 7 months ago

Selected Answer: A

WPA3 superseded AES after being released.

upvoted 5 times

[-] **JollyGinger27** **Most Recent** 1 year, 7 months ago

Selected Answer: A

WPA3 uses SAE, which is much stronger encryption than AES. Therefore, A is the answer.

upvoted 3 times

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

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

Touch screens -

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

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

Correct Answer: C

  **PatrickH** Highly Voted  1 year, 8 months ago

Its kinda misleading. a 64bit OS can use more than 4GB, a 32 bit can only use up to 4GB of RAM. The question is implying that by changing to 64Bit you can use the full 6GB of Ram that the new Application requires.

upvoted 9 times

  **007madmonk** Highly Voted  1 year, 8 months ago

Selected Answer: C

The 64-bit version of Windows handles large amounts of random access memory (RAM) more effectively than a 32-bit system



upvoted 5 times

  **alexandrasexy** Most Recent  1 year, 9 months ago

Selected Answer: C

C. definitely the RAM

upvoted 3 times

  **examtopics11** 1 year, 9 months ago

Selected Answer: C

32-bit OS max RAM is 4GB.

upvoted 2 times

  **ryanzou** 1 year, 11 months ago

Selected Answer: C

The 64-bit version of Windows handles large amounts of random access memory (RAM) more effectively than a 32-bit system

upvoted 4 times




A user is unable to log in to the domain with a desktop PC, but a laptop PC is working properly on the same network. A technician logs in to the desktop PC with a local account but is unable to browse to the secure intranet site to get troubleshooting tools. Which of the following is the MOST likely cause of the issue?

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

Correct Answer: A

  **wepaid** Highly Voted  1 year, 7 months ago

If the time on the computer's clock is outside of this range, the user will be unable to log in to the domain. Therefore answer is A.
upvoted 8 times

  **Raffaello** Most Recent  8 months, 4 weeks ago

Selected Answer: A

Various methods have been devised to correct drift. The simplest and most reliable way is to implement Network Time Protocol (NTP) and receive accurate time signals from a server that is dedicated to that task and maintained to a very high standard of accuracy.30 Nov 2023
upvoted 2 times

  **Raffaello** 9 months ago

Selected Answer: A



When your server's time doesn't match an authoritative time, such as ntp.org, you have a problem called time drift. This problem is incredibly common and happens slowly over weeks and months. To easily check the time drift, compare the server's current date and time to The Official NIST Time.
upvoted 1 times

  **Zalounfathom** 1 year, 1 month ago

Time Drift: Gradual difference or offset between a computer's system clock and the accurate time maintained by a reference time source or a time server.
upvoted 1 times

  **[Removed]** 1 year, 4 months ago

CompTia states that if a users log in is failing on one device but not on the other, its time drift.
upvoted 4 times

  **JollyGinger27** 1 year, 7 months ago

Selected Answer: A

Having an incorrect, out of range, time will cause connection issues in both the intranet and internet. So, A is most likely the answer.
upvoted 3 times

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

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

Correct Answer: C

  **Dido1963** Highly Voted  1 year, 9 months ago

A, B, D and E would have an effect to all users in this computer.
Only C makes a change only to the one user, who has Problems.
upvoted 10 times

  **[Removed]** 1 year, 5 months ago

isn't adding system memory or virtual ram to that specific solve the problem too?
upvoted 1 times

  **[Removed]** 1 year, 5 months ago

*specific user
upvoted 2 times



  **vshaagar** Most Recent  4 months, 2 weeks ago

Selected Answer: D

i think adding system memory would be the right answer and if this doesn't solve then the rebuild of users profile. Please help me if this is right.
taking the exam in 4 days
upvoted 1 times

  **kwas00** 12 months ago

nice :)
upvoted 2 times

  **JollyGinger27** 1 year, 7 months ago

Selected Answer: C

Like that other comment said, C would only affect the current user and would most be the most likely out of them to solve the problem.
upvoted 3 times

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.

Correct Answer: A

  **JollyGinger27** Highly Voted  1 year, 7 months ago

Selected Answer: A

According to Professor Messer in one of his videos, you can't share files with other computers on the network without turning on the private network.

upvoted 14 times

  **Channon** Highly Voted  1 year, 8 months ago

A public network will hide your computer from other devices on the network and prevent sharing. A private network is considered trusted, allows the computer to be discoverable to other devices on the network. A is correct

upvoted 7 times

  **Raffaello** Most Recent  8 months, 4 weeks ago

Selected Answer: A

Private network?

In Internet networking, a private network is a computer network that uses a private address space of IP addresses. These addresses are commonly used for local area networks (LANs) in residential, office, and enterprise environments. Both the IPv4 and the IPv6 specifications define private IP address ranges



upvoted 1 times

  **alexandrsexy** 1 year, 9 months ago

Selected Answer: D

D. Create a shortcut to public documents.

upvoted 2 times

  **Rockrl** 1 year, 9 months ago

Selected Answer: A



A is the correct answer, Windows computer needed to be on private network to share resource with other computer.

upvoted 5 times

  **matthenao** 1 year, 9 months ago

Can anyone explain?

upvoted 2 times

  **Mar7yi6** 1 year, 7 months ago

They already explained above, the correct answer is A.

upvoted 2 times

Which of the following is a proprietary Cisco AAA protocol?



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

Correct Answer: D

  **vshaagar** 4 months, 1 week ago

Selected Answer: D

TACAS+ - This is the protocol that uses the Accounting, Authorization, and Authentication service (AAA).
upvoted 1 times

  **GabeReal_** 4 months, 3 weeks ago



jksfhyd

upvoted 3 times

  **Raffaello** 9 months ago

Selected Answer: D

TACACS Plus (TACACS+) is a protocol developed by Cisco and released as an open standard beginning in 1993. Although derived from TACACS, TACACS+ is a separate protocol that handles authentication, authorization, and accounting (AAA) services.
upvoted 1 times

  **JollyGinger27** 1 year, 7 months ago

Selected Answer: D

TACACS and TACACS+ are often associated with Cisco since they made it, so D is the answer.
upvoted 1 times

  **Dido1963** 1 year, 9 months ago

<https://en.wikipedia.org/wiki/TACACS>
upvoted 2 times

  **SR1991** 10 months, 2 weeks ago

Did you really use Wikipedia as a source.....
upvoted 4 times

  **TeenDadAres** 6 months ago

hating ass hoe
upvoted 4 times

  **yutface** 6 months ago

Proolly more reliable than ChatGPT - which everyone else here uses.
upvoted 3 times

  **alexandrasexy** 1 year, 9 months ago



Selected Answer: D

D. TACACS+ is the Cisco AAA protocol
upvoted 3 times

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

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

Correct Answer: B

  **Raffaello** 8 months, 4 weeks ago

Selected Answer: B

You can use Disk Utility on your Mac to manage internal and external storage devices. Using Disk Utility, you can: Format and manage volumes on physical storage devices. Create a disk image, a single file you can use to move files from one computer to another or to back up and archive your work



upvoted 4 times

  **rah555** 1 year, 5 months ago

Selected Answer: B

Disk Utility

upvoted 3 times

  **JollyGinger27** 1 year, 7 months ago

Selected Answer: B

According to Professor Messer, you need to use Disk Utility on MacOS to manage disks, so B is the answer.

upvoted 4 times

  **nwachukwu** 1 year, 9 months ago

Disk Utility is correct

upvoted 4 times

A desktop specialist needs to prepare a laptop running Windows 10 for a newly hired employee. Which of the following methods should the technician use to refresh the laptop?

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

Correct Answer: C

  **[Removed]** **Highly Voted**  1 year, 9 months ago

Selected Answer: C

C is the answer. A clean install wipes all of the data on the system and then installs the operating system. The other options will either repair or update the OS, but not delete the data before doing so.

upvoted 5 times



  **princedarcy** **Most Recent**  1 year, 1 month ago

Selected Answer: B

A Repair installation is a type of installation that attempts to replace the existing version of the operating system files with a new copy of the same version. A repair installation will only affect the system files and not any of the user's settings, customizations, or applications. The use of the word refresh in the question strongly implies this installation as this is a refresh of system files.



However, to start fresh for a new employee a clean install may be the best option. In most enterprise environments though a new user account would be created the so purpose of deleting all user data through a clean install would be rendered null.

upvoted 1 times

  **Rixon** 2 weeks, 4 days ago

Your voted B but your ChatGPT output explains that C is correct lmao



upvoted 1 times

  **JollyGinger27** 1 year, 7 months ago

Selected Answer: C

A clean install will help best to have the device software be made new for the employee.

upvoted 4 times

  **dbo98** 1 year, 10 months ago

Selected Answer: C

From what I found online the problem with E is the previous users files and folders stay on the device. Out of all the options C is the best option.

upvoted 3 times

  **imtiazL** 1 year, 10 months ago

answer is E - in place upgrade is the more suitable option in this scenario

upvoted 1 times

  **Rixon** 2 weeks, 4 days ago

Absolutely not. "An in-place upgrade involves upgrading the existing Windows installation to a newer version "

upvoted 1 times

A user reports that a PC seems to be running more slowly than usual. A technician checks system resources, but disk, CPU, and memory usage seem to be fine.

The technician sees that GPU temperature is extremely high. Which of the following types of malware is MOST likely to blame?

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

Correct Answer: B

  **vshaagar** 4 months, 1 week ago



Selected Answer: B

Cryptominer because A,B and D doesnt impact the GPU
upvoted 1 times

  **TeenDadAres** 6 months ago

Selected Answer: B

Think about why we gaymers need to pay a gizz ton of money for a GPU its because of these crypto miners freaks abusing GPUS answer is B
upvoted 4 times

  **Raffaello** 8 months, 4 weeks ago

Selected Answer: B

Graphics Processing Units (GPUs) have been used in the mining process for years, simply because they were more efficient than their immediate counterparts. Today, GPUs, too, have been rendered obsolete in crypto mining by highly-efficient application-specific integrated circuits (ASICs)
upvoted 2 times

  **insanegrizly** 1 year, 2 months ago

Selected Answer: B

Only cryptomining would heat up the GPU.
upvoted 2 times

  **[Removed]** 1 year, 6 months ago

Selected Answer: B

Refer to extrahop.com - "This malware uses a systems CPU and sometimes GPU to perform complex mathematical calculations that result in long alphanumeric strings called hashes. These calculations serve to verify previous cryptocurrency transactions, and successfully solving them can generate a token of currency (like bitcoin)."
upvoted 4 times

A user is experiencing frequent malware symptoms on a Windows workstation. The user has tried several times to roll back the state, but the malware persists.

Which of the following would MOST likely resolve the issue?

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

Correct Answer: B

  **rah555** Highly Voted  1 year, 5 months ago

Selected Answer: B

Reimaging is a process of wiping out everything on a computer's hard drive and reinstalling a fresh copy of the operating system. This will remove all malware and other unwanted software that may have been installed on the computer.

upvoted 6 times

  **TeenDadAres** Most Recent  6 months ago

Selected Answer: B

Seems to be a boot attack only way to solve this is to clean install.

upvoted 1 times

  **Raffaello** 9 months ago

Selected Answer: B

A reimage is the process of installing a new operating system on a machine. This process includes wiping, or clearing, the hard drive entirely, and installing a fresh operating system. When the reimage is complete, it is almost like getting a brand new machine

upvoted 3 times

  **mohdAj** 9 months, 3 weeks ago

Selected Answer: B

Reimaging the workstation involves wiping the system and reinstalling the operating system and software from a clean and trusted source. Options A (Quarantining system files), C (Encrypting the hard drive), and D (Disabling TLS 1.0 support) may not be sufficient to completely eliminate the malware and restore the system's integrity.

upvoted 1 times

  **Bogardinc** 1 year, 9 months ago

Reimaging is the process of installing a new operating system on a machine

upvoted 4 times

  **Q1W2E3R41277** 1 year, 9 months ago

Selected Answer: B



A reimage is the process of installing a new operating system on a machine. This process includes wiping, or clearing, the hard drive entirely, and installing a fresh operating system.

upvoted 3 times

  **jtmonster** 1 year, 9 months ago

this is confusing, they want to take a image now after it is corrupt?

upvoted 2 times

  **sigidy** 1 year, 7 months ago

nope, reimaging will mean using an image file in ISO to install

upvoted 2 times

  **[Removed]** 1 year, 4 months ago

Reimaging would out put a new ISO image on the computer. If you continued to roll it back then then any points of restore that you've made will be infected also, so a whole new image is what its talking about here.

upvoted 4 times

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

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

Correct Answer: C

Dido1963 Highly Voted 1 year, 9 months ago

Selected Answer: C

if implementation failed you need a rollback plan
upvoted 7 times

Skydragon207 Most Recent 8 months, 4 weeks ago

where can I find all the steps of change advisory?
upvoted 1 times

DMC71 1 year, 2 months ago

Is reimagining the same as reformatting?
upvoted 1 times

Delawasp 1 year, 3 months ago

Selected Answer: C

C. Rollback plan should be updated before requesting approval again. If the change advisory board did not approve a requested change due to the lack of alternative actions if implementation failed, then updating the rollback plan would be the logical next step. A rollback plan outlines the steps to be taken if the change does not produce the desired results or causes problems in the system. By updating the rollback plan, the requester can provide the change advisory board with a clear understanding of how they plan to address issues that may arise if the change is implemented. Updating the scope of change, risk level, or end user acceptance may also be necessary, but they are not directly related to the issue of lack of alternative actions in case of failure.
upvoted 3 times

rah555 1 year, 5 months ago

Selected Answer: C

A rollback plan is a contingency plan that outlines the steps that will be taken if a change fails or causes problems.
upvoted 3 times

examreviewer 1 year, 6 months ago

Selected Answer: C

C. Rollback plan

If a change advisory board did not approve a requested change due to the lack of alternative actions if implementation failed, the rollback plan should be updated before requesting approval again. A rollback plan outlines the steps that will be taken to undo the changes if the implementation fails or causes unexpected issues.

The scope of change, risk level, and end-user acceptance may also need to be updated if they are found to be insufficient, but they are not directly related to the lack of alternative actions in case of implementation failure. Updating the rollback plan can help provide assurance to the change advisory board that appropriate measures are in place to mitigate the risks associated with the change.
upvoted 2 times

[Removed] 1 year, 8 months ago

Selected Answer: C

C, it says failed due to lack of alternative options. So c is the answer.
upvoted 4 times

alexandrsexy 1 year, 8 months ago

Selected Answer: B

B. Risk level
upvoted 1 times

simsbow1098 1 year, 11 months ago

Selected Answer: B

The answer should be B.

upvoted 2 times

  **minx98** 1 year, 6 months ago

hahaha this guy's gonna fail

upvoted 1 times

  **Jackybro** 1 year, 11 months ago

I don't think so. The question says "lack of options if implementation fails", which is the literal definition of a backout plan.

upvoted 6 times

  **LayinCable** 1 year, 5 months ago

But he's saying its Risk Level, not Rollback Plan. Risk level is B.

upvoted 2 times

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

- A. UEFI password
- B. Secure boot
- C. Account lockout
- D. Restricted user permissions

Correct Answer: A

  **oatmealturkey** Highly Voted 1 year, 4 months ago

Selected Answer: A

This question was on my exam and I did not get anything wrong in this objective, so A is the right answer.
upvoted 21 times

  **Zalounfathom** 1 year, 1 month ago

When I took the exam, there was no way for me to know what I got right or wrong. so how do you know?
upvoted 8 times

  **Mango7** 11 months, 2 weeks ago

to know you got it right or wrong, they give you a sheet of paper once your test is done which is your result sheet and that includes where you need to improve and such so if that paper didnt list out any of the objectives that mean you got it all right or vice versa.
upvoted 4 times

  **Ade319** 1 year, 4 months ago

Thanks pls share any other answer you are sure of
upvoted 3 times



  **DandyAndy** Highly Voted 1 year, 5 months ago

You could enable secure boot but if you dont have a UEFI password, the user could just disable it. Having a UEFI password and disabling AMD-V and Hyper V is the most logical solution to prevent virtualization.
upvoted 12 times

  **Raffaello** Most Recent 9 months ago

Selected Answer: A

Surface Unified Extensible Firmware Interface (UEFI) replaces the standard basic input/output system (BIOS) with new features including faster startup and improved security. You can use Surface UEFI to manage the firmware features on your Surface.
upvoted 2 times

  **Mozzy83** 10 months ago

Selected Answer: A

Virtualization is enabled in the UEFI BIOS so setting a password for it would prevent it.
upvoted 3 times

  **alexkeung** 1 year ago

Selected Answer: A

Lock UEFI for preventing virtualization technology
upvoted 4 times

  **glenpharmd** 1 year ago

To prevent users from enabling virtual technology on their laptops, particularly from accessing the BIOS/UEFI settings where virtualization options are typically found, the technician should set up a UEFI/BIOS password. This password will restrict unauthorized users from making changes to the BIOS/UEFI settings.

The correct answer is:

A. UEFI password

upvoted 1 times

  **Nabilrrhmn** 1 year, 1 month ago

Selected Answer: A

UEFI password: A password that prevents unauthorized users from accessing or changing the UEFI (Unified Extensible Firmware Interface) settings, which are the modern replacement for BIOS (Basic Input/Output System) settings.
Secure boot: A feature of UEFI that prevents malware from infecting the boot process by verifying that each component is trusted before using it.

A. UEFI password. This is because setting a UEFI password will prevent users from enabling virtual technology on their laptops by blocking them

from accessing the UEFI settings where they can change the virtualization options. The other options are either irrelevant or insufficient for this purpose.

upvoted 3 times

  **solaWONDER** 1 year, 2 months ago

B. Secure boot

Secure boot is a feature available in modern computer systems that ensures only trusted operating systems and software components are loaded during the boot process. It helps protect the system against unauthorized modifications and malware. By enabling secure boot, the system verifies the integrity of the boot process and prevents the execution of unauthorized or unsigned code.


upvoted 1 times

  **Delawasp** 1 year, 3 months ago

Selected Answer: B

B. Secure boot should be implemented to prevent users from enabling virtual technology on their laptops. Secure boot is a UEFI (Unified Extensible Firmware Interface) feature that ensures the integrity of the boot process by only allowing trusted software to run during startup. This can help prevent unauthorized software, such as virtual machines, from being installed and run on the laptop. While a UEFI password, account lockout, and restricted user permissions can also provide some level of security, they may not specifically prevent virtual technology from being enabled on the laptop.

upvoted 2 times

  **LeRoux** 1 year, 4 months ago

Selected Answer: B

The best solution to prevent users from enabling virtual technology on their laptops would be to implement B. Secure Boot.

Secure Boot is a UEFI (Unified Extensible Firmware Interface) feature that ensures the system boots using only software trusted by the PC manufacturer. It helps protect the system against malware and other unauthorized changes to the boot process. By enabling Secure Boot, the technician can prevent the laptop from booting into unauthorized environments, such as virtual machines.

UEFI password (A) would prevent unauthorized access to the system's UEFI settings but would not necessarily prevent the user from enabling virtual technology.

upvoted 2 times

  **[Removed]** 1 year, 4 months ago

I really think A. Block the user from the BIOS and they cant access any Hyper-V or anything of that nature. Booting into a virtual would be disabled.

upvoted 3 times

  **rah555** 1 year, 4 months ago

Selected Answer: B

I will go with B.

upvoted 2 times

  **lordcheekklappur** 1 year, 4 months ago

Option A, UEFI (Unified Extensible Firmware Interface) password, is a security feature that prevents unauthorized users from accessing and modifying the UEFI/BIOS settings. While it can provide an additional layer of security, it does not directly prevent users from installing or running virtual machines on their laptops.

Option D, restricted user permissions, is the better choice because it directly addresses the concern of users installing virtual machines. By limiting user permissions, a technician can prevent users from installing new software, including virtualization software, or modifying system settings that could enable virtualization features. This approach aligns with the company's security policy and effectively prevents users from enabling virtual technology on their laptops.

upvoted 1 times

  **[Removed]** 1 year, 5 months ago

Selected Answer: A

definitely A, block the user from accessing bios, parameters to your liking like ask password if boot on bios not on booting OS, disable virtualization, solve.

upvoted 4 times

  **[Removed]** 1 year, 5 months ago

this is like mdm on a mobile device, restrict rooting, and installing third-party application, You do that by not letting the user to enable developer options settings.

upvoted 1 times

  **jambreaker** 1 year, 5 months ago

Selected Answer: B

To prevent users from enabling virtual technology on their laptops, the technician should implement Secure Boot.

Secure Boot is a feature available in most modern UEFI (Unified Extensible Firmware Interface) firmware that ensures only trusted software is executed on the system during bootup. This helps prevent malicious software, such as rootkits and bootkits, from running on the system.

Secure Boot can also be used to prevent users from enabling virtualization technology. Virtualization requires software to run at a low level of the system, which can be blocked by Secure Boot. By enabling Secure Boot and configuring it to only allow trusted software to run, the technician can prevent users from enabling virtualization technology.


UEFI passwords, account lockout, and restricted user permissions are security measures that can help protect the laptop from unauthorized access, but they do not specifically address the issue of virtualization.

upvoted 2 times

  **[Removed]** 1 year, 5 months ago

but that doesn't mean the user won't be able to access bios and turn it off, then turn on svm or virtualization setting on bios. So setting up uefi password on bios restricting user trying to go to bios all he can do is boot up the os, which solves the default disabled virtualization that can only be turn on by administrator or anyone who put the password on uefi.

upvoted 2 times

  **Boats** 1 year, 5 months ago

Selected Answer: D

You can create a GPO to restrict the use of Virtual Machines and deploy it across your environment.

upvoted 1 times

  **examreviewer** 1 year, 6 months ago

B. Secure Boot

UEFI password, account lockout, and restricted user permissions can also be used to enhance security, but they are not directly related to preventing users from enabling virtual technology on their laptops. An UEFI password can protect the UEFI settings from unauthorized access, but it does not prevent the installation of virtual machine software. Account lockout can prevent unauthorized access to user accounts, but it does not prevent the installation of virtual machine software. Restricted user permissions can limit the actions that users can perform on their laptops, but it does not specifically prevent the installation of virtual machine software.

upvoted 3 times

Question #78

Topic 1

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

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

Correct Answer: A

  **LayinCable** **Highly Voted**  1 year, 5 months ago


If anybody says anything other than A, they are a troll. carry on.

upvoted 5 times

  **realOneThrive** **Most Recent**  3 months, 1 week ago

Instantly got dark highschool flashbacks from this one hahahah definitely A

upvoted 1 times

  **mohdAj** 9 months, 3 weeks ago

Selected Answer: A

This option provides a specific control within the Apple ecosystem to limit the sources from which files can be shared to the executive's device, improving privacy and security.

upvoted 3 times

  **[Removed]** 1 year, 6 months ago

Selected Answer: A

Refer to knowyourmobile.com - "AirDrop does not require an internet connection. Instead, it uses Bluetooth and/or Wi-Fi to make a local area connection between two devices so they can transfer files between them – this is why you can use AirDrop to send files to other people even when on a plane or a subway without an internet connection."

upvoted 2 times

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

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

Correct Answer: D

  **Ace_of_Spaded** Highly Voted 1 year, 6 months ago

Selected Answer: D

Answer is D, question makes no comment of the user receiving a registry error. Simply outlook wont open. Also the PC rebooted overnight in comptia language this means that the PC has updated the OS.

upvoted 11 times

  **Raffaello** Most Recent 8 months, 4 weeks ago

Selected Answer: D

A recent update could include a fix for the problem of not being able to start Outlook. Check for and install any available updates, even if you cannot open Outlook. Select Help > Check for Updates. Choose Update to download and install all available updates

upvoted 1 times

  **Nabilrrhmn** 1 year, 1 month ago

Selected Answer: D

D. Operating system update. This is because operating system updates often require a restart to complete, and they could introduce changes that affect Outlook's performance or stability. The other options are less likely because they are either unrelated to the restart or less common causes of Outlook problems.

upvoted 2 times

  **Sebatian20** 1 year, 3 months ago

D Doesn't make sense. Outlook is part of Windows; why would an update break it's own application?

upvoted 2 times

  **FreddieB** 9 months, 2 weeks ago

Im wondering the same thing. Comptia non sense

upvoted 1 times

  **orsopdx** 1 year, 3 months ago

ChatGPT thinks:

The correct answer is A. Port forwarding.

When a new SOHO router is installed, it is likely that the default settings of the router will prevent external users from accessing the company-hosted public website. Port forwarding is a technique used to allow external users to access resources on a private network. By configuring port forwarding on the router, traffic from the internet can be directed to the internal IP address of the web server hosting the company website.

upvoted 1 times

  **Delawasp** 1 year, 3 months ago

ChatGPT thinks:

B. Invalid registry settings is the MOST likely reason Outlook has stopped functioning. Invalid registry settings are a common cause of Outlook issues, and changes to the registry can occur during system updates or software installations. If the computer restarted overnight, it is possible that the registry settings were changed during the restart, causing Outlook to stop functioning. While malware infections and spam filters can also cause issues with Outlook, they are less likely to be the cause in this scenario. An operating system update could potentially cause issues with Outlook, but it is less likely than invalid registry settings.

upvoted 1 times

  **[Removed]** 1 year, 4 months ago

The compatibility between the application and the operating system would've changed. Only logical answer.

upvoted 2 times

  **rah555** 1 year, 5 months ago

Selected Answer: D

Answer : D

upvoted 2 times

  **[Removed]** 1 year, 6 months ago

Selected Answer: B

Refer to technewstoday.com - "The "Invalid Values for Registry" error occurs when opening a Microsoft Store app, such as Photos, if there are some errors on its corresponding registry entries. You'll usually encounter this issue after you upgrade your system or update the app. An update or upgrade should replace the previous incompatible registry entries and set up new ones."

upvoted 4 times

Question #80

Topic 1

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

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

Correct Answer: B

  **[Removed]** **Highly Voted**  1 year, 5 months ago

Selected Answer: B

It's obviously B. Bollards are essentially little metal or concrete pillars that are spaced far enough apart for people to walk through but not allow a vehicle.

upvoted 9 times

  **dluck** **Highly Voted**  1 year, 4 months ago

what does this have to do with IT?

upvoted 9 times

  **Avengers_inc** 5 months, 2 weeks ago

A+ is like an envelope of the IT world. You gotta know a little of a lot! You have to think hollistically. A+ really is a beast that people dont really give it its accolades. This question is a strong question when it comes to Cybersecurity certifications (For instance the ISC Certified in Cybersecurity Exam, this was one of the questions that came out as well.)

upvoted 1 times

  **DMC71** 1 year, 2 months ago

I agree, what a strange question it's like they are trying to confuse you with it, it may be the security side of the course.

upvoted 2 times

  **Dat_Oyin** **Most Recent**  1 month, 1 week ago


I think is D reasons because they said into the building meaning access to inside the bank. They used vehicle to confuse everyone.

upvoted 1 times

  **jrplANT2048** 6 months ago

bollards? , no it's true.

upvoted 1 times

  **Ham_inclined** 8 months, 2 weeks ago

I don't usually see cars driving into my building

upvoted 1 times

  **Hogslayer** 10 months, 3 weeks ago

B. lol

upvoted 1 times

  **ImpactTek** 1 year, 2 months ago

lolllll

upvoted 1 times

  **[Removed]** 1 year, 4 months ago

oh bollards

upvoted 3 times

After a company installed a new SOHO router, customers were unable to access the company-hosted public website. Which of the following will MOST likely allow customers to access the website?

- A. Port forwarding
- B. Firmware updates
- C. IP filtering
- D. Content filtering

Correct Answer: C

[-]  **[Removed]** Highly Voted  1 year, 9 months ago

C doesn't make sense because you would have to create a list that allows certain IP addresses in (an access list) or blocks certain IP addresses out (a block list). Neither of these options will allow customers (who have various IP addresses incoming from the Internet) to access the website hosted by a web server. Thus, the answer is A because configuring the router to redirect certain port traffic to the web server (port forwarding) will allow customers to access the website via TCP/443.

upvoted 13 times

[-]  **solaWONDER** Highly Voted  1 year, 2 months ago

The answer is A. Port forwarding.

Port forwarding is a technique that allows specific ports on a router to be forwarded to a specific IP address on a local network. This is necessary for external users to access internal resources, such as a company-hosted public website.

upvoted 7 times

[-]  **Ryan_0323** Most Recent  4 months, 3 weeks ago

Selected Answer: C

The answer is C on Quizlet. But I think its correct just because of the way COMPTIA thinks. Its not a super logical Practice because youd need to select all the IP's to filter. But it hypothetically would work. So im going C

upvoted 1 times

[-]  **ImpactTek** 9 months, 1 week ago

firmware updates is the correct answer

upvoted 1 times

[-]  **alexandrasexy** 1 year, 8 months ago

Selected Answer: A

A. Port forwarding


upvoted 4 times

[-]  **Dido1963** 1 year, 9 months ago

Selected Answer: A

A) Port forwarding means, if someone ist connecting the routers IP and there Port 443, the router will forward the IP-Packages to Port 443 of the Web-Server inside of the SOHO-net

upvoted 3 times

[-]  **Rockrl** 1 year, 9 months ago

Selected Answer: A

The answer is since the company website is for external users port forwarding will allow then to connect to internal resources.

upvoted 4 times

Which of the following is the proper way for a technician to dispose of used printer consumables?

- A. Proceed with the custom manufacturer's procedure.
- B. Proceed with the disposal of consumables in standard trash receptacles.
- C. Empty any residual Ink or toner from consumables before disposing of them in a standard recycling bin.
- D. Proceed with the disposal of consumables in standard recycling bins.

Correct Answer: D

  **enoyl** Highly Voted 1 year, 11 months ago

Selected Answer: A

A is the best answer
upvoted 6 times


  **johnnyboi408** Highly Voted 1 year, 11 months ago

shouldn't the answer be A?
upvoted 6 times

  **CodeOnTren** Most Recent 1 month ago

Selected Answer: A

Shouldn't we follow manufacture's procedure
how to dispose of the item ?
upvoted 1 times

  **088b925** 4 months, 4 weeks ago

Selected Answer: C

Option A (proceed with the custom manufacturer's procedure) may be necessary if the manufacturer provides specific instructions or guidelines for disposing of their consumables. Option B (disposal of consumables in standard trash receptacles) is not environmentally friendly and should be avoided if possible. Option D (disposal of consumables in standard recycling bins) may be appropriate if the consumables are completely empty, but it's important to ensure that any residual ink or toner is removed first to avoid contamination of recycling materials. Therefore, option C is the most appropriate and environmentally responsible way to dispose of used printer consumables.
upvoted 1 times

  **PhilCert** 10 months, 3 weeks ago

Selected Answer: A

It's A, I work as IT support in a lawer firm, we use everything Xerox when it comes to printers. Theres a separate container, managed by Xerox, where we dispose of used toners and other printer related consumables.
upvoted 5 times

  **007madmonk** 1 year, 8 months ago

It is worded badly. The question is referring to paper media as the consumables. But that is kinda half right as toner is also a consumable.
upvoted 3 times

  **yutface** 6 months ago

I really don't think that is true.
upvoted 1 times

  **alexandrasexy** 1 year, 8 months ago

Selected Answer: A

A. Proceed with the custom manufacturer's procedure.
upvoted 3 times

  **jtmonster** 1 year, 9 months ago

Answer is A. Comptia should define what a consumable is and what it is not.
upvoted 5 times

  **ryanzou** 1 year, 11 months ago

Selected Answer: A

A is correct
upvoted 6 times

An Android user reports that when attempting to open the company's proprietary mobile application, it immediately closes. 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. Uninstall and reinstall the application.
- B. Reset the phone to factory settings.
- C. Install an alternative application with similar functionality.
- D. Clear the application cache.

Correct Answer: D

  **danishkayani11** Highly Voted 1 year ago

D. Clear the Cache

Android apps have clear cache button when you go into app details. uninstalling and reinstalling the app might delete all the related company databases and files while deleting cache will only delete temporary data. you might need to login again.

upvoted 7 times

  **maggie22** Most Recent 1 year ago

If you were the technician, what would you do after the user said that the issue persists, even after rebooting the phone? I would Clear the application cache to verify what the user stated is true. Then I would uninstall and reinstall the application.

upvoted 3 times

  **Fannan** 1 year ago

Selected Answer: A

Since the application is misbehaving after a reboot, it probably should be reinstalled.

upvoted 1 times

  **rah555** 1 year, 5 months ago

Selected Answer: D

Clear the application cache it is best way!

upvoted 4 times

  **pmneggers** 1 year, 5 months ago

D. Reinstalling an app simply means uninstalling the app from the phone and then installing it back. For the unaware, uninstalling an app means to completely delete the app from the phone. You will have to install the app again on your phone if you want to use it. The installed app will behave and look like you installed it the first time. That is, you will have to set up the app again. Uninstalling an app removes the app data, cache, and user data. Therefore through process of elimination, I would say D as its not all user data and app data lost, only the cache .

upvoted 2 times

  **Mukthadir** 1 year, 5 months ago

Selected Answer: D

I'm going with D. Questions says which of the following steps should a systems administrator attempt FIRST? So I assume clear cache first, if that doesn't resolve the issue then you can proceed to uninstall and reinstall the app.

upvoted 2 times


  **oatmealturkey** 1 year, 6 months ago

Selected Answer: A

Think about it for a minute. When you reboot any computer including a phone, the cache is empty because it's in RAM. So that has been done already according to the question.

Now, think about how an app works. Would uninstalling & reinstalling an app actually result in data loss? Very unlikely.

upvoted 1 times



  **Riderzz** 1 year, 4 months ago

Also, this cache is used by the application and it won't be cleared after a reboot. If you have an android phone, go into app info>storage>view data and cache being taken. Then reboot your phone, the cache for the app will be the same.

If the app requires a login/account, then sure data won't be lost but re-installing would be data loss without an account.

The answer is D.

upvoted 3 times

  **minx98** 1 year, 6 months ago

Selected Answer: A

I would go with A. The question states that the user has already rebooted the phone, so I would assume the application cache is cleared already so it can't be D



upvoted 2 times

  **ronniehaang** 1 year, 6 months ago

Selected Answer: D

The first step the systems administrator should attempt is to clear the application cache, as this may resolve the issue without causing any data loss. To clear the cache on an Android phone, the user can go to "Settings," then "Apps & notifications," and select the problematic application. From there, they can select "Storage & cache" and then "Clear cache." If this step does not resolve the issue, the administrator can consider other options such as uninstalling and reinstalling the application or resetting the phone to factory settings, but these steps should be taken with caution as they may result in data loss. Installing an alternative application is not a recommended solution, as it may not have the same level of security or functionality as the company's proprietary application.



upvoted 2 times

  **Rafid51** 1 year, 6 months ago

Selected Answer: D

because over time, the cache gets filled with too much data and can cause the application to malfunction or crash. So clearing the cache can resolve this issue.

upvoted 1 times

  **lilbuu** 1 year, 7 months ago

A. Uninstall and reinstall the application.

Explanation:

A. Uninstalling and reinstalling the application is the first step that a systems administrator should attempt to resolve the issue. This step will remove any corrupted files or settings that may be causing the application to crash and will also ensure that the latest version of the application is installed. This step should be attempted before other options are considered as it will often resolve the issue without losing any data or functionality.

upvoted 1 times

  **Cuddles** 1 year, 7 months ago

Clearing the cache is the easier first step for sure

upvoted 4 times

  **minx98** 1 year, 6 months ago

Yes but the question says the phone has already been rebooted, so there is nothing in the cache

upvoted 2 times

  **[Removed]** 1 year, 5 months ago

Are you sure?

upvoted 1 times

  **StrawberryTechie** 1 year, 4 months ago



Research the question "does rebooting my phone clear the cache?" I did this and it said that it does in fact clear the cache. I am going with A.

upvoted 1 times

  **StrawberryTechie** 1 year, 4 months ago

However, regardless of whether or not the phone was rebooted, it asks "what would the technician do first?" So now I am back to thinking the answer is D. Just because that is the least invasive and simplest thing to try first. I am so torn.

upvoted 1 times

  **Rural0** 1 year, 7 months ago

The Application contains critical info that cannot be lost if you do a reinstall you may lose that info therefore clearing the cache is a less invasive step that will preserve the info

upvoted 4 times

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

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

Correct Answer: A

  **Dido1963** 1 year, 9 months ago

Selected Answer: A



<https://www.metageek.com/training/resources/why-channels-1-6-11/>
upvoted 2 times

  **Dido1963** 1 year, 9 months ago


<https://www.metageek.com/training/resources/why-channels-1-6-11/>
upvoted 1 times

  **TiaAnizia** 1 year, 9 months ago

Is this answer correct?
upvoted 1 times

  **LayinCable** 1 year, 5 months ago

Yes, as changing the wifi channels from the channels that all your neighbors are using will mitigate how much interference you will get on your own wifi, thus making it faster/more responsive.
upvoted 9 times

  **sigidy** 1 year, 7 months ago

yes it is.
upvoted 2 times

A user rotates a cell phone horizontally to read emails, but the display remains vertical, even though the settings indicate autorotate is on. Which of the following will MOST likely resolve the issue?

- A. Recalibrating the magnetometer
- B. Recalibrating the compass
- C. Recalibrating the digitizer
- D. Recalibrating the accelerometer

Correct Answer: D



  **Newfy123** Highly Voted  1 year, 7 months ago

Selected Answer: D

Accelerometers in mobile phones are used to detect the orientation of the phone.
upvoted 11 times

  **amityGanoofib** Most Recent  5 months, 3 weeks ago

for those curious like i was "A magnetometer is a device that measures magnetic field or magnetic dipole moment. Different types of magnetometers measure the direction, strength, or relative change of a magnetic field at a particular location." answer is Accelerometer btw
upvoted 3 times



  **Raffaello** 8 months, 4 weeks ago

Selected Answer: D

The accelerometer plays a crucial role in auto rotate. It's a hardware component present in your device that detects changes in its physical position. When you tilt your device, the accelerometer senses this movement and communicates it to the operating system, which then rotates the screen accordingly
upvoted 3 times

  **supermanklly** 1 year, 8 months ago

is this correct
upvoted 1 times

  **Rural0** 1 year, 7 months ago

Yes its correct
upvoted 3 times

A Microsoft Windows PC needs to be set up for a user at a large corporation. The user will need access to the corporate domain to access email and shared drives. Which of the following versions of Windows would a technician MOST likely deploy for the user?

- A. Windows Enterprise Edition
- B. Windows Professional Edition
- C. Windows Server Standard Edition
- D. Windows Home Edition

Correct Answer: A

  **JollyGinger27** Highly Voted  1 year, 7 months ago

Selected Answer: A

Windows Enterprise was designed for mass deployment and has the most features, so the answer is A.
upvoted 5 times

  **088b925** Most Recent  4 months, 4 weeks ago

Selected Answer: B

Option A (Windows Enterprise Edition) may also be used in some corporate environments, particularly in larger organizations that require additional management and security features. However, Windows Professional Edition is more commonly deployed for standard users.
upvoted 1 times

  **joe_sol_arch** 1 year, 1 month ago


A. Windows Enterprise Edition

Windows Enterprise Edition is typically used in large organizations as it includes advanced features and capabilities for managing and securing devices within a corporate network. It supports domain joining, which allows the user to connect their PC to the corporate domain, granting access to email and shared drives hosted on the corporate network. Additionally, Enterprise Edition includes various management and security tools that are essential for large-scale IT environments.
upvoted 2 times

  **solaWONDER** 1 year, 2 months ago

B. Windows Professional Edition

Windows Professional Edition is the version of Windows that is commonly used in business environments and provides the necessary features and functionality to connect to a corporate domain. It includes features such as domain join, group policy management, and support for network file sharing and access to corporate resources like email and shared drives.
upvoted 1 times

  **Avengers_inc** 5 months, 2 weeks ago

Key word being "Large Organization", Enterprise is your answer
upvoted 2 times

  **GryffindorOG** 1 year, 9 months ago

You can also use Professional
upvoted 1 times

  **LayinCable** 1 year, 5 months ago

Pro does have domain access but yes, the key words are "large corporation," which means Enterprise will be your go-to for the user.
upvoted 3 times

  **LayinCable** 1 year, 5 months ago

*yes, but
upvoted 2 times

  **[Removed]** 1 year, 9 months ago

Not really, as Enterprise allows mass deployment via site-based licenses and other tools such as AppLocker to control which applications can run or not.

Also, it is a "user for a large corporation." Common sense is to choose A.
upvoted 7 times

  **RevItRob** 1 year, 9 months ago

Exactly! Always read the questions carefully to pick the best answer.
upvoted 1 times

An Android user contacts the help desk because a company smartphone failed to complete a tethered OS update. A technician determines there are no error messages on the device. Which of the following should the technician do NEXT?

- A. Verify all third-party applications are disabled.
- B. Determine if the device has adequate storage available.
- C. Check if the battery is sufficiently charged.
- D. Confirm a strong internet connection is available using Wi-Fi or cellular data.

Correct Answer: D

JJ_Stone Highly Voted 1 year, 3 months ago

If you don't have enough storage wouldn't you get an error?
upvoted 17 times

examreviewer Highly Voted 1 year, 6 months ago

Selected Answer: C

Verifying all third-party applications are disabled (Option A) and determining if the device has adequate storage available (Option B) may be necessary steps in some troubleshooting scenarios, but they are less likely to be the issue if there are no error messages on the device.

Confirming a strong internet connection is available using Wi-Fi or cellular data (Option D) may also be necessary for downloading the update, but since there are no error messages, it is less likely to be the issue.

So C.

upvoted 8 times

joeshmungus 3 months, 2 weeks ago

it says a tethered update, so the device is plugged in, most likely charging
upvoted 2 times

CodeOnTren Most Recent 1 month ago

Selected Answer: B

not having enough storage can cause an error
upvoted 1 times

danishkayani11 2 months, 3 weeks ago

Selected Answer: C

No Error message might indicate some disruption i.e power saving modes or even shutdown during the update process. C sounds more plausible. My first choice would be Low storage issue which is very common but that would almost always trigger an error. can't be an internet issue because it's a tethered connection which means software is being loaded to the phone via a usb connection to the pc (most probably through offline copy). I'll go with C

upvoted 1 times

Jay23AmMonsIV 3 months ago

Selected Answer: B

OS updates often require a significant amount of storage space to download and install. If there is not enough storage available on the device, the update cannot be completed. Checking for adequate storage is a straightforward and crucial step in troubleshooting the issue.

Mnemonic to Remember:

"Space First for Safe Updates"

This phrase helps you remember that ensuring sufficient storage space is a critical first step when troubleshooting failed OS updates.

upvoted 1 times

SDXIN 4 months, 2 weeks ago

Selected Answer: D

No error message, then it could be network connection issue.
upvoted 2 times

jsmthy 5 months, 2 weeks ago

Selected Answer: B


Eliminate C and D because the OS update is TETHERED. Device is plugged in and downloading through the wire, not wireless. Eliminate A because it is irrelevant to an OS update.

upvoted 4 times

amityGanoofib 5 months, 3 weeks ago

really annoying that they call a usb connection between phone and computer "tethered," makes it hard to find info to answer this question. trying to reword it without the word tethered also brings up a bunch of stuff unrelated to this question. my instinct is to say B, but i have no idea if an error message would show up or not when updating by connecting to a computer, i know it would if you were doing a regular OS update over cellular connection. the battery shouldnt be to much of a problem cause the computer would power the phone over the USB connection, unless it was at like 1 percent and was about to die i guess. the computer it is connected to would need wifi or ethernet but the phones cellular data wouldnt matter am i right? weird question.

upvoted 2 times

  **bdemps98** 5 months, 3 weeks ago

Selected Answer: D

I believe it is D. Reasoning is deduced from other answers being false from my own experience.



A. Doesn't make sense.

B. It wouldn't let you download the application without enough available space.

C. It's tethered aka power source/plugged in.

D. While its possible to have ethernet and power tethered to an Android device, its highly unlikely, so a failed update that was initiated is likely due to bad connectivity.

upvoted 1 times

  **igorclapa** 5 months, 3 weeks ago

Selected Answer: B


Leaning strongly on "B" as the proper answer.

If you read the question carefully, the update was attempted on a TETHERED connection, meaning plugged into a PC or something similar. The question gives us no indication of the technician changing/attempting a wireless update instead.

Only logical answer left is checking to see if the device storage is full.

Does it make 100% sense? Not entirely, I can't recall a device I used that didn't provide some sort of error code/alert but here we are.

upvoted 1 times

  **Heberm** 6 months, 2 weeks ago

bullshit worded questions like this are what piss me off the most about comptia

upvoted 4 times

  **crazymonkeh** 6 months ago


Agreed, but the good news is, you still get partial pts if you get the 2nd best answer. That's why the test is graded on a scale to 900, rather than 1-100%.

upvoted 1 times

  **Angelo42** 5 months, 3 weeks ago

makes sense, how did you find out that they give partial points

upvoted 1 times

  **didi_10** 8 months, 1 week ago

Selected Answer: C


the content has already been downloaded which means no extra storage is needed to complete the update. The device needs to have sufficient battery life to update the content. So it's C

upvoted 1 times

  **yutface** 7 months, 1 week ago

Doesn't say anywhere that it has already been downloaded.

upvoted 2 times

  **Dave93266** 8 months, 3 weeks ago

Selected Answer: D

A) doesn't make sense in this scenario.

B) would produce an error.

C) I feel like the user would have noticed if their phone died during an installation.

D) is the only one that makes sense.

upvoted 3 times

  **yutface** 6 months ago

Tethered means it won't use wifi or cell data. B would produce an error. Stupid as it sounds, I think CompTIA might be pointing toward C. What the user would notice or not is irrelevant to the question - would it stop the phone from updating? Yes.

upvoted 2 times

  **Chavozamiri** 9 months, 1 week ago

Selected Answer: D

There are no error messages on the device.

that's the point on this question!

upvoted 1 times

  **CookieChip** 10 months, 3 weeks ago

Selected Answer: D

B and C would generate a message. So it should be D

upvoted 1 times

  **CookieChip** 11 months ago

Selected Answer: D

Not enough storage and low battery would generate an error.
So it should be D.

upvoted 1 times

  **Christianjr35** 12 months ago

This question makes no sense.

B and C makes the most sense, here is why.

It mentions tether update, which rules out D, wifi or cellular data as update is through tethering from another device that assumes that it has the OS file.

It also rules out A, because why you don't have to perform an update.

But, both B and C will show error messages... B will say not enough storage, C will say unable to update please charge...

Take a guess between b and c lol

upvoted 1 times

Question #88

Topic 1

A technician just completed a Windows 10 installation on a PC that has a total of 16GB of RAM. The technician notices the Windows OS has only 4GB of RAM available for use. Which of the following explains why the OS can only access 4GB of RAM?

- A. The UEFI settings need to be changed.
- B. The RAM has compatibility issues with Windows 10.
- C. Some of the RAM is defective.
- D. The newly installed OS is x86.

Correct Answer: D

  **LayinCable** **Highly Voted**  1 year, 5 months ago

Selected Answer: D

If anybody says anything other than D, they are indeed doing what we call trolling.

upvoted 8 times

  **Dido1963** **Highly Voted**  1 year, 9 months ago

Selected Answer: D

the 32-Bit-Version (x86) of Windows supports only 4 GB RAM.

So you should install the x64 Version

upvoted 7 times

  **igorclapa** **Most Recent**  5 months, 3 weeks ago

x86 = 32bit = 4gb MAXIMUM available RAM



upvoted 2 times

  **Jscho** 7 months, 3 weeks ago

Selected Answer: D

this technician needs to be fired

upvoted 3 times

  **igorclapa** 5 months, 3 weeks ago

based boss

upvoted 1 times

A call center handles inquiries into billing issues for multiple medical facilities. A security analyst notices that call center agents often walk away from their workstations, leaving patient data visible for anyone to see. Which of the following should a network administrator do to BEST prevent data theft within the call center?

- A. Encrypt the workstation hard drives.
- B. Lock the workstations after five minutes of inactivity.
- C. Install privacy screens.
- D. Log off the users when their workstations are not in use.

Correct Answer: B

  **DoesItEvenMatter** Highly Voted  1 year, 6 months ago

How could D not be the BEST way to prevent data theft here?
upvoted 10 times

  **igorclapa** 5 months, 3 weeks ago

Because option D goes way further than necessary. Locking the device is enough, what if the technician stepped away for a couple of minutes? Having to login every time you step away is pretty cumbersome.
upvoted 1 times

  **Skimbeeble** 1 week ago

Its common practice to make sure you lock your screen while leaving a workstation to prevent any type of security breaching. 5 mins would be too far for this type of practice. Therefore, I believe D would be the correct answer here.
upvoted 1 times

  **mcgirthius** 1 year, 4 months ago

Well, it doesn't define what "in-use" means in the answer. If the technician is logged in, technically the workstation is in-use. So, if they walked away after logging in the computer is still in use and displaying information.
The only answer here that actually provides a solution in the text is a 5-minute lockout timer. Because D is worded so poorly, I would always choose B here.
upvoted 1 times

  **randomh1p** 11 months, 2 weeks ago

because D states= log off the users when their workstations are not in use. (meaning someone else have to log off from their workstation when its not in use and not the user itself). And If admin or supervisor is in the room when the user leaves they might logg off different user.
upvoted 1 times

  **Philco** Most Recent  2 weeks ago

I thought D would be a good answer
five minutes is still a pretty long time . Anything can happen in 5-min
I would say Bor D accomplish the same thing. Because D did not mentioned time, I would favour D
upvoted 1 times

  **CodeOnTren** 1 month ago

Selected Answer: B

This should be the right answer it mentions the agent walking away , so a privacy screen wouldn't prevent someone walking up to the computer and steal data , so locking the screen definitely the best answer
upvoted 1 times

  **jade290** 2 months ago

Selected Answer: C

Privacy screens block visibility of anyone not looking directly at the screen. Locking the workstations only works after 5 minutes. It is definitely C.
upvoted 1 times

  **Jay23AmMonsIV** 3 months ago

What is the difference between this and the Police Officer question? It has the same cintext?
upvoted 1 times

  **Jackphygurz** 1 month ago

the options are slightly different in the sense that, in the police officer's question, there is an option for the police office to lock the system before leaving using a combination key (windows key + L).
upvoted 1 times

  **vshaagar** 4 months, 1 week ago

Selected Answer: C

Why cant it be C? Having a privacy screen eliminates all the shoulder surfing attacks.

upvoted 4 times

  **joeshmungus** 4 months ago

Agreed, I believe this is the issue this question is adressing

upvoted 1 times

  **Christianjr35** 12 months ago

Answer is B. It says call centre agentS, does the security analyst really want to log off all the agents' account manually when each of them leave?

upvoted 1 times

  **EngAbood** 1 year ago

why i have to walk to user device and lock his computer ? what about if there are many of htem there ? so i will go for B :(

upvoted 1 times

  **Wildhunt37** 1 year, 3 months ago

It's a poorly worded answer because D almost sounds like the administrator would have to personally log off the users if they noticed unattended systems but I still think it's the correct answer due to the information below.

Log off when not in use—A lunchtime attack is where a threat actor is able to access a computer that has been left unlocked. Policies can configure screensavers that lock the desktop after a period of inactivity. Users should not depend on these, however. In Windows, START+L locks the desktop. Users must develop the habit of doing this each time they leave a computer unattended.

upvoted 2 times

  **yggggg** 1 year, 4 months ago

Locking the workstations after five minutes of inactivity still leaves a 5 minute window for data theft. I'll go with D.

upvoted 4 times

  **IT_isfornerds** 1 year ago

LOL

I thought the same, but who is locking these computers? The technician? Best chance at mitigation is answer B.

upvoted 1 times

  **[Removed]** 1 year, 5 months ago

B anD should be on one sentence haha weird choices

upvoted 2 times

  **inturist** 1 year, 6 months ago

ChatGPT says:

The BEST option to prevent data theft within the call center is to lock the workstations after five minutes of inactivity. This ensures that unauthorized individuals cannot access the patient data when the agents are away from their workstations. Encrypting the workstation hard drives and installing privacy screens can also provide some level of protection, but they do not address the issue of agents leaving their workstations unattended. Logging off users when their workstations are not in use may also provide some level of protection, but it can be inconvenient for the agents to have to log in every time they return to their workstation. Therefore, locking the workstations after a period of inactivity is the most effective and practical solution to prevent data theft.

upvoted 2 times


  **AntMan777** 1 year, 6 months ago

I just Char GPT'd this and got this:

Log off the users when their workstations are not in use.

why? Logging off the users when their workstations are not in use is the best way to prevent data theft in the call center. Encrypting the workstation hard drives, locking the workstations after five minutes of inactivity, and installing privacy screens will not prevent data theft.


upvoted 1 times

  **Rafid51** 1 year, 6 months ago

Selected Answer: B

The best solution here is to lockout the screen after 5 minutes of inactivity.

upvoted 2 times

  **Cuddles** 1 year, 7 months ago

I think it's privacy screens since the question seems to emphasize being able to see the screens while they are away. But locking out after 5 minutes still leaves 5 minutes of downtime where anyone can see their screens walking by.



upvoted 3 times

  **Dido1963** 1 year, 9 months ago

Selected Answer: B

privacy screens only help, that you can read only if you look perpendicular to the screen. So everybody can read, if he moves a little bit

upvoted 3 times

  **dimeater** 1 year, 9 months ago

Selected Answer: B

Read the question... Privacy screens prevent shoulder surfing.

upvoted 2 times

  **MacheenZero** 1 year, 9 months ago

Privacy Screens help prevent shoulder surfing. Locking the work station after inactivity is the correct answer
upvoted 2 times

Question #90

Topic 1

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

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

Correct Answer: C

  **rah555** 1 year, 5 months ago

Selected Answer: C

A full backup of the data that is stored off site in cold storage.
upvoted 2 times

  **dimeater** 1 year, 9 months ago

Selected Answer: C

Off site storage is most secure
upvoted 2 times

  **dimeater** 1 year, 9 months ago

off site storage is correct
upvoted 2 times

  **NadirM_18** 1 year, 3 months ago

In cloud computing, cold storage environments are object storage areas designed for data that is accessed infrequently, such as information retained long-term for business or compliance purposes and archived files
upvoted 3 times

  **jtmonster** 1 year, 9 months ago

cold or cloud storage?
upvoted 2 times

  **[Removed]** 1 year, 6 months ago


Cold storage, meaning that it is stored in a secure location that is not connected to the internet.
upvoted 3 times

  **LayinCable** 1 year, 5 months ago

And its also chilly in there, and data likes to be cold. Just sayin'
upvoted 2 times

  **Mango7** 11 months, 1 week ago

and they can be froze and impossible to decrypt.
upvoted 1 times

  **Waldem** 8 months, 2 weeks ago

I like it!
upvoted 1 times

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.


Correct Answer: A

  **Rixon** 2 weeks, 3 days ago

I read "Key combination" and I was thinking about physical keys instead of keys on the keyboard.. smh.
upvoted 1 times

  **MikeGeo** 5 months, 3 weeks ago

Former police officer here: our "workstation" was frequently "our vehicle"; and the best way to solve the issue in question often was "have a key fob auto lock the vehicle when fob goes too far away from vehicle". I understand that's not the question here, but I figured y'all would like a practical opinion. Yes, I'm aware that this would require the vehicle to use a fob; but this isn't the 70's anymore.
upvoted 1 times

  **Waldem** 8 months, 1 week ago

If a police officer often leaves a workstation for several minutes at a time, the best way to secure the workstation quickly when walking away is to use a key combination to lock the computer. This will prevent unauthorized access to the computer while the officer is away .

Ensuring no unauthorized personnel are in the area is not a practical solution as it is difficult to control who enters the area. Configuring a screensaver to lock the computer automatically after approximately 30 minutes of inactivity is a good security practice, but it is not the best solution to the problem described in the question. Turning off the monitor to prevent unauthorized visibility of information is also not a practical solution as it does not prevent unauthorized access to the computer.

Therefore, the correct answer is A. Use a key combination to lock the computer when leaving.
upvoted 2 times

  **Raffaello** 9 months ago

Selected Answer: A

Press the Ctrl + Alt + Del
These days, this three-key shortcut can perform a number of tasks, one of which is to lock Windows. Ctrl + Alt + Del should all be pressed simultaneously. Options should show on a screen
upvoted 1 times

  **Mango7** 11 months, 1 week ago



Selected Answer: A

key combo = win+L
upvoted 2 times


  **Fannan** 1 year ago

Selected Answer: A

Out of the answers given: The only one that would make sense is to force a screen lock when you leave the system
upvoted 1 times

  **Kinjie** 1 year, 2 months ago

A is correct answer
upvoted 1 times

  **Nonickname176798512478** 1 year, 2 months ago

Why isn't it D? D sounds plausible to me
upvoted 1 times

  **Zalounfathom** 1 year ago

Turning off the monitor does not lock the computer
upvoted 1 times

  **Stormcloudlive** 1 year, 1 month ago

Because anyone else who comes along could just turn on the monitor, the monitor requires no password to turn back on.
upvoted 3 times

[-]  **Dido1963** 1 year, 9 months ago

Selected Answer: A

One possibility is to press WIN + L
(or you press CTRL + ALT + DEL and chose Lock)

upvoted 4 times

[-]  **Channon** 1 year, 9 months ago

Selected Answer: A

A is correct

upvoted 1 times

[-]  **Thejphall** 1 year, 10 months ago

Answer stated is correct. I assume its the something similar in other OS's but on windows you can just hit WinKey+L to quickly lock your screen.

upvoted 2 times

[-]  **Sarooor** 1 year, 11 months ago

A looks the correct and best answer in this senior

upvoted 3 times

[-]  **johnnyboi408** 1 year, 11 months ago

what's the right answer to this?

upvoted 1 times

A homeowner recently moved and requires a new router for the new ISP to function correctly. The internet service has been installed and has been confirmed as functional. Which of the following is the FIRST step the homeowner should take after installation of all relevant cabling and hardware?

- A. Convert the PC from a DHCP assignment to a static IP address.
- B. Run a speed test to ensure the advertised speeds are met
- C. Test all network sharing and printing functionality the customer uses.
- D. Change the default passwords on new network devices.

Correct Answer: D

  **racoონice12** Highly Voted 1 year, 4 months ago

Gee getting hacked or fast internet, you choose lol
upvoted 6 times

  **GRONDBOTTER** 9 months, 2 weeks ago

best comment i have read so far
upvoted 1 times

  **alexandrasexy** Most Recent 1 year, 8 months ago

Selected Answer: D

D. Change the default passwords on new network devices.
upvoted 3 times

  **Dido1963** 1 year, 9 months ago

Selected Answer: D

They ask, what you should do FIRST. At First you change the password of the new Router. After that you can check the speed of the connection
upvoted 3 times

  **matthenao** 1 year, 9 months ago

Selected Answer: D

Definitely D, you need a secure network before good speeds
upvoted 4 times

  **cooldude0901** 1 year, 10 months ago

Selected Answer: B

Shouldn't it be B? Most people would check their speed after internet has been installed
upvoted 1 times

  **Thejphall** 1 year, 10 months ago

While that is probably what happens most often in the real world this is a question on a comptia exam so its probably being looked at from a security perspective. Changing default passwords is the "FIRST" thing that should be done to secure the network.
upvoted 6 times

While browsing a website, a staff member received a message that the website could not be trusted. Shortly afterward, several other colleagues reported the same issue across numerous other websites. Remote users who were not connected to corporate resources did not have any issues. Which of the following is MOST likely the cause of this issue?



- A. A bad antivirus signature update was installed.
- B. A router was misconfigured and was blocking traffic.
- C. An upstream internet service provider was flapping.
- D. The time or date was not in sync with the website.

Correct Answer: D

  **jackjack007** Highly Voted 1 year, 9 months ago

Selected Answer: D

There are three reasons for this error: 1. commonly it is because of certificate error, so certificate needs to be updated. 2. SSL/TLS that browser cannot make a secure connection, so we see this error. 3. the third reason is synchronization of date and time. Definitely D is the answer
upvoted 14 times

  **yutface** 7 months, 1 week ago

Would multiple computers would experience this issue at the same time?
upvoted 1 times

  **amityGanoofib** 5 months, 3 weeks ago

i think the problem is the uh, forgot what it was called the server that keeps time for the network, that thing messed up, so the time for all the computers on the network was off, so when they saw the time for the websites were off they thought the sites were sketchy.
upvoted 1 times

  **amityGanoofib** 5 months, 3 weeks ago

NTP server thats what meant, had to look it up.
upvoted 1 times

  **ollie93** Most Recent 4 months ago

Selected Answer: B

The MOST likely cause of the issue where staff members receive messages that websites cannot be trusted, especially if remote users not connected to corporate resources do not have the issue, is:

B. A router was misconfigured and was blocking traffic.

A misconfigured router can lead to various network issues, including blocking legitimate traffic to certain websites. This can result in users receiving messages that the website is not trusted due to the router incorrectly handling SSL/TLS certificates or other security-related configurations. Verifying the router configuration and ensuring that it allows traffic to trusted websites should help resolve the issue for affected staff members.
upvoted 1 times

  **yutface** 6 months ago

Selected Answer: A

Looked around a bunch, including multiple AI answers. This one made the most sense to me.
A. A bad antivirus signature update was installed.

When users across multiple systems experience issues with websites being flagged as untrusted shortly after one user encounters the problem, it suggests a common factor affecting all users. A bad antivirus signature update could cause this behavior by incorrectly flagging legitimate websites as untrusted, leading to warnings or blocks when users attempt to access them.

Options B, C, and D are less likely to be the cause of the issue:

Option B, a misconfigured router blocking traffic, would likely result in more widespread connectivity issues beyond just website trust messages. Option D, the time or date not being in sync with the website, could cause SSL certificate validation issues, but it would typically not manifest as a widespread problem across numerous websites. Additionally, it's less likely to be the cause if remote users unaffected by corporate resources are not experiencing the same issue.
upvoted 2 times

  **amityGanoofib** 5 months, 3 weeks ago

if it was a bad antivirus signature update i would think it would affect maybe one or a few websites, not many of them right? also i misread the question at first and thought it meant users who like were using RDP, but it just means users who are on their own network doing their own thing, not connected to the corporate network at all. so if there's an issue with the time server dealio it wouldnt affect them just users on the corporate network.
upvoted 1 times

  **amityGanoofib** 5 months, 3 weeks ago

NTP server thats what i meant

upvoted 2 times

  **ap___** 6 months, 2 weeks ago

Selected Answer: D



I thought it was B at first until i read "nearly all websites that use encrypted data need your computer to be synchronised to the server as a security measure. So you can do a lot of things with the wrong date set, but not social media, buying items, or banking"

upvoted 1 times

  **Annamarie0408** 6 months, 4 weeks ago

The answer is B as users not on the corporate wifi had no issues.

upvoted 1 times

  **Abe_Santi** 8 months, 3 weeks ago

Selected Answer: B

After reading the question multiple times, I will have to say that B. A router was misconfigured and was blocking traffic, is the correct answer. The questions states that it's not one user but multiple users having the same issues and while trying to access multiple sites, while others who are not on the company's network were not having any issues. If it was just one person then I would agree that D would have been the most logical reason but since it's multiple users that it has to be a misconfigured router issue.

upvoted 2 times

  **JTur** 11 months ago

Considering these points, a bad antivirus signature update is a plausible explanation. Antivirus software often includes features that scan websites for potential threats and determine their trustworthiness. If a recent antivirus signature update contained an error or false positive, it could incorrectly flag websites as untrusted or potentially unsafe. This would result in the consistent warnings experienced by multiple colleagues across different websites.

So its A

upvoted 1 times

  **Fannan** 1 year ago

Selected Answer: D

D. The time or date was not in sync with the website.

This issue is likely related to SSL/TLS certificates used by websites. When a device's time and date are not synchronized correctly with the actual time, SSL/TLS certificates may appear as expired or not trusted, leading to security warnings. SSL/TLS certificates have validity periods, and if the device's clock is significantly off, it can cause these certificates to appear invalid, resulting in the warning message about the website not being trusted.

Remote users who were not connected to corporate resources might not have experienced the issue because their devices' clocks were likely synchronized correctly with internet time servers.



It's a common security practice to ensure that devices have accurate time and date settings to prevent these types of issues with SSL/TLS certificates.

upvoted 4 times

  **ComPCertOn** 1 year ago

i thought we cannot just assume things with this exam ? i still think it is B

upvoted 2 times

  **Crezzki** 1 year, 4 months ago

Selected Answer: B

B. A router was misconfigured and was blocking traffic.

The most likely cause of this issue is a misconfigured router that is blocking traffic to certain websites. This could be due to a number of factors, such as incorrect firewall settings or a problem with the router's configuration. The fact that several colleagues are experiencing the same issue across numerous websites suggests that the problem is not specific to any one website, but rather a broader network issue affecting multiple sites. Remote users who are not connected to corporate resources are not affected because they are not using the same network infrastructure as the affected staff members. A bad antivirus signature update or a problem with the time or date would not likely cause this type of issue, and an upstream internet service provider flapping would affect all users, not just those within a specific organization.

-ChatGPT

upvoted 2 times

  **amityGanoofib** 5 months, 3 weeks ago

it just says the website couldn't be trusted not that it couldn't or wouldn't access it right? seems more of a certification issue.

upvoted 1 times

  **[Removed]** 1 year, 4 months ago

When date or time arent in sync, can cause cert issues. That would explain why people who were working remote were not experiencing the same issues.

upvoted 1 times

  **lordcheekklappur** 1 year, 4 months ago

Selected Answer: D

D. The time or date was not in sync with the website.

When the time or date on a computer is not in sync with the website's server, it can cause SSL/TLS certificates to appear invalid, resulting in trust warnings. This issue can affect multiple users within a corporate network, while remote users who are not connected to the same network may not experience any problems.

upvoted 1 times

  **[Removed]** 1 year, 6 months ago

The most likely cause of this issue is D. The time or date was not in sync with the website.


When a user receives a message that a website cannot be trusted, it means that the security certificate used by the website is not trusted by the user's web browser. Web browsers rely on security certificates to verify the authenticity of websites and to establish secure connections with them. If the security certificate is not trusted, the browser will display a warning message.

One common cause of this issue is when the time or date on the user's computer is not in sync with the time or date on the website's server. This can cause the security certificate to appear as if it has expired or is otherwise invalid, even if it is still valid.

To resolve the issue, the user should check that the time and date on their computer are correct and adjust them if necessary. They may also need to clear their browser's cache and cookies, or adjust their browser's security settings to recognize the website's security certificate as trusted.

Source: ChatGPT

upvoted 1 times

  **AntMan777** 1 year, 6 months ago

ChatGPT says:

A. A bad antivirus signature update was installed.

why? This is the most likely cause of the issue, as the antivirus signature update could have caused the system to mistakenly identify the websites as malicious, causing the messages to appear. The other options are less likely causes of the issue.

upvoted 1 times

  **max319** 1 year, 6 months ago

Selected Answer: B

Unless the NTP server was off B makes the most sense. It is relatively easy to block websites from a router. I think the key thing is that "Remote users who were not connected to corporate resources did not have any issues." Meaning that they were not using the corporate router. But same could be said about an NTP server, however, NTP servers are typically using a NIST timing standard so its unlikely that it would be off.

upvoted 1 times

  **oatmealturkey** 1 year, 6 months ago

It does not say that websites are being blocked, it says they are not trusted. You can still proceed to an untrusted website.

upvoted 1 times

  **oatmealturkey** 1 year, 6 months ago

In fact it says in the question that the user browsed the untrusted website, therefore it could not have been blocked

upvoted 1 times

  **ronniehaang** 1 year, 6 months ago

Selected Answer: D

D. The time or date was not in sync with the website.

This issue is often caused by an incorrect time or date on the computer, which can cause the browser to not recognize the SSL certificate presented by the website as being valid. As a result, the browser may display a warning message stating that the website is not trusted or secure.

upvoted 2 times

  **1Abel1** 1 year, 7 months ago

Selected Answer: B

A site that could not be "trusted" doesn't only point to certificate issues, so the "Time or Date" is not the issue in this scenario because several other colleagues reported the same issue across numerous other websites. Besides, the question doesn't make mention of certificate issue.

With this, I can say the answer is B

upvoted 2 times

  **Nick40** 1 year, 8 months ago

Selected Answer: D

None of the other answers make sense.

upvoted 3 times

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

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

Correct Answer: B

[-]  **Nabilrrhmn** Highly Voted  1 year, 1 month ago

Selected Answer: B

B. Name on a medical diagnosis. This is because medical data is considered sensitive personal data that can reveal information about a person's health, well-being, and identity³. Medical data is subject to strict data protection laws in many countries, such as the GDPR in the EU³. The other options are not as sensitive or personal as option B.

upvoted 5 times

[-]  **Yeb0h** Most Recent  1 month, 3 weeks ago

I'll write core 2 this week wish me luck

upvoted 1 times

[-]  **re777** 4 months ago

I do not know, names in phone books are well known for being private and hard to come by.

upvoted 1 times

[-]  **[Removed]** 1 year, 5 months ago

Selected Answer: B

B is Correct

upvoted 3 times

A company is deploying mobile phones on a one-to-one basis, but the IT manager is concerned that users will root/jailbreak their phones. Which of the following technologies can be implemented to prevent this issue?

- A. Signed system images
- B. Antivirus
- C. SSO
- D. MDM

Correct Answer: D

  **Nabilrrhmn** Highly Voted  1 year, 1 month ago

Selected Answer: D

D. MDM. This is because MDM stands for Mobile Device Management, which is a software solution that allows IT managers to remotely control and secure mobile devices. MDM can enforce policies and restrictions on devices, such as disabling USB debugging, blocking installation of unknown apps, or detecting and blocking rooted or jailbroken devices. The other options are not as effective or relevant as option D.
upvoted 8 times

  **LayinCable** Highly Voted  1 year, 5 months ago

If anyone says anything other than D, they are the things that live under bridges and rocks: Trolls. Carry on.
upvoted 7 times

  **cgrilly** 10 months, 1 week ago

the awnser is clearly A youre wrong.
upvoted 2 times

  **dimeater** Most Recent  1 year, 9 months ago

Selected Answer: D

MDM Mobile device management is the answer
upvoted 3 times

A technician is setting up a conference room computer with a script that boots the application on log-in. Which of the following would the technician use to accomplish this task? (Choose two.)

- A. File Explorer
- B. Startup Folder
- C. System Information
- D. Programs and Features
- E. Task Scheduler
- F. Device Manager

Correct Answer: BE

  **andre0994** Highly Voted  1 year, 5 months ago

Selected Answer: BE

Definitely

Startup Folder: The Startup Folder is a folder on the computer that contains shortcuts to programs that should be launched automatically when the user logs in. By placing a shortcut to the application in the Startup Folder, the application will automatically launch when the user logs in.

Task Scheduler: The Task Scheduler is a tool in Windows that allows you to schedule tasks to run automatically at specific times or events, such as when the user logs in. By creating a task in Task Scheduler to run the application on log-in, the application will automatically launch when the user logs in.

upvoted 7 times

  **1T_wizard** 1 year, 1 month ago

You just copied and pasted from Chatgpt.

upvoted 1 times

  **yutface** 7 months, 1 week ago



So is every explanation you see on here.

upvoted 3 times

  **6809276** Most Recent  6 months, 3 weeks ago

This question is on the exam words for words

upvoted 3 times

  **Raffaello** 8 months, 4 weeks ago

Selected Answer: BE

Open Run command box by pressing the Windows logo + R keys. In the Run command field, type shell: Startup and then press Enter key to open Startup folder. Copy and paste the app shortcut from the desktop to this Startup folder and the app is added to startup Scheduler?

To start a program minimized using Task Scheduler, you can try the following steps:

Open Task Scheduler and create a new task.

On the "Action" tab, set the "Action" to "Start a program".

In the "Program/script" field, enter the path to the executable file of the program you want to start minimized.

upvoted 1 times

  **HR7** 1 year, 5 months ago

is this correct?

upvoted 2 times

  **AyeGodly** 1 year, 5 months ago

yea I believe so, I found this link to help with it as well. Going to the startup folder is the right choice.

<https://www.devdungeon.com/content/windows-run-script-startup>

upvoted 1 times

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

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

Correct Answer: A

  **[Removed]** 1 year, 6 months ago

Selected Answer: A

The systems administrator should enforce a password policy that requires the user to change the password after the first login with the new password. This will ensure that the user can immediately set a new password that only they know, further protecting their account. The systems administrator should also ensure that the password policy requires a strong and unique password that includes a mix of uppercase and lowercase letters, numbers, and special characters.

Source: ChatGPT



upvoted 4 times

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. DRM
- B. NDA
- C. EULA
- D. MOU

Correct Answer: C

  **hafiz871111** 6 months ago

Nobody read this. C is correct.

upvoted 2 times

  **insanegrizly** 1 year, 2 months ago

Selected Answer: C

End user license agreement seems correct.

upvoted 4 times

  **[Removed]** 1 year, 5 months ago

C is correct

upvoted 4 times

  **LayinCable** 1 year, 5 months ago

Even though I know who you are and you are a compulsive liar. They are telling the truth with this. C is corrrrrrrrect.

upvoted 6 times

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

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

Correct Answer: B

Dido1963 Highly Voted 1 year, 9 months ago

Selected Answer: D

with "del" you can delet only a file, not a direktoary!

You need to use rd

upvoted 9 times

Byteszn Most Recent 1 month, 2 weeks ago

I've always known it to be "rd" since MS-Dos days, powershell isn't that commonly used by all techs.

upvoted 1 times

Raffaello 8 months, 4 weeks ago

Selected Answer: D

In computing, rmdir (or rd) is a command which will remove an empty directory on various operating systems.

upvoted 1 times

Jolt 10 months ago

answer is del, try it it out in powershell! , make a folder, then go on in powershell browse to to parent directory an del directory and poof it's gone

upvoted 3 times

Fannan 1 year ago

Selected Answer: D

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).

upvoted 1 times

EngAbood 1 year ago

mkdir -- create directory , rmdir -- remove direktry , i was looking for rmdir :((((((((

upvoted 2 times

CircaG 7 months, 1 week ago

rmdir = rd

mkdir = md

upvoted 1 times

solaWONDER 1 year, 2 months ago

The command-line tool that can be used to delete a directory is the "rd" command. This command is specifically designed to remove directories from a file system

upvoted 1 times

solaWONDER 1 year, 2 months ago

D. rd (or rmdir)

The "rd" command in Windows or "rmdir" command in Unix-like systems is used to remove or delete a directory. This command deletes an empty directory. If the directory is not empty, you may need to use additional options or flags with the command to force the deletion and remove all the files and subdirectories within it.

upvoted 1 times

[Removed] 1 year, 5 months ago

Selected Answer: D

Answer is 10000% "rd". like many have said, it stands for remove directory.

upvoted 4 times

LayinCable 1 year, 5 months ago

I know who you are and you do not know what you are talking about pal. Get off your high horse and get on your rightful pony. (The answer is D though)

upvoted 2 times

  **Rafid51** 1 year, 6 months ago

Selected Answer: D

Answer is "rd" short for "remove directory"


upvoted 2 times

  **cecegilbert** 1 year, 7 months ago

Selected Answer: D

Remove directory=rd

upvoted 1 times

  **aisling** 1 year, 9 months ago

Selected Answer: D

rd remove directory

upvoted 4 times

  **dimeater** 1 year, 9 months ago

Selected Answer: D

Remove directory = rmdir | rmdir = RD

upvoted 1 times

  **Thejphall** 1 year, 10 months ago

answer is D.

"rd" is an alias for the command "rmdir" which functions to remove directories.



upvoted 2 times

  **Sammy2323** 1 year, 10 months ago

Selected Answer: D

verified from microsoft windows commands.

upvoted 3 times

  **imtiaziL** 1 year, 10 months ago

Correct rd deletes the folder and all data within the folder
del deletes only the data within the folder

upvoted 2 times

  **longbob** 1 year, 11 months ago

Out of curiosity, What operating system are we deleting the directory from?

upvoted 1 times

  **longbob** 1 year, 11 months ago

In Windows Command Prompt you can use the "del" command to delete objects.

In Linux, -bash: rd: command not found

rm -d is the command to remove/delete a directory.

Hopefully this will add some clarity to this poorly written question.

upvoted 2 times

  **Sarooor** 1 year, 11 months ago

i think the right answer is D

upvoted 1 times

A technician is troubleshooting a computer with a suspected short in the power supply. Which of the following is the FIRST step the technician should take?

- A. Put on an ESD strap.
- B. Disconnect the power before servicing the PC.
- C. Place the PC on a grounded work bench.
- D. Place components on an ESD mat.

Correct Answer: B

  **ronniehaang** Highly Voted  1 year, 6 months ago

Selected Answer: B

B. Disconnect the power before servicing the PC.

This is the first and most important step that a technician should take when troubleshooting a computer with a suspected short in the power supply. Disconnecting the power helps prevent any electrical hazards and is important for the technician's safety. After disconnecting the power, the technician can then proceed with other troubleshooting steps such as testing the power supply, checking connections, or replacing components if necessary.

upvoted 8 times

  **_Ecks** Most Recent  1 year, 6 months ago

The best choice for accessing the necessary configuration to complete this task is B. Network and Sharing Center. This utility allows for the network connections to be managed, which is essential for configuring the new proxy server settings. It can be accessed by opening Control Panel, then selecting Network and Internet, followed by Network and Sharing Center. This utility provides all the necessary settings to configure the proxy server, including the ability to configure the proxy server settings for each individual connection.

upvoted 3 times

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

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

Correct Answer: D

  **cecegilbert** Highly Voted  1 year, 7 months ago

Selected Answer: D

Internet Explorer: Open the Internet Properties window, which can be opened from the browser, or go to Control Panel > Internet Options. From there, access the Connections tab, click the LAN settings button, and click the Proxy server checkbox

upvoted 11 times

  **Raffaello** Most Recent  9 months ago

Selected Answer: D

Select the Start button, then select Settings > Network & Internet > Proxy. Under Manual proxy setup, turn on Use a proxy server. Do the following: In the Address and Port boxes, enter the proxy server name or IP address and port (optional) in the respective boxes

upvoted 1 times

  **Uzoe** 11 months, 1 week ago

CORRECT ANSWER IS D

upvoted 1 times

  **[Removed]** 1 year, 6 months ago

Selected Answer: D

The best choice for accessing the necessary configuration for setting up a new proxy server on desktop systems in a Windows environment is the Internet Options utility. This utility can be accessed through the Control Panel or through the Settings menu in Microsoft Edge or Internet Explorer. Within the Internet Options utility, the systems administrator can configure the proxy server settings for the system, including the proxy server address and port number. They can also configure authentication settings if required.

Source: ChatGPT


upvoted 2 times

  **Dime_Baggins** 1 year, 7 months ago

Selected Answer: D



D is correct

upvoted 1 times

  **sigidy** 1 year, 7 months ago

B - network and sharing

upvoted 1 times

  **lilbuu** 1 year, 7 months ago

Is this True? I thought windows firewall would be the best choice

<https://www.techtarget.com/searchsecurity/definition/content-filtering>

upvoted 2 times

An analyst needs GUI access to server software running on a macOS server. Which of the following options provides the BEST way for the analyst to access the macOS server from the Windows workstation?

- A. RDP through RD Gateway
- B. Apple Remote Desktop
- C. SSH access with SSH keys
- D. VNC with username and password

Correct Answer: D

—  **tooEducated** Highly Voted 1 year, 8 months ago

VNC = Virtual network computing
upvoted 7 times

—  **[Removed]** Highly Voted 1 year, 4 months ago

Also, VNC allows for graphical manipulation. Its VNC
upvoted 5 times

—  **Raffaello** Most Recent 8 months, 4 weeks ago

Selected Answer: D

VNC Connect's multi-platform support allows you to connect to the Windows remote desktop client from Mac, Linux, and even Raspberry Pi devices. You can also use our VNC Viewer app on iOS, iPadOS, and Android devices for limitless productivity on the move
upvoted 1 times

—  **ScorpionNet** 1 year ago

Selected Answer: D

D is correct. RDP is Windows proprietary, so it won't work on a Mac. VNC is the best solution.
upvoted 2 times

—  **solaWONDER** 1 year, 2 months ago

The BEST way for the analyst to access the macOS server from the Windows workstation, considering GUI access, is option B: Apple Remote Desktop.


Apple Remote Desktop is a specialized tool designed for remote management and administration of macOS systems. It provides a graphical user interface (GUI) for accessing and controlling macOS servers remotely. With Apple Remote Desktop, the analyst can connect to the macOS server from their Windows workstation and have full GUI access to the server software.

upvoted 2 times

—  **solaWONDER** 1 year, 2 months ago

The best way for an analyst to access a macOS server from a Windows workstation would be to use Apple Remote Desktop (option B). Apple Remote Desktop is a powerful tool specifically designed for managing and accessing macOS systems remotely. It provides a graphical user interface (GUI) that allows users to connect to and control macOS servers from their Windows workstations.


upvoted 1 times

—  **minx98** 1 year, 6 months ago

Selected Answer: A

RDP is available for Windows, VNC is for macOS and Linux. It says the client is macOS servers to be accessed FROM a Windows workstation. Therefore, the answer must be RDP

upvoted 1 times

—  **minx98** 1 year, 6 months ago


my bad its D. VNC, RDP only allows connections between the same OS such as windows to windows

upvoted 6 times

—  **rick2461** 1 year, 1 month ago

RDP allows Mac and ios clients to a windows server.
Apple remote desktop does not allow windows clients.
Best answer here is D - VNC

upvoted 2 times

—  **Rafid51** 1 year, 6 months ago

Selected Answer: D

Answer is D

upvoted 4 times

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

Correct Answer: D

alexandrasexy Highly Voted 1 year, 8 months ago

Selected Answer: D

Something you have + something you know!
upvoted 16 times

Jay23AmMonsIV Most Recent 3 months ago

Selected Answer: D

MFA requires two or more different types of authentication factors from the following categories:

Something you know (e.g., password, PIN)

Something you have (e.g., smart card, security token)

Something you are (e.g., fingerprint, retina scan)

Using a smart card (something you have) and a password (something you know) fulfills the requirement of MFA by combining two different types of factors.

upvoted 1 times

Raffaello 8 months, 4 weeks ago

Selected Answer: D

Multifactor authentication can be performed using a multifactor authenticator or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are

upvoted 2 times

wejdanali 11 months ago

"all 2FA is an MFA, but not all MFA is a 2FA"

upvoted 1 times

ScorpionNet 1 year ago

Selected Answer: D

This question is related to something you have and something you know! TestOut thinks it's PIN and password which I disagree on because PIN and password are both something you know! D is the one.

upvoted 1 times

phanton 1 year, 4 months ago

Option A seems to be the most accurate answer to choose

upvoted 1 times

Sebatian20 1 year, 3 months ago

MFA can't be bother 'Something you are.'

upvoted 1 times

Kristheitguru 1 year, 5 months ago

Selected Answer: A

The example of MFA (Multi-Factor Authentication) is A. Fingerprint scan and retina scan.

MFA is a security mechanism that requires the user to provide two or more authentication factors to verify their identity. These factors are typically categorized into three types:

Something the user knows, such as a password or PIN.

Something the user has, such as a smart card or token.

Something the user is, such as a fingerprint, retina scan, or other biometric data.

In this example, the user is required to provide two different biometric factors, a fingerprint scan and a retina scan, to verify their identity. This provides a high level of security since it is difficult for an attacker to fake both biometric factors.

upvoted 2 times

CompCertOn 1 year ago

What you suggested is two of "something you are! Which is wrong! The correct answer is D

upvoted 1 times

  **Thunder_Cat** 1 year, 4 months ago

Your answer and example are not right. Please understand MFA before leaving comments.

CompTIA CertMaster Learn for A+ 220-1102, the definition of MFA is as follows:

Authentication scheme that requires the user to present at least two different factors as credentials; for example, something you know, something you have, something you are, something you do, and SOMEWHERE you are. Specifying two factors is known as 2FA.

Also, there are 5 categories. Researching is important in IT. This will continue throughout your career, especially if you plan to pursue a career in penetration testing.

upvoted 5 times

  **[Removed]** 1 year, 5 months ago

Selected Answer: D

Its D. Two different types of authentication. Ex: Something you know, Something you have, Something you are

upvoted 3 times

  **Rafid51** 1 year, 6 months ago

Selected Answer: D

MFA stands for Multi-Factor Authentication, Smart card and password are two different authentications in here.

upvoted 3 times

  **dimeater** 1 year, 9 months ago

Selected Answer: D

This is the way

upvoted 1 times

  **LAM2002** 1 year, 10 months ago

Selected Answer: D

Something physical that I have and something that I know.


upvoted 3 times

  **ryanzou** 1 year, 11 months ago

Selected Answer: D

D is correct, something you have plus something you know

upvoted 4 times

  **Sarooor** 1 year, 11 months ago

Because password and pin are both something you know . For MFA you need 2 different authentications. D is the correct answer


upvoted 3 times

  **sebwalsh** 1 year, 11 months ago

Selected Answer: B

Any reason why the answer isn't (B)? Thought this was a very common form of MFA.

upvoted 1 times

  **Sarooor** 1 year, 11 months ago

Because password and pin are both something you know . For MFA you need 2 different authentications. D is the correct answer

upvoted 6 times

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.

Correct Answer: B

  **Jimmy_Jam** Highly Voted  1 year, 7 months ago

Selected Answer: B

If you set a pc to DHCP it would remove the static address in the process. Two birds one stone.
upvoted 11 times



  **ydnatree** 1 year ago

This would only set the DHCP for the laptop, but won't resolve the issue if the specialized software requires a specific IP address.
upvoted 8 times

  **Fannan** Highly Voted  1 year ago

Selected Answer: C

The question says the software "requires a specifically allocated (IP) address" to connect to the software and it seems like the old desktop has been assigned that specific static IP address. Since the desktop is old and probably being replaced by the new laptop, it should be configured to use DHCP instead so that the new laptop can be assigned that specific IP address as it will be used more often by the user.
upvoted 8 times

  **apaiva25** 4 months ago

set the laptop to dhcp is not an option
upvoted 1 times

  **Vukky** 7 months, 2 weeks ago

*The question says the *user* (instead of software as u wrote it)
upvoted 1 times

  **b27480c** Most Recent  2 months, 2 weeks ago


Selected Answer: C

Removing the static IP will remove the duplicate and in theory, fix the issue at hand.
upvoted 1 times

  **danishkayani11** 2 months, 3 weeks ago

Selected Answer: C

to use software on Laptop you need static ip on laptop because software requires specific address. to avoid conflict of ip you have to remove static ip address from the old desktop pc
upvoted 1 times

  **PatrickH** 8 months, 4 weeks ago

Its C because: They need to remove the Static IP address form the Desktop AND configure the Laptop with that static IP address. Definatly NOT B Give the Laptop a DHCP address. So its C but it needs a bit more clarity in fairness.
upvoted 4 times

  **[Removed]** 10 months, 2 weeks ago

Selected Answer: C

C ist correct. B is not a solution, because even when you use DHCP reservation for setting up a the specific static IP address for the laptop, the desktop will still have the same static IP address and the conflict of IP addresses will persist.
upvoted 1 times

  **TacosInMyBelly** 10 months, 4 weeks ago

Selected Answer: C

The key is in the wording...remove the static IP from the DESKTOP (old) so that the LAPTOP (new) can use the IP address without conflict.

upvoted 1 times

  **AsadArif** 12 months ago

Selected Answer: B

The question never mentions that either the laptop or the desktop have static IP. It just says that both of them get the same error message. So, the only way would be to set it on DHCP to avoid conflicts and get the device's specific IP address.

upvoted 1 times

  **ScorpionNet** 1 year ago

Selected Answer: C

C is the best option. If you set it to DHCP, it's completely fine, but you would have to update the exclusions. C is considered a better option so the way that it would prevent any conflicts. To ensure it's not causing any conflicts, make sure you update the exclusions on the DHCP server.

upvoted 2 times

  **alexkeung** 1 year ago

Selected Answer: C

As setting the laptop to dhcp alone will not provide a specific address for the machine (need a reservation as well), B is incorrect. C is a better answer, the old desktop is changed to DHCP, the IP conflict is resolved and it also gives the new laptop a specific address.

upvoted 2 times

  **CompCertOn** 1 year ago

Selected Answer: C

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.

upvoted 4 times

  **NickDrops** 11 months, 4 weeks ago

This is def it. Thanks!

upvoted 1 times

  **ZainKambo** 1 year ago

Selected Answer: C

Remove the static IP configuration from the desktop, As app need a specific address, New laptop can get that address. but before we have to change that address in old desktop, which may be will not in use anymore.

upvoted 2 times

  **sean01** 1 year, 1 month ago

Selected Answer: C

'the user requires a specifically allocated address' makes me choose C over B.

upvoted 2 times

  **solaWONDER** 1 year, 2 months ago

To resolve the issue of receiving a message stating that the address is already in use when attempting to log in to specialized software, the technician should most likely perform the following steps:



C. Remove the static IP configuration from the desktop.

upvoted 1 times

  **Kinjie** 1 year, 2 months ago

B is the correct option, doing so will remove static address, set reservation in DHCP


upvoted 1 times

  **Nonickname176798512478** 1 year, 2 months ago

Selected Answer: C

The "specially allocated address" is what pulled me towards C

upvoted 2 times

  **RoPsur** 1 year, 2 months ago

Selected Answer: B

When you set DHCP, also configure the reservation of the address you need. :)

upvoted 1 times

A user is having issues with document-processing software on a Windows workstation. Other users that log in to the same device do not have the same issue.

Which of the following should a technician do to remediate the issue?



- A. Roll back the updates.
- B. Increase the page file.
- C. Update the drivers.
- D. Rebuild the profile.

Correct Answer: B

  **ryanzou** Highly Voted 1 year, 11 months ago

Selected Answer: D

D is the correct answer
upvoted 7 times

  **Bioka** 1 year, 4 months ago

Sure, D is the correct answer.
upvoted 1 times

  **Dido1963** Highly Voted 1 year, 8 months ago

Selected Answer: D

If it would be the page file, all users would have that Problem
upvoted 6 times

  **CodeOnTren** Most Recent 1 month ago

Selected Answer: D

"Other users that log in to the same device do not have the same issue." so it cant be the device , otherwise all the user had to increase the page file , definitely is the use profile
upvoted 1 times

  **Raffaello** 9 months ago

Selected Answer: D

Answer: D Explanation: The issue is specific to the user's profile, so the technician should rebuild the profile.
upvoted 1 times

  **Mehsotopes** 1 year, 1 month ago

D seems reasonable, however, Windows domain controllers utilize page files to perhaps create temporary files in use by profiles connected to said network for transferring files.
<https://learn.microsoft.com/en-us/troubleshoot/windows-client/performance/introduction-to-the-page-file>
upvoted 1 times



  **solaWONDER** 1 year, 2 months ago

The answer is D. Rebuild the profile.

The issue is most likely caused by a corrupt user profile. A user profile is a collection of settings and files that are specific to a user. When a user logs in to a Windows workstation, their profile is loaded, and the settings and files are made available to the user.
upvoted 1 times

  **solaWONDER** 1 year, 2 months ago

D is the answer
upvoted 1 times

  **pop3** 1 year, 3 months ago

D is the corect anser
upvoted 1 times

  **PatrickH** 1 year, 8 months ago



Its D. Issue not affecting other users. Therefore its this users profile.
upvoted 3 times

  **jackjack007** 1 year, 9 months ago

Selected Answer: D


it is the same device so definitely the account has problem, so we should rebuild it. 100% D is correct.

upvoted 4 times

  **toshiro** 1 year, 11 months ago

Other users may not be using the same number or type of apps this user is, so memory could be an issue. Best to start with that than something more drastic like rebuilding a profile

upvoted 2 times

  **Sarooor** 1 year, 11 months ago

what is the correct answer?

upvoted 1 times

  **lazyyoung** 1 year, 11 months ago

B wouldn't make sense because Page file error would be if you get a message "Your system is low on virtual memory"

upvoted 4 times

  **antman2k89** 1 year, 11 months ago

why wouldn't it be D

upvoted 5 times

Question #106

Topic 1

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

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

Correct Answer: B

  **LayinCable** Highly Voted  1 year, 5 months ago

Selected Answer: B

Home is the lowest version of windows and it doesn't have BitLocker. Pro is the next version up but it DOES have BitLocker. Therefore, it is Pro

upvoted 6 times

  **marcotshks** Most Recent  1 week, 1 day ago


A
i have win 11 home edition and bitlocker is active

upvoted 1 times

  **BozoBenty** 5 months ago

I dont even have windows activated and have it lmao

upvoted 1 times

  **mohdAj** 9 months, 3 weeks ago

Selected Answer: B

In terms of editions, "Windows 10 Pro" is the more common and widely used version, and it can be considered the more basic or standard option compared to "Windows 10 Pro for Workstations."

"Windows 10 Pro for Workstations" is a specialized edition designed for high-performance workstations with demanding hardware configurations. It includes features tailored for such environments, including support for higher-end hardware, but it may include features that are not essential for typical users or business scenarios.

Therefore, if you're looking for the most basic version between "Windows 10 Pro" and "Windows 10 Pro for Workstations," "Windows 10 Pro" is the standard and widely-used version for general business and personal use

upvoted 2 times

  **Xzahmed1990** 1 year, 5 months ago

B
Looks good for me

upvoted 1 times

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.

Correct Answer: D

  **jackjack007** Highly Voted  1 year, 9 months ago

Selected Answer: C

- A. Run the virus scanner in an administrative mode: virus scanner always use administrative mode, so this is irrelevant = no
- B. Reinstall the operating system: this does not preserve user files so = no
- C. Reboot the system in safe mode and rescan: In safemode malwares can't run and antiviruses can kill them, so= yes
- D. Manually delete the infected files: this does not preserve user files = no

Therefore I go with D

upvoted 19 times

  **jackjack007** 1 year, 9 months ago

I mean C is correct not D

upvoted 10 times

  **PatrickH** Highly Voted  1 year, 8 months ago

Selected Answer: C

Again bad answer. Happening too often. The answer is C. Boot into safe mode, run antivirus. Recommended procedure

upvoted 5 times

  **Bmc2994** 1 year, 6 months ago

Agreed. Much too often! Answer is C!

upvoted 3 times

  **dlittle** Most Recent  9 months, 3 weeks ago

So who's confirming these answers because I notice that some seem to be incorrect but no administrator chimes in to clarify.

upvoted 2 times

  **Saeidsmart** 1 year ago

Selected Answer: C

Reboot the system in safe mode and rescan: Booting in safe mode loads a minimal set of drivers and services. Many types of malware are designed to start automatically with Windows, but booting in safe mode can prevent their activation. Scanning in safe mode can increase the chances of detecting and removing malware that might be active and hidden during a normal boot.

upvoted 2 times

  **solaWONDER** 1 year, 2 months ago

The answer is C. Reboot the system in safe mode and rescan.

Safe mode is a diagnostic mode of Windows that starts the computer with a limited set of drivers and services. This can be helpful for troubleshooting problems, such as malware infections.



upvoted 1 times

  **alexandrasexy** 1 year, 8 months ago

Selected Answer: C

C. Reboot the system in safe mode and rescan.

upvoted 3 times

  **cobbs** 1 year, 9 months ago

Selected Answer: C

Safe mode is necessary to allow access to the malware files. You would not be able to manually delete them.

upvoted 2 times

A technician is installing a new business application on a user's desktop computer. The machine is running Windows 10 Enterprise 32-bit operating system. Which of the following files should the technician execute in order to complete the installation?

- A. Installer_x64.exe
- B. Installer_Files.zip
- C. Installer_32.msi
- D. Installer_x86.exe
- E. Installer_Win10Enterprise.dmg

Correct Answer: D

  **Raffaello** 9 months ago

Selected Answer: D

These terms refer primarily to the type of CPU and operating system on which Cantabile will run. x86 refers to a 32-bit CPU and operating system. x64 refers to a 64-bit CPU and operating system.

upvoted 1 times

  **[Removed]** 1 year, 5 months ago

It can be C if you wanted to.

upvoted 1 times

  **Mango7** 11 months, 1 week ago

nope it dont work like that my guy. 32bit=x86

upvoted 3 times

  **[Removed]** 1 year, 5 months ago

Selected Answer: D

question states what needs to be "executed". so we know it's a .exe document. we also know its a 32bit system. therefore its the answer is D



upvoted 3 times

  **Nick40** 1 year, 9 months ago

Selected Answer: D

it is D

upvoted 1 times

  **examtopics11** 1 year, 9 months ago

Selected Answer: D



Seeing how this is A+ and not much mention of .msi in study material. From Stack overflow. I first installed from MSI, which only installed the program files (not any prerequisites or dependencies, and didn't create Start Menu icons). When I manually launched the program, it failed saying certain DLLs were missing. Installing from the EXE installed other things too, and the product ran just fine. I would say, if a software maker provides both an EXE and MSI option for installing, use the EXE

upvoted 2 times

  **Sarooor** 1 year, 11 months ago

does any one know why D is the answer?

upvoted 2 times

  **LayinCable** 1 year, 5 months ago

Theres ONLY 32-bit and 64-bit operating system versions.

64 bit= x64

32 bit= x86

upvoted 6 times

  **longbob** 1 year, 11 months ago

Because x86 is 32 bit. Read up on the earlier operating systems and how they transitioned to 64 bit OS.

upvoted 9 times

A user calls the help desk to report potential malware on a computer. The anomalous activity began after the user clicked a link to a free gift card in a recent email.

The technician asks the user to describe any unusual activity, such as slow performance, excessive pop-ups, and browser redirections. Which of the following should the technician do NEXT?

- A. Advise the user to run a complete system scan using the OS anti-malware application.
- B. Guide the user to reboot the machine into safe mode and verify whether the anomalous activities are still present.
- C. Have the user check for recently installed applications and outline those installed since the link in the email was clicked.
- D. Instruct the user to disconnect the Ethernet connection to the corporate network.

Correct Answer: D

  **Dido1963** Highly Voted  1 year, 8 months ago

Selected Answer: D

Comptia malware removal steps:

1. Identify and research malware symptoms. ...
2. Quarantine the infected systems. ...
3. Disable System Restore (in Windows). ...
4. Remediate the infected systems. ...
5. Schedule scans and run updates. ...
6. Enable System Restore and create a restore point (in Windows). ...
7. Educate the end user.

You did Step 1, now you should do Step 2, even if you are in a SOHO and not in an Enterprise, you should stop the malware, that it can not infect other PCs

upvoted 13 times

  **TKW36** Highly Voted  1 year, 10 months ago

Selected Answer: D

First thing you want to do is quarantine/disconnect the affected system from the network so whatever malicious software doesn't spread. So the answer is D.

upvoted 8 times

  **Redbttomjane** Most Recent  3 months, 2 weeks ago

It says "potential malware" so wouldn't the tech have to run a full scan to see what the actual issue would be before taking any further steps?

upvoted 1 times

  **vshaagar** 4 months, 2 weeks ago

Selected Answer: B

Why would answer be D? Here they never stated the user is from an organization or a Soho. This could be a single user. I think the best answer is B.

upvoted 1 times

  **vshaagar** 4 months, 2 weeks ago

Sorry i chose the wrong answer. The answer is A. Scan the computer. The small fix first before going to the big stages.

upvoted 2 times

  **Fannan** 1 year ago

Selected Answer: B

The best way to scan a computer for viruses is to boot the computer in safe mode. Safe mode only loads the drivers needed to operate windows, so any potential viruses will not load in this mode.

upvoted 1 times

  **[Removed]** 1 year, 6 months ago

Selected Answer: D

D is correct because it follows CompTIA's malware removal steps.

upvoted 5 times

  **Cuddles** 1 year, 7 months ago

So it's assumed that by asking a couple of questions that we successfully identified the problem?

upvoted 1 times

  **wepaid** 1 year, 7 months ago

Answer is B
upvoted 1 times

  **wepaid** 1 year, 7 months ago

This is a User complaining.... what does the user know? that user isn't the expert.... its the technician's job to determine if there is really a virus or not.... you run it into safe mode because when you do that you can tell if there is a virus present... after doing that you would do A.
upvoted 2 times

  **Nick40** 1 year, 9 months ago

Selected Answer: A

A.
the question says nothing about this being a computer on a corporate network to begin with. And the first thing you're supposed to do if you notice any of the problems listed is run a scan...
upvoted 4 times

  **navvvarroooo** 1 year, 8 months ago

"calls help desk"? would this suggest the comp was on a corporate network?
upvoted 3 times

  **Monyluv** 1 year, 10 months ago

Why would the answer be D can someone explain?
upvoted 1 times

  **og1olu** 1 year, 10 months ago

The technician is required to quarantine the system after identifying the problem. So, I believe D is correct.
upvoted 9 times

Question #110

Topic 1

A technician is setting up a new laptop for an employee who travels. Which of the following is the BEST security practice for this scenario?

- A. PIN-based login
- B. Quarterly password changes
- C. Hard drive encryption
- D. A physical laptop lock

Correct Answer: C

  **Mehsotopes** 1 year, 1 month ago

Selected Answer: C

Encrypting your disk with bitlocker is the safest option for security, especially if you're traveling or in an untrusted are, you can find it under Control Panel > Bitlocker Encryption to run bitlocker.
You may have to turn off the option of "Allow BitLocker without a compatible TPM (requires a password, or a startup key on a USB flash drive)."
This can be found in Group Policy Editor for Windows Pro or above, find the "Require additional authentication at startupA" key under [Compuer Configuration > Administrative Template > Windows Componenets > Bitlocker Drive Encryption > Operating System Drives. Here you will find the check box for "Allow BitLocker without a compatible TPM (requires a password, or a startup key on a USB flash drive)."
upvoted 1 times

  **Mehsotopes** 1 year, 1 month ago

Selected Answer: C

Encrypting your disk with bitlocker is the safest option for security, especially if you're traveling or in an untrusted are, you can find it under Control Panel > Bitlocker Encryption to run bitlocker.
You may have to turn off the option of "Allow BitLocker without a compatible TPM (requires a password, or a startup key on a USB flash drive)."
This can be found in Group Policy Editor for Windows Pro or above, find the "Require additional authentication at startupA" key under [Compuer Configuration > Administrative Template > Windows Componenets > Bitlocker Drive Encryption > Operating System Drives. Here you will find the check box for "Allow BitLocker without a compatible TPM (requires a password, or a startup key on a USB flash drive)."
upvoted 1 times

  **[Removed]** 1 year, 5 months ago

Selected Answer: C

My vote is C. Just based off the fact that the user is traveling. while all the options are good options it makes most sense that the biggest risk is the device getting stolen. C is the best option in case the laptop is stolen in my opinion.
upvoted 4 times

A technician is troubleshooting a lack of outgoing audio on a third-party Windows 10 VoIP application. The PC uses a USB microphone connected to a powered hub. The technician verifies the microphone works on the PC using Voice Recorder. Which of the following should the technician do to solve the issue?

- A. Remove the microphone from the USB hub and plug it directly into a USB port on the PC.
- B. Enable the microphone under Windows Privacy settings to allow desktop applications to access it.
- C. Delete the microphone from Device Manager and scan for new hardware.
- D. Replace the USB microphone with one that uses a traditional 3.5mm plug.

Correct Answer: B

  **[Removed]** Highly Voted  1 year, 6 months ago

Selected Answer: B

We know that it is B because the other answers imply that it is a hardware problem, which we know to be false because the question stated that the microphone is functional, its just a matter of enabling the microphone to be used with third party applications
upvoted 8 times

  **danishkayani11** Most Recent  2 months, 3 weeks ago

i'm still confused what kind of powerhub enables audio connection to the PC? Powerhubs normally don't have data connections to the PCs
upvoted 1 times

  **danishkayani11** 2 months, 3 weeks ago

my bad. it's a powered hub. not a power hub. powered hubs have usb connection to the pc and can connect multiple peripherals. B is correct
upvoted 1 times

  **Mehsotopes** 1 year, 1 month ago

Selected Answer: B

This is most likely due to needing to set applications to have access to microphone from Windows Settings > Privacy > Microphone (App Permissions)
upvoted 1 times

  **Nabilrrhmn** 1 year, 1 month ago

Selected Answer: B

I think the best option to solve the issue is B. Enable the microphone under Windows Privacy settings to allow desktop applications to access it. This is because the user is trying to log in to a specialized software, which may be a desktop application that does not have permission to use the microphone by default. Enabling the microphone under Windows Privacy settings can allow desktop applications to access it and resolve the issue. The other options are not as relevant or effective as option B.
upvoted 1 times

  **insanegrizly** 1 year, 2 months ago

Selected Answer: A



I'd go with A, this has fixed these kinds of issues for me countless times.
upvoted 3 times

  **insanegrizly** 1 year, 2 months ago

Nevermind, it's clearly B...
upvoted 3 times

  **solaWONDER** 1 year, 2 months ago

Based on the given scenario, the BEST action for the technician to solve the lack of outgoing audio issue on the third-party Windows 10 VoIP application is option A: Remove the microphone from the USB hub and plug it directly into a USB port on the PC.
upvoted 2 times

  **_Ecks** 1 year, 6 months ago

The technician should first remove the microphone from the USB hub and plug it directly into a USB port on the PC. They should then check to see if the microphone works on the PC using Voice Recorder. If the microphone still does not work after being plugged directly into the PC, the technician should then enable the microphone under Windows Privacy settings to allow desktop applications to access it. If the microphone still does not work after enabling it in Windows Privacy settings, the technician should delete the microphone from Device Manager and scan for new hardware. If the microphone still does not work after completing these steps, the technician should replace the USB microphone with one that uses a traditional 3.5mm plug.
upvoted 4 times

  **Abz1999** 1 year, 6 months ago

Answer is B, Read the question properly. It says what should be done to SOLVE the issue not what should be done NEXT. A will be correct if asked what should be done NEXT and B is correct if asked what should be done to solve it.

upvoted 4 times

  **minx98** 1 year, 6 months ago

I'm dead man wrote a whole paragraph explaining why he was wrong 😂😂😂

upvoted 7 times

Question #112

Topic 1

A user who is unable to connect to the network submits a help desk ticket. The assigned help desk technician inquires about whether any recent changes have been made. The user reports there is construction activity in the surrounding offices. The help desk technician proceeds to ping the user's desktop, which does not respond. Which of the following is the MOST likely cause of this issue?

- A. A duplicate IP address has been issued to the user's desktop.
- B. The HDD of the OS is failing.
- C. The network cable has become disconnected.
- D. Malware has infected the system.

Correct Answer: C

  **[Removed]** **Highly Voted**  1 year, 5 months ago

Selected Answer: C

C seems to be the only answer here that really makes sense

upvoted 6 times

Question #113

Topic 1

A user has been unable to access a website and has submitted a help desk ticket. The website has been verified to be online. Which of the following troubleshooting steps will MOST likely resolve the issue?

- A. Deleting the browser history
- B. Clearing the cache
- C. Enabling private mode browsing
- D. Enabling ad blocking

Correct Answer: B

  **Mehsotopes** 1 year, 1 month ago

Selected Answer: B

This website can be verified as Online probably through ping.

The most likely issue is that it's data cache is full & needs to be cleared, this can be done by clicking the settings tab that is usually represented by three dots, or lines, go to "more tools" & the pop-out dialog box should have option for clearing browsing data cache. This can also be done by pushing CTRL+SHIFT+DEL while in your web browser.

upvoted 2 times

  **[Removed]** 1 year, 5 months ago

Selected Answer: B

all of the other options would not help the user access a specific website. therefore the only answer that makes any sense is B

upvoted 3 times

A desktop support technician is tasked with migrating several PCs from Windows 7 Pro to Windows 10 Pro. The technician must ensure files and user preferences are retained, must perform the operation locally, and should migrate one station at a time. Which of the following methods would be MOST efficient?

- A. Golden image
- B. Remote network install
- C. In-place upgrade
- D. Clean install

Correct Answer: C

  **DonnieDuckoe** 1 year, 4 months ago

Selected Answer: C

An in-place upgrade is the process of upgrading or updating a software or operating system on a computer system without erasing or removing the existing data, settings, and applications. In other words, it is the process of upgrading or updating the software or operating system while retaining all the user's data and settings in the same location as before the upgrade. This is usually done to avoid the need for a clean installation of the software, which would require the user to back up and transfer their data and settings to a new location. An in-place upgrade is typically faster and less disruptive to the user's workflow than a clean installation.

upvoted 4 times

  **DonnieDuckoe** 1 year, 4 months ago

Source: ChatGPT

upvoted 1 times

The findings from a security audit indicate the risk of data loss from lost or stolen laptops is high. The company wants to reduce this risk with minimal impact to users who want to use their laptops when not on the network. Which of the following would BEST reduce this risk for Windows laptop users?

- A. Requiring strong passwords
- B. Disabling cached credentials
- C. Requiring MFA to sign on
- D. Enabling BitLocker on all hard drives

Correct Answer: C

  **Manzer** Highly Voted 1 year, 11 months ago

Selected Answer: D

Bit locker is the answer.
upvoted 18 times

  **longbob** Highly Voted 1 year, 11 months ago

Selected Answer: D

The question has two requirements. Prevent data loss, minimal impact to users.
MFA would impact users, they have to do an extra step to login.
BitLocker encrypts the entire hard drive, thereby making the information "unreadable" in case of a lost laptop.
Answer is D
upvoted 16 times

  **crazymonkeh** Most Recent 6 months ago

Selected Answer: D

The answer is definitely D: Bitlocker

It is not "C" because the HDD can simply be removed from the case, and use a drive reader to directly access the files themselves without the use of a Windows Login/MFA.
upvoted 3 times

  **Mehsotopes** 1 year, 1 month ago

Answer could be C because it simply involves knowledge factor & possession factor without requiring you to tamper with all the data on disks.
upvoted 1 times

  **solaWONDER** 1 year, 2 months ago

To reduce the risk of data loss from lost or stolen laptops for Windows laptop users, the BEST option is option D: Enabling BitLocker on all hard drives.

BitLocker is a full disk encryption feature available in Windows operating systems. By enabling BitLocker, the data on the laptop's hard drives is encrypted, providing protection against unauthorized access in case of loss or theft. This ensures that even if the physical device is compromised, the data remains encrypted and inaccessible to unauthorized individuals.

upvoted 2 times

  **solaWONDER** 1 year, 2 months ago

The best way to reduce the risk of data loss from lost or stolen laptops is to enable BitLocker on all hard drives. BitLocker is a full disk encryption feature that encrypts all of the data on a laptop's hard drive. This makes it very difficult for unauthorized users to access the data on the laptop if it is lost or stolen.
upvoted 1 times

  **Brightside** 1 year, 4 months ago

Key phrases here are 'reduce the risk' & 'BEST'
MFA fits those two .
upvoted 1 times

  **rick2461** 1 year, 1 month ago

other key phrases are "minimal impact" and "prevent data loss". MFA is an extra step for users, and MFA itself is useless without encryption.
Answer: D
upvoted 3 times

  **[Removed]** 1 year, 5 months ago

Selected Answer: D

D is the most correct answer to the specific question.
upvoted 1 times

[-]  **max319** 1 year, 6 months ago

D is just not it, BitLocker will impact performance heavily. For example, With my T7300 2.0GHz and Kingston V100 64gb SSD the results are:
Bitlocker off → on

Sequential read 243 MB/s → 140 MB/s

Sequential write 74.5 MB/s → 51 MB/s

Random read 176 MB/s → 100 MB/s

Enabling MFA negates the issue with stolen laptops because there is a multitude of ways to use mfa, something you have, something you know, something you are. Requiring users to use biometrics in conjunction with a password will have minimal impact. Therefore I am choosing C.

upvoted 1 times

[-]  **mtrJacky** 1 year, 5 months ago

If using MFA, how can I protect the data as I can remove the hdd or ssd to another computer to read the data. Although "D" will affect the speed, but it would be the best answer.

upvoted 4 times

[-]  **jtmonster** 1 year, 8 months ago

I think the reason for C is that you would need to access a key for using bitlocker which would increase the impact to the user. Any thoughts?


upvoted 1 times

[-]  **alexandrasexy** 1 year, 8 months ago

Selected Answer: D

D. Enabling BitLocker on all hard drives

upvoted 2 times

[-]  **1T_wizard** 1 year, 1 month ago

What if the laptops are using SSDs

upvoted 1 times

[-]  **Thenewf_boy** 11 months, 1 week ago

i haven't tried on my laptop but i did try on my desktop with multiple drives and ssd's can use bit locker,, hope this helps..

upvoted 1 times

[-]  **Nick40** 1 year, 9 months ago

Selected Answer: D

D for sure

upvoted 2 times

[-]  **ryanzou** 1 year, 11 months ago

Selected Answer: D

D is the answer, no doubt

upvoted 4 times

A technician has been asked to set up a new wireless router with the best possible security. Which of the following should the technician implement?

- A. WPS
- B. TKIP
- C. WPA3
- D. WEP

Correct Answer: C

  **ScorpionNet** 1 year ago

Selected Answer: C

WPA3 is the best answer. WEP is an older wireless security protocol, so it will not provide the best security in today's WiFi networks.
upvoted 2 times

  **Rafid51** 1 year, 6 months ago

Selected Answer: C

WPA3 is the latest wireless security protocol with stronger encryption and better protection against brute-force attacks.
upvoted 2 times

  **cecegilbert** 1 year, 7 months ago

Selected Answer: C

WPA3 IS Ans
upvoted 3 times

After returning from vacation, a user is unable to connect to the network at the corporate office. Windows allows the user to log in; however, no internal or external websites are accessible when running a browser. The user's expected network shares are unreachable, and all websites attempted return the message, `Hmm, we can't reach this page.` Which of the following is the MOST likely cause of this issue?

- A. The user's password expired while on vacation.
- B. The user clicked on a malicious email.
- C. The user connected to a captive portal while traveling.
- D. The user enabled airplane mode.

Correct Answer: D

—  **sigidy** Highly Voted 1 year, 7 months ago

D is the answer
upvoted 9 times

—  **mayur3151089** Most Recent 3 weeks, 1 day ago

Selected Answer: A

Clicking on a malicious email would likely result in different symptoms, such as compromised data or unusual behavior, rather than a complete inability to connect to any network resources.
Connecting to a captive portal usually only affects the user's network when they are connected to that specific Wi-Fi network, and it wouldn't be an issue after returning to the corporate office.
Enabling airplane mode would likely prevent any network login entirely, but the user wouldn't be able to log in at all, and this mode is typically easy to notice and fix so A I think
upvoted 1 times

—  **danishkayani11** 2 months, 3 weeks ago


Selected Answer: D

D is simple and clearly fits the situation. C can be true by assuming a lot of things. if the user connected to a captive portal which usually require DHCP settings, coming back assuming again that office requires static ip or some other conflict. in that case C can be correct. simple answer is D, i would choose both if i was asked to choose 2
upvoted 1 times

—  **crazymonkeh** 6 months ago

I'll be honest, I've encountered this issue many times on the job. Usually caused by the computer being disconnected from the corp network so long that it's no longer able to join the domain. The laptop is disabled in Active Directory, or has been removed entirely. This means it won't be able to connect to the corporate network, but the last logged in user should still be able to login to Windows because their credentials are cached on the HDD.

I don't really see any of the answers as "correct" but it should be between A and D.
upvoted 2 times

—  **c22e828** 6 months, 1 week ago

wait... how are they logging on to Windows if they're in airplane mode??? Its C
upvoted 2 times

—  **crazymonkeh** 6 months ago


The credentials are stored locally on the HDD. As the last logged on user of this laptop, her credentials are cached. She's currently the only user that can login to this computer. Any other employees will not be able to, even if they have a windows user account stored on this laptop, because they weren't the last person to use it.

The only exception would be the local admin account.
upvoted 1 times

—  **RyeBread** 7 months ago

Selected Answer: D

I really hate these questions. We have to assume a few things that are not clear. First it says the user returned from vacation, but does not say they took their laptop with them. Only based on answers in C and D can we assume the user had their laptop with them to which I say, was it really a vacation? Captive portal is possible but so is Airplane mode. User could have been using the laptop and connected to the wifi provided on the plane and went through a captive portal. But the last thing the user may have done was placed the laptop in airplane mode before they landed. Then again, you do have to stow away laptops during landing so I am not sure that Airplane mode may have been necessary. Regardless, I will still go with airplane mode.
upvoted 3 times

—  **bobzilla96** 9 months, 3 weeks ago

correct answer is C
upvoted 1 times

  **ConqiD** 12 months ago

Selected Answer: C

Captive Portal: When the user connected to a captive portal while traveling, it's possible that their network configuration settings were altered or that the portal's captive portal login page is interfering with their internet connectivity. Captive portals often require users to log in or accept terms and conditions before granting access to the internet. If the user didn't complete this process or if the captive portal settings were misconfigured, it could explain why they can log into Windows but can't access websites or network shares.

upvoted 1 times

  **DerekM** 1 year, 4 months ago

Selected Answer: D

option D, "The user enabled airplane mode," is the closest to the correct answer. If the user enabled airplane mode on their device, it would disable all wireless connectivity, which would explain why they cannot connect to any network or website.

upvoted 2 times

  **Navigator** 1 year, 4 months ago

Selected Answer: D

This has nothing to do with captive portals. The right answer should be D. I even experienced this yesterday.

upvoted 3 times

  **Thapas** 1 year, 5 months ago

in the scenario, it is stated that the user's device allows them to log in to Windows, which suggests that the device is not in airplane mode or in a state where all wireless connectivity is disabled. Additionally, the symptoms described - the inability to access internal and external websites - are more consistent with a captive portal issue.

upvoted 2 times

  **[Removed]** 1 year, 4 months ago

You can log into Windows with local access that does not require an internet connection.

upvoted 8 times

  **FreddieB** 9 months, 2 weeks ago

RIGHT im thinking the same thing. You can be in the middle of the desert and log in to windows/your computer. That was there to throw us off most likely

upvoted 1 times

  **[Removed]** 1 year, 5 months ago

Selected Answer: D

while C is a possibility. D is much more likely.

upvoted 2 times

  **lilbuu** 1 year, 7 months ago

Selected Answer: C

C. The user connected to a captive portal while traveling is the most likely cause of this issue. A captive portal is a webpage that is presented to the user before they can access the internet. It is often used by hotels, airports, and other public Wi-Fi networks to authenticate users and accept terms and conditions. Connecting to a captive portal can cause the user's network settings to change, making it difficult to connect to the corporate network when they return. This would explain why the user is able to log in to Windows but is unable to access any internal or external websites.

upvoted 2 times

  **KingM007** 1 year ago

Lol straight off of ChatGPT

upvoted 2 times

  **Cuddles** 1 year, 7 months ago

It's possible, but I don't think it's the MOST possible. It's much more likely they turned on airplane mode while flying and never turned it back on

upvoted 7 times

Which of the following file extensions are commonly used to install applications on a macOS machine? (Choose three.)

- A. .mac
- B. .pkg
- C. .deb
- D. .dmg
- E. .msi
- F. .appx
- G. .app
- H. .apk

Correct Answer: BCG

Manzer Highly Voted 1 year, 11 months ago

Selected Answer: BDG

.deb is linux
upvoted 13 times

andrizo 1 year, 11 months ago

.dmg is the 3rd one i believe
upvoted 3 times

cecegilbert Highly Voted 1 year, 7 months ago

Selected Answer: BDG

pkg, dmg, app
upvoted 8 times

Philco Most Recent 2 weeks ago

B;D;G;

C---A deb package (.deb file) is a software package in a specific format designed for Debian-based distributions recognized by the .deb extension. Deb packages allow installing local software on an Ubuntu system.

upvoted 1 times

Philco 3 weeks, 5 days ago

D.dmg---B.pkg---G.app are the correct answers-----check comptia exam objectives #1.10 The C answer here is wrong
upvoted 1 times

Jay23AmMonsIV 3 months ago

Selected Answer: BDG

For installing applications on a macOS machine, the commonly used file extensions are:

.pkg - This is a package file used by macOS Installer. It can install software and place files in various locations on the system.

.dmg - This is a disk image file used to distribute software. When opened, it mounts a virtual disk on the desktop containing the application, which can then be dragged to the Applications folder.

.app - This is an application bundle containing the executable and all necessary resources for the application. It is usually found in the Applications folder after installation.

upvoted 1 times

Startropic1 3 months, 3 weeks ago

Mac files do not use file extensions....
upvoted 1 times

ConqiD 12 months ago

Pkg
Dmg
App
upvoted 2 times

sinfulhymn 1 year ago

yall need to stop voting like dumbasses

you dumbasses should read the book instead of cheating

upvoted 2 times

  **Jordan3525** 9 months, 1 week ago

dumbasses

upvoted 3 times

  **HQvRuss** 1 year ago

Selected Answer: BDG

pkg, dmg, app

upvoted 2 times

  **DerekM** 1 year, 4 months ago

Selected Answer: BDG

.deb files are for debian packages. Used by Debian-based linux distributions such as ubuntu, debian, and mint.

upvoted 3 times

  **[Removed]** 1 year, 7 months ago

this was the only multiple choice question I remebered.

upvoted 1 times

  **NotAHackerJustYet** 1 year, 7 months ago

B. .pkg, D. .dmg, and G. .app are the file extensions commonly used to install applications on a macOS machine.

A. .mac is not a valid file extension.


C. .deb is the file extension used to install applications on a Debian-based Linux operating system, not macOS.

E. .msi is the file extension used to install applications on a Windows operating system, not macOS.

F. .appx is the file extension used to install applications on a Windows 10 operating system, not macOS.

H. .apk is the file extension used to install applications on an Android operating system, not macOS.

upvoted 8 times

  **44034** 9 months, 2 weeks ago

.good I think its correct

upvoted 1 times

  **alexandrasexy** 1 year, 8 months ago



Selected Answer: BDG

B. .pkg

D. .dmg

G. .app

upvoted 2 times

  **RJ4** 1 year, 11 months ago

Selected Answer: BDG

.dmg .pkg .app

upvoted 5 times

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

Correct Answer: B

  **lilbuu** Highly Voted 1 year, 7 months ago

B. The first step that should be taken when troubleshooting the issue of a slow computer after installing a suite of security applications is to check the resource utilization using Performance Monitor. This will allow to see the usage of CPU, memory, and disk space, and identify if any specific process or application is causing high resource usage

upvoted 12 times

  **bigggman** Most Recent 4 months, 2 weeks ago

B. is correct because one must check what process is causing the high load before doing anything specific.

upvoted 1 times

  **Navigator** 1 year, 4 months ago

Selected Answer: B

This response is on point. B is the right option

upvoted 4 times

A field technician applied a Group Policy setting to all the workstations in the network. This setting forced the workstations to use a specific SNTP server. Users are unable to log in now. Which of the following is the MOST likely cause of this issue?

- A. The SNTP server is offline.
- B. A user changed the time zone on a local machine.
- C. The Group Policy setting has disrupted domain authentication on the system.
- D. The workstations and the authentication server have a system clock difference.

Correct Answer: D

  **lilbuu** Highly Voted  1 year, 7 months ago

Selected Answer: D

D. The most likely cause of the issue of users being unable to log in after a Group Policy setting was applied to all the workstations in the network is that the workstations and the authentication server have a system clock difference. This is because, when the Group Policy setting was applied it forced the workstations to use a specific SNTP server, which may not be in sync with the authentication server. This can cause issues with domain authentication as the server may not recognize the login attempts because the timestamps are not in sync.

- A. The SNTP server being offline may cause issues with time syncing, but it would not cause issues with domain authentication.
 - B. A user changing the time zone on a local machine may cause issues with time syncing, but it would not cause issues with domain authentication.
 - C. The Group Policy setting disrupting domain authentication on the system is a possible cause, but it is less likely than the system clock difference.
- upvoted 14 times

  **GL1494** Highly Voted  1 year ago

This question was exactly like that in my test that I passed today. If you study from here you have 85% to pass the test. D is the answer

upvoted 12 times

  **phanton** Most Recent  1 year, 4 months ago

The Group Policy setting that forced the workstations to use a specific SNTP server is the most likely cause of the issue where users are unable to log in now. The reason for this is that time synchronization is critical in Active Directory domains, and if the SNTP server is not accessible or incorrect, domain authentication will fail. Therefore, the Group Policy setting has disrupted domain authentication on the system. The issue can be resolved by either removing the Group Policy setting or ensuring that the SNTP server is accessible and correct.

upvoted 2 times

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

Correct Answer: D

  **Belachin** Highly Voted 1 year, 11 months ago

The answer is Differential, A
upvoted 15 times

  **ha_ha** 8 months, 3 weeks ago

It would require fewer tapes than a full backup but potentially more than two, depending on the backup schedule.
upvoted 2 times

  **Slindsey0304** Highly Voted 1 year, 4 months ago


Selected Answer: A

The answer is A. Per Professor Messer. Restoring a differential backup is also a moderate amount of time, because we're not going to need any more than two sets of backup information. That would be your full backup and the last differential backup. When you perform a differential backup, you are not clearing the archive attribute because you're going to perform this backup again on the next differential backup.
upvoted 5 times

  **Mr_Tension** Most Recent 5 months, 1 week ago

Selected Answer: A

you guys are everywhere. keep it simple .yeah? they required 2 set of tapes to restore. First tape which has full backup and second tape (differential) which has all differential data since last back up. if you still confused, watch out here:
https://docs.google.com/document/d/1u4Tfh8v_EHV-Jkc1lLa1qCN1N_0FwHcEwllHKv0y4RU/edit?usp=sharing
upvoted 2 times


  **yutface** 5 months, 1 week ago

Nowhere in the study material is there a mention of these tapes and what their capacity may be or what they even are really. It requires knowledge outside of the scope of core 2. Another example of a bad question from comptia.
upvoted 4 times

  **bobby** 5 months, 3 weeks ago

Selected Answer: A

While in the real world i believe the answer should be D as I would want to have a backup in 2 location the answer appears to be A. I hate these questions because a large # of them are opinion based.
upvoted 3 times


  **sam3210** 7 months ago

Selected Answer: C

Incremental backup (Option C): An incremental backup includes only the data that has changed since the last backup, whether it was a full or incremental backup. In a scenario where only two sets of tapes are required for restoration, incremental backups are more efficient as they capture changes since the last backup, be it full or incremental.
upvoted 1 times

  **ha_ha** 8 months, 3 weeks ago

The correct answer is D. full backup. A full backup creates a complete copy of all selected files and folders. This would indeed be the option that requires only two sets of tapes for a restore, as each set would represent a complete backup.
upvoted 2 times

  **Jimbojkd** 8 months, 1 week ago

I agree, I have done my research.
A full backup involves creating a copy of all data on the workstation, including system files and user-created data, and storing it on a set of tapes. This ensures that all data is backed up, and ensures that the data can be restored in the event of a system failure or data loss.
upvoted 1 times

  **Jimbojkd** 8 months ago

The 3-2-1 backup rule states that technicians should keep backed-up data across two media types.The 3-2-1 backup rule states one full backup copy will be held offline and off-site.
upvoted 1 times

[-]  **Chavozamiri** 9 months, 1 week ago

Selected Answer: A

A. Differential backup
upvoted 1 times

[-]  **FrostyBoi** 11 months, 2 weeks ago

The way I see it, a differential backup works because of the two tapes.
One tape is a full backup, with the second having a differential backup for the changed files. That way you save both your baseline, as well as the up to date files.
upvoted 3 times

[-]  **joe_sol_arch** 1 year ago

Correct answer is D, Full backup. Read the question again. He is using TAPES for backup.
upvoted 3 times

[-]  **Mehsotopes** 1 year, 1 month ago

Selected Answer: D

You need at least one full backup between two drives to keep full storage security incase of failure at any time.
upvoted 3 times

[-]  **tolchandler** 1 year, 1 month ago

C: An incremental backup method would be the best option for setting up a backup method on a workstation that only requires two sets of tapes to restore.
upvoted 1 times

[-]  **Christianjr35** 12 months ago

Incremental backup needs more than 2 set of tapes because they require new tape for each day of backup.
upvoted 3 times

[-]  **solaWONDER** 1 year, 2 months ago

THE ANSWER IS A
upvoted 1 times

[-]  **[Removed]** 1 year, 7 months ago

Selected Answer: A

Absolutely A
upvoted 1 times

[-]  **NotAHackerJustYet** 1 year, 7 months ago

The correct answer is D. Full Backup. A full backup only requires two sets of tapes to restore because it backs up all the data from the workstation. With a differential backup, the backups need to be taken multiple times over a period of time, so more tapes would be needed to restore the data. Off-site backup involves storing the data in a remote location, so tapes would not be necessary. Lastly, an incremental backup requires multiple tapes because it only backs up the data that has changed since the last backup, so multiple tapes would be necessary to restore the data.
upvoted 4 times

[-]  **007madmonk** 1 year, 8 months ago

Selected Answer: D

A full backup takes two tapes. The question asks for two tapes.
upvoted 2 times

[-]  **KURALEW** 1 year, 1 month ago

In full backup you may need more than 2 tapes .so the correct answer is C
upvoted 1 times

[-]  **007madmonk** 1 year, 8 months ago

no wait nevermind it is A. Tape 1 the full back up tape 2 the data that changed since the last full backup.
upvoted 6 times

[-]  **alexandrasexy** 1 year, 8 months ago

Selected Answer: A

Two tapes = A. Differential backup
upvoted 2 times

A technician receives a call from a user who is on vacation. The user provides the necessary credentials and asks the technician to log in to the user's account and read a critical email that the user has been expecting. The technician refuses because this is a violation of the:

- A. acceptable use policy.
- B. regulatory compliance requirements.
- C. non-disclosure agreement.
- D. incident response procedures.

Correct Answer: A

[-]  **NotAHackerJustYet** Highly Voted  1 year, 7 months ago

The correct answer is A. acceptable use policy. Acceptable use policies are designed to protect the security and privacy of user accounts and data, and it is a violation of these policies for a technician to log in to a user's account without the user's explicit permission. Regulatory compliance requirements are not related to this issue, as they generally refer to specific laws and regulations that a company must follow, such as those related to data privacy and security. Non-disclosure agreements typically refer to contracts that are signed between two or more parties, and may not apply in this situation. Incident response procedures generally refer to steps that a company takes in response to a security incident, such as a data breach, and do not apply here.

upvoted 7 times

[-]  **[Removed]** 1 year, 4 months ago

You stated the tech did not have permission, but the question states the user gave his credentials and made a request for the tech to log into his account- sounds like permission was given to me.

upvoted 5 times

[-]  **newbytechy** Most Recent  6 months, 1 week ago

I'm leaning towards B. My reasoning is that the question states "critical email". We don't necessarily know what type of information could be in that email. It can range from PII, Health Care information etc. Since those fall within the category of Common compliance requirements which are EU GDPR (General Data Protection Regulation)

GLBA (Gramm-Leach-Bliley Act)

HIPAA (Health Insurance Portability and Accountability Act)

PIPEDA (Personal Information Protection and Electronic Documents Act)

CCPA (California Consumer Privacy Act). These are all Regulatory Compliance Requirements. Even though the user gave the technician permission to log on, this isn't something the technician should do. Which falls under the "least privilege access rule". This isn't something the technician is required to do his/her job so the technician should not be engaging and that's why the technician refused.

upvoted 1 times

[-]  **AnnoyingIAGuy** 1 year, 6 months ago

Selected Answer: A

A is the answer

upvoted 2 times

[-]  **Rafid51** 1 year, 6 months ago

Selected Answer: A

(AUP) Acceptable use policy is the answer.


upvoted 2 times

[-]  **LeeRoy616** 1 year, 6 months ago

Selected Answer: A

The Answer is A, Acceptible use policy (AUP). Regulatory compliance involves following external legal mandates set forth by state, federal, or international government.

upvoted 3 times

[-]  **sigidy** 1 year, 7 months ago

B is the answer

upvoted 1 times

[-]  **examreviewer** 1 year, 7 months ago

Selected Answer: B

B should be the Answer

upvoted 1 times

[-]  **PatrickH** 1 year, 8 months ago

Selected Answer: B

Thats a compliance issue. Complying to HIPAA, GDPR etc... Not an acceptable Usage issue

upvoted 2 times

  **Ralf_G** 8 months ago

The "definition", from Google, of: regulatory compliance states: Organizational efforts to comply with relevant laws, policies, and regulations.

This has more to do with data protection and money laundering etc. than with security in a network

upvoted 1 times

Question #123

Topic 1

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 .lock file extension. Which of the following actions is the FIRST step the technician should take?

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

Correct Answer: D

  **Dido1963** Highly Voted  1 year, 8 months ago

A ransomware attack may be the reason for the lock-files.

And the second step of malware removal steps is, to bring the computer into Quarantine.

(First step was "Identify and research malware symptoms", and to see *.lock-Files is that step)

upvoted 10 times

  **NotAHackerJustYet** Highly Voted  1 year, 7 months ago

The first step the technician should take is to disconnect the machine from the network. This is important to prevent the spread of the malicious software or virus which has caused the files to be changed, and to prevent the user from opening any additional files which may be affected.

Disconnecting the machine from the network will also prevent the hacker from continuing their attack. The other options are not appropriate as a first step, as they will not prevent further attacks or the spread of the malicious software.

upvoted 5 times

  **JollyGinger27** Most Recent  1 year, 7 months ago

Selected Answer: D

The first step is to identify the symptoms of malware, which was done already by looking at the .lock files, likely caused by ransomware. The first thing to do after that is to quarantine (disconnect) the machine from the network to prevent further contamination to other systems. D is the answer

upvoted 3 times

A user is attempting to browse the internet using Internet Explorer. When trying to load a familiar web page, the user is unexpectedly redirected to an unfamiliar website. Which of the following would MOST likely solve the issue?

- A. Updating the operating system
- B. Changing proxy settings
- C. Reinstalling the browser
- D. Enabling port forwarding

Correct Answer: B

  **NotAHackerJustYet** Highly Voted  1 year, 7 months ago

The correct answer is B. Changing proxy settings. Proxy settings determine where a user's internet traffic is routed and can sometimes be hijacked by malicious websites, redirecting the user to unexpected destinations. By changing the proxy settings, the user can ensure that their internet traffic is routed to the correct destination.

Updating the operating system and reinstalling the browser will not necessarily solve the issue, as the problem is not with the browser or operating system, but with the proxy settings. Additionally, enabling port forwarding will not help, as port forwarding is used to open a specific port for incoming traffic and does not affect the web traffic that is associated with the issue.

upvoted 17 times

  **andriipovkh** Most Recent  1 month, 1 week ago

Selected Answer: B

Mr_Tension is right.

upvoted 1 times

  **Mr_Tension** 5 months, 1 week ago

Selected Answer: B

ShukazoPenguin is right

upvoted 2 times

  **ShukazoPenguin** 9 months, 1 week ago

Selected Answer: B


Calebdames is right.

upvoted 3 times

  **maggie22** 1 year ago

Answer is A. Because an attacker can use many different tactics to launch browser redirection, the mitigation is not straightforward. However, implementing end-user education, maintaining updates for browsers and operating systems, and ensuring that your antimalware/antivirus software is up-to-date are best practices to protect against browser redirection. Comptia a+ study guide latest edition Chapter 19, page 1318 "Troubleshooting Operating Systems and Security.

upvoted 1 times

  **FreddieB** 9 months, 2 weeks ago

That sounds more like a proactive response but in this case the issue is already in effect. So checking the proxy makes sense.

upvoted 1 times

  **Calebdames** 1 year, 4 months ago

Selected Answer: B

NotAHackerJustYet is right

upvoted 2 times

  **Dido1963** 1 year, 8 months ago

Selected Answer: B

A Proxy can redirect a website to another website.

So may be there is a wrong proxy in the Internet Explorer configurated

upvoted 3 times

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

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

Correct Answer: A

  **mohdAj** 9 months, 3 weeks ago

Selected Answer: A

A risk analysis must be completed before a change request for an upcoming server deployment can be approved
upvoted 2 times

  **Wiz_tech101** 1 year, 4 months ago

Selected Answer: A

By going through the Change Management Processes:

- Request Forms
- Purpose of the change
- Scope of the change
- Risk analysis
- Change board and approvals
- End user acceptance

Thus, it is A: Risk Analysis as this step must be completed before approvals.

upvoted 4 times

  **EngAbood** 1 year ago

Thanks

upvoted 2 times

  **Wiz_tech101** 1 year, 4 months ago

By going through the Change Management Processes:

- Request Forms
- Purpose of the change
- Scope of the change
- Risk analysis
- Change board and approvals
- End user acceptance

Thus, it is A: Risk Analysis as this step must be completed before approvals.

upvoted 3 times

Which of the following is a consequence of end-of life 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.

Correct Answer: C

[-]  **[Removed]** Highly Voted  1 year, 5 months ago

Selected Answer: C

End-Of-Life operating systems are just OS's that are no longer supported by the manufacture. So it will still work as before but will no longer receive updates.

upvoted 5 times

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

- A. The technician presses the Ctrl+Alt+Del keys to open the Force Quit menu, selects the frozen application in the list, and clicks Force Quit.
- B. The technician clicks on the frozen application and presses and holds the Esc key on the keyboard for 10 seconds which causes the application to force quit.
- C. The technician opens Finder, navigates to the Applications folder, locates the application that is frozen in the list, right-clicks on the application, and selects the Force Quit option.
- D. The technician opens the Apple icon menu, selects Force Quit, selects the frozen application in the list, and clicks Force Quit.

Correct Answer: D

[-]  **DeQyaba** Highly Voted  9 months, 2 weeks ago

This is absolutely a question on the test and the answer is D.

upvoted 5 times

[-]  **Raffaello** Most Recent  9 months ago

Selected Answer: D

Correct is D

Similar to Windows' Ctrl+Alt+Delete Task Manager, the Command+Option+Esc shortcut opens the Force Quit box, which lets you force-quit troublesome programs

upvoted 2 times

[-]  **Christianjr35** 12 months ago

cmd + option + escape for force quit not control.

upvoted 3 times

[-]  **Calebdames** 1 year, 4 months ago

Selected Answer: D

Dido is Right

upvoted 2 times

[-]  **Dido1963** 1 year, 8 months ago

Selected Answer: D

<https://support.apple.com/de-de/HT201276>

upvoted 4 times

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

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

Correct Answer: C

  **Raffaello** 9 months ago

Selected Answer: C

Computer users who are blind usually use a screen reader for most computing activities. This, in simple terms, is a piece of software that "figures out" what is on the screen and sends information to a speech synthesizer to be spoken or to a braille display

upvoted 2 times

  **SadRabbit** 9 months ago

Selected Answer: C

The Ease of Access Center is there for individuals who have a hard time operating Windows. This often means someone who is colorblind, hard of hearing, or cant read the screen typically.

upvoted 3 times

  **DeQyaba** 10 months, 1 week ago

Ease of access is the answer.

upvoted 1 times

A user received the following error upon visiting a banking website:

The security certificate presented by this website was issued for a different website's address.

A technician should instruct the user to:

- A. clear the browser cache and contact the bank.
- B. close out of the site and contact the bank.
- C. continue to the site and contact the bank
- D. update the browser and contact the bank.

Correct Answer: B

  **DerekM** Highly Voted  1 year, 4 months ago

Selected Answer: B

A technician should instruct the user to B. close out of the site and contact the bank.

The error message indicates that the security certificate presented by the website does not match the address of the website the user is trying to access. This could be due to a misconfiguration on the website's end or a potential phishing attempt. In either case, it is not safe to continue to the site, and the user should contact the bank to verify the website's legitimacy. Clearing the browser cache or updating the browser would not resolve this issue.

upvoted 6 times

  **sam3210** Most Recent  7 months ago

Selected Answer: A

Clear the browser cache (Option A): The error message suggests a mismatch between the website's security certificate and the actual website address. Clearing the browser cache can help resolve issues related to cached or outdated information, including certificates.

upvoted 1 times

  **chenhan** 11 months, 2 weeks ago

Selected Answer: B

B. close out of the site

"Security certificate problems may indicate an attempt to fool you or intercept data you send to the server. We recommend that you close this webpage and do not continue to this Web site."

Reference from Microsoft Support: <https://support.microsoft.com/en-us/topic/-there-is-a-problem-with-this-website-s-security-certificate-when-you-try-to-visit-a-secured-website-in-internet-explorer-0b8931a3-429d-d0e2-b38f-66b8a15fe898>

upvoted 2 times

  **Ily5031** 12 months ago

Selected Answer: A

The technician should instruct the user to clear the browser cache and contact the bank (option A). This error indicates that the website the user is visiting is not the correct website and is likely due to a cached version of the website being stored in the user's browser. Clearing the browser cache should remove any stored versions of the website and allow the user to access the correct website. The user should also contact the bank to confirm that they are visiting the correct website and to report the error.

upvoted 1 times

A technician connects an additional monitor to a PC using a USB port. The original HDMI monitor is mounted to the left of the new monitor. When moving the mouse to the right from the original monitor to the new monitor, the mouse stops at the end of the screen on the original monitor. Which of the following will allow the mouse to correctly move to the new monitor?

- A. Rearranging the monitor's position in display settings
- B. Swapping the cables for the monitors
- C. Using the Ctrl+Alt+=> to correct the display orientation
- D. Updating the display drivers for the video card

Correct Answer: A

  **lilbuu** Highly Voted 1 year, 7 months ago


Selected Answer: A

A. Rearranging the monitor's position in display settings

Explanation:

A. Rearranging the monitor's position in display settings will allow the mouse to correctly move to the new monitor. This is because the position of the monitors in the display settings determines how the mouse behaves when moving between them. By rearranging the monitors, the technician can ensure that the mouse moves seamlessly between them, allowing the user to work across both screens.

upvoted 11 times

  **Sayed1245** 1 year, 1 month ago

Hello sir do you have the rest of questions if you have could you please give it to me thanks.

upvoted 2 times

A user is unable to use any internet-related functions on a smartphone when it is not connected to Wi-Fi. When the smartphone is connected to Wi-Fi, the user can browse the internet and send and receive email. The user is also able to send and receive text messages and phone calls when the smartphone is not connected to Wi-Fi. Which of the following is the MOST likely reason the user is unable to use the internet on the smartphone when it is not connected to Wi-Fi?

- A. The smartphone's line was not provisioned with a data plan
- B. The smartphone's SIM card has failed.
- C. The smartphone's Bluetooth radio is disabled
- D. The smartphone has too many applications open

Correct Answer: A

  **BabaBoer** 7 months, 2 weeks ago

Selected Answer: A

Cant believe it is an actual question *facepalm*

upvoted 1 times

  **Footieprogrammer** 1 year ago

Selected Answer: A

It's A, the user can send and receive calls. So the sim card is functional but lacking a dataplan

upvoted 2 times

  **[Removed]** 1 year, 5 months ago

Selected Answer: A

Key is correct. it's A

upvoted 3 times

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.

Correct Answer: D

  **Dido1963** Highly Voted  1 year, 8 months ago

Selected Answer: D

A Python Interpreter has to be installed before a ".py"-Script can run
upvoted 11 times

  **Dat_Oyin** Most Recent  1 month, 2 weeks ago

D I think
upvoted 1 times

  **tolchandler** 1 year, 1 month ago

B: This message is often seen when attempting to open a file that does not have a default program associated with it. The error message likely appears because the script "Inventory.py" was not built or designed to run on the Windows operating system.
upvoted 1 times

  **dcv1337** 1 year, 1 month ago



Selected Answer: D

The Python interpreter is not installed or associated with .py files on the computer.
upvoted 1 times

  **[Removed]** 1 year, 5 months ago

Selected Answer: D

This is covered in 1102 material. anything with .py at the end is python related. process of elimination indicates "D" is the only answer that makes sense.
upvoted 1 times

  **fiela1** 1 year, 5 months ago

There are always questions in the Comptia exams that aren't relevant to the module or even certificate being done. They're there for research purposes and don't count towards the person sitting the exams grade
upvoted 3 times

  **SeeSeeE** 1 year, 6 months ago

This is not mentioned in the Prof. Messor when he speaks about Python in the "Scripting Languages" video. I rewatched it; nothing. I'm not a programmer, so D wasn't my first guess.
upvoted 2 times

A company discovered that numerous computers from multiple geographic locations are sending a very high number of connection requests which is causing the company's web server to become unavailable to the general public. Which of the following attacks is occurring?



- A. Zero day
- B. SQL injection
- C. Cross-site scripting
- D. Distributed denial of service

Correct Answer: D

  **shkhsprre** 10 months, 2 weeks ago

why isn't this a brute force attack?

upvoted 1 times

  **igorclapa** 5 months, 3 weeks ago

DDoS is a kind of brute-force attack

upvoted 1 times

  **Footieprogrammer** 1 year ago

Selected Answer: D

It's D, DDoS-ing is when you overload a webserver with traffic requests

upvoted 3 times

  **dcv1337** 1 year, 1 month ago

Selected Answer: D

The numerous computers from multiple geographic locations are sending a very high number of connection requests, which is causing the company's web server to become unavailable to the general public. So, the correct answer is D. Distributed denial of service.

upvoted 1 times

  **ScorpionNet** 1 year, 4 months ago

Selected Answer: D

D is correct. Because DDoS is when an attacker send so many ping requests like DoS but there's more than one device. And when theres multiple computers that became zombies or botnets. Then the attacker including zombies, or bots sends too many ping requests that it decreases performance on the server itself making internet connections very slow.

upvoted 3 times

A technician suspects the boot disk of a user's computer contains bad sectors. Which of the following should the technician verify in the command prompt to address the issue without making any changes?

- A. Run sfc / scannow on the drive as the administrator
- B. Run cleanmgr on the drive as the administrator
- C. Run chkdsk on the drive as the administrator
- D. Run dfrgui on the drive as the administrator

Correct Answer: C

  **NotAHackerJustYet** Highly Voted  1 year, 7 months ago

Answer: C. Run chkdsk on the drive as the administrator.

The command chkdsk (check disk) is used to detect and repair disk errors, including bad sectors. It runs a scan of the disk and displays any errors that are found. The other commands (sfc / scannow, cleanmgr, and dfrgui) are not used to detect and repair disk errors and therefore are not the correct answer.

upvoted 8 times

  **lizb7223** 1 year, 3 months ago

Ditto Notahacker- some resources

For chkdsk info: <https://www.dell.com/support/kbdoc/en-us/000148643/using-the-chkdsk-utility>

For sfc /scannow <https://support.microsoft.com/en-us/topic/use-the-system-file-checker-tool-to-repair-missing-or-corrupted-system-files-79aa86cb-ca52-166a-92a3-966e85d4094e>

cleanmgr is a basic disk clean up tool

dfrgui is for defragmenting (Which obv changes the files)

upvoted 2 times

  **1337Minty** Most Recent  1 year, 5 months ago

Selected Answer: C

The key words in the question is: "without making any changes"

Which would leave the answer to be C because with chkdsk: examines disk space and disk use and provides a status report specific to each file system.

sfc /scannow will replace corrupted files.

upvoted 4 times

  **user82** 1 year, 9 months ago

Why isn't A the answer? chkdsk removes bad sectors from hard disk permanently. sfc/scannow scans all protected system files and replaces corrupted files with cached copy in a compressed folder.

<https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/chkdsk?tabs=event-viewer>

upvoted 1 times

  **[Removed]** 1 year, 9 months ago

You literally answered your own question and even provided proof of it. C is the correct answer.

upvoted 12 times

A BSOD appears on a user's workstation monitor. The user immediately presses the power button to shut down the PC, hoping to repair the issue. The user then restarts the PC, and the BSOD reappears, so the user contacts the help desk. Which of the following should the technician use to determine the cause?

- A. Stop code
- B. Event Viewer
- C. Services
- D. System Configuration

Correct Answer: A

  **Dido1963** Highly Voted 1 year, 8 months ago

Selected Answer: A

If the Blue Screen of Death comes again, if you switch the computer off and than on, than you can not go to the eventviewer. But you can read in the BSOD a stopp Code and look for that code in the internet

upvoted 23 times

  **Dido1963** 1 year, 8 months ago

look (not lock)

upvoted 7 times

  **BIZ2021** Most Recent 2 months, 1 week ago

Selected Answer: A

BSOD describes an error of some kind that hits the operating system hard enough that it's forced to quit. Microsoft itself labels such errors with "stopcodes." Thus these errors may also be generically named "stop errors."

upvoted 1 times

  **Kirby87** 7 months, 1 week ago

You raise a valid point. My apologies for the oversight. In the scenario where the system encounters a BSOD, and the user is unable to access the desktop or Event Viewer after restarting, the best initial step for a technician would be to analyze the Stop Code displayed on the BSOD screen.

A. Stop code

The Stop Code (Option A) is a specific error code displayed on the BSOD that can provide valuable information about the cause of the system crash. Technicians can use the Stop Code to identify the nature of the error and start troubleshooting the issue.

I appreciate your clarification, and I apologize for any confusion caused by the initial response.



upvoted 1 times

  **Raffaello** 9 months ago

Selected Answer: B

Click the Restart button on the Startup Settings screen, and when your system reboots to the Startup Options page, hit the number beside Safe Mode or Safe Mode with Networking (if you want to use the Internet). Once your PC boots into Safe Mode, open the Event Viewer to check for the cause of the BSOD.

upvoted 2 times

  **StayPorras** 9 months, 2 weeks ago

Selected Answer: B

Its B.

If you already completed core 1 you should know To check the blue screen log in Windows, go to Event Viewer, expand "Windows Logs," and select "System." Look for events labeled "BugCheck" to find information about the blue screen error.

Professor messer agrees too <https://www.youtube.com/watch?v=L2E7vpj3lq8>

upvoted 1 times

  **[Removed]** 1 year, 5 months ago

Selected Answer: A

Has to be A. While event viewer could help. the BSOD will not allow you in to use it so the only option is the stop code.

upvoted 3 times

  **Oxolane** 1 year, 6 months ago

The answer is A, using Jason Dion's Practice quizzes, this answer is literally on there. You need the stop code to solve this issue. I also thought event viewer but you can't access the computer and the BSOD is intended to help diagnose the problem with a stop code.

upvoted 3 times

  **Dime_Baggins** 1 year, 7 months ago



Selected Answer: A

A and not B because you cant login to look at the event viewer due to the BSODs.
upvoted 2 times

  **cecegilbert** 1 year, 7 months ago

Selected Answer: A

the screen will show additional code that you can research on Microsoft's websites by tha technician can determine the cause
upvoted 2 times

  **lilbuu** 1 year, 7 months ago



Selected Answer: B

B. Event Viewer is the best option to determine the cause of a BSOD on a user's workstation. Event Viewer is a tool that allows administrators to view detailed information about system events and application events. The tool can be used to troubleshoot and diagnose system errors, including BSODs. The technician can look at the event logs to identify the cause of the BSOD, such as a driver issue, hardware malfunction, or software problem.
upvoted 2 times

  **Nick40** 1 year, 8 months ago

Selected Answer: B

gonna go with event viewer.
upvoted 1 times

  **Rockrl** 1 year, 8 months ago



How can the answer be B when your are unable to log into the systems because you keep getting BSOD?

The best answer would be A - BSOD Stop Code, you can then research the code and find what exactly is causing the crash.
upvoted 11 times

  **Nick40** 1 year, 9 months ago

Selected Answer: B

I'm going to go with B.
upvoted 1 times

  **LayinCable** 1 year, 5 months ago

youre trolling.
upvoted 1 times

  **kingwillowdon** 11 months, 1 week ago

chatgpt says event viewer and after asking it how can that be the answer when you cant view event viewer from BSOD it changed its answer to stop code
upvoted 1 times

Which of the following is the STRONGEST wireless configuration?

- A. WPS
- B. WPA3
- C. WEP
- D. WMN

Correct Answer: B

  **yutface** 7 months, 1 week ago

Strongest? WPA3 is most secure maybe. This is not worded well.

upvoted 2 times

  **SadRabbit** 9 months ago

Selected Answer: B

WPA3 superseded all the other options making WPA3 the strongest

upvoted 3 times

A technician is installing new network equipment in a SOHO and wants to ensure the equipment is secured against external threats on the Internet. Which of the following actions should the technician do FIRST?

- A. Lock all devices in a closet.
- B. Ensure all devices are from the same manufacturer.
- C. Change the default administrative password.
- D. Install the latest operating system and patches.

Correct Answer: C

  **ScorpionNet** **Highly Voted**  1 year, 4 months ago

Selected Answer: C

C is correct because you want to change the default administrator password because the default password is considered insecure. The reason is that default passwords can be easy for the attacker to guess for example the username is admin and the password is password (cisco for Cisco, and pfsense for PfSense). SuperAdmin and P@\$w0rd is more secure.

upvoted 6 times

  **SadRabbit** **Most Recent**  9 months ago

Selected Answer: C



Default administrative passwords in general are usually unsecure and can be brute forced so its good practice to change them first

upvoted 2 times

  **Oxolane** 1 year, 6 months ago

Yes, I believe so as this sort of question was answered before. You would first have to change default passwords and then you could do other things such as installing the latest operating system and patches.

upvoted 2 times

  **minx98** 1 year, 6 months ago

is this correct?

upvoted 1 times

While assisting a customer with an issue, a support representative realizes the appointment is taking longer than expected and will cause the next customer meeting to be delayed by five minutes. Which of the following should the support representative do NEXT?

- A. Send a quick message regarding the delay to the next customer.
- B. Cut the current customer's time short and rush to the next customer.
- C. Apologize to the next customer when arriving late.
- D. Arrive late to the next meeting without acknowledging the time.

Correct Answer: A

  **EddyNL** 1 year, 5 months ago

Selected Answer: A

One could argue that sending a message cost time , and also you should apologize for being late. But the key words here are NEXT and QUICK. Therefore I believe it is A.

upvoted 3 times

  **minx98** 1 year, 6 months ago

is it not D?

upvoted 1 times

  **minx98** 1 year, 6 months ago

I MEAN C

upvoted 1 times

  **SadRabbit** 9 months ago

It makes sense to apologize but informing them you will be late should be first so they know you are acknowledging that you're late and then you can apologize right after

upvoted 1 times

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

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

Correct Answer: D

  **DerekM** Highly Voted  1 year, 4 months ago

Selected Answer: D

An Evil Twin attack is a type of wireless network attack where an attacker sets up a rogue wireless access point (AP) that mimics a legitimate one. The attacker's goal is to intercept wireless traffic from legitimate users who connect to the rogue AP, steal sensitive information such as login credentials, financial information, or other confidential data, and potentially conduct other malicious activities. The Evil Twin attack can be carried out using several methods, including using social engineering techniques to trick users into connecting to the rogue AP or using tools to deauthenticate users from the legitimate AP to force them to connect to the rogue one.

upvoted 12 times

  **ted19** Most Recent  1 month, 1 week ago

Selected Answer: D

Evil Twin

upvoted 1 times

  **Footieprogrammer** 1 year ago

Selected Answer: D


Evil twin attack

upvoted 1 times

  **Neldave027** 1 year, 4 months ago

B is the correct answer

upvoted 1 times

  **bleufee** 1 year, 2 months ago

vishing is by phone

upvoted 1 times

  **TonxhiPatonxhi** 1 year, 1 month ago

that guy and more like him recently on the dumps gets the answers from ChatGPT without even thinking for themselves...even ChatGPT needs to be corrected or challenged into thinking

upvoted 6 times

  **ScorpionNet** 1 year, 4 months ago

Selected Answer: D

D is correct because Evil Twin aka WAP spoofing is a wireless related attack where the attacker makes a fake access point to steal information from the victim.

upvoted 3 times

  **Dido1963** 1 year, 8 months ago

<https://www.pandasecurity.com/en/mediacenter/security/what-is-an-evil-twin-attack/>

upvoted 3 times

A new service desk is having a difficult time managing the volume of requests. Which of the following is the BEST solution for the department?

- A. Implementing a support portal
- B. Creating a ticketing system
- C. Commissioning an automated callback system
- D. Submitting tickets through email

Correct Answer: A

  **[Removed]** Highly Voted  1 year, 9 months ago

Selected Answer: B

There's just no way it's A. Sure, you can have a database where everyone can search up help for themselves, but as a guy who is currently working as a Tech Support Rep, the number of dumb callers who can't read a support portal is astounding.

Also, if you want to manage requests, just have a ticketing system. A support portal will maybe lessen the number of requests, but there is no way that it helps in managing those requests.

upvoted 17 times

  **Nick40** 1 year, 9 months ago

As someone who works in a support desk position, I see how it could be the answer. A ticketing system is inevitable, so I could see how adding a support portal would help, it does in fact help us.

upvoted 6 times

  **NotAHackerJustYet** Highly Voted  1 year, 7 months ago

The best solution for the department is B. Creating a Ticketing System. A ticketing system is a comprehensive tool for managing the volume of requests that come in, allowing for assignments, tracking, and updates. It also allows for the department to track the progress of requests and prioritize their workload. With a ticketing system, the department can ensure that no requests go unanswered and that requests are serviced in an efficient and timely manner. The other solutions are not as comprehensive and do not provide the same level of management and tracking that a ticketing system does.

upvoted 6 times

  **SDXIN** Most Recent  4 months, 2 weeks ago

Selected Answer: A

Reducing volume means user guidance without any action from IT.

upvoted 1 times

  **yutface** 5 months, 3 weeks ago

Selected Answer: A

The hidden question here is "How do you cut back on the amount of service requests?" The answer is the Service Portal, preventing so many tickets from coming in.

upvoted 1 times

  **crazymonkeh** 6 months ago

Selected Answer: A

Creating a ticketing system does not reduce the amount of requests. It just organizes them appropriately where a tech will service them in the order they were received...

The correct answer is A because a support portal contains self help tools, and FAQ documents that customers can use to help solve their own issues by themselves.

upvoted 2 times

  **Studyingcerts** 7 months, 1 week ago

Idk how but ChatGPT said it's A

upvoted 1 times

  **BestSumy** 7 months, 1 week ago

interesting my ChatGPT give me B

upvoted 1 times

  **Pisces225** 8 months, 3 weeks ago

Selected Answer: A

I agree with A.

upvoted 1 times

  **StayPorras** 9 months, 2 weeks ago

Selected Answer: A

A. Implementing a support portal

Explanation:

Implementing a support portal is a comprehensive solution for managing the volume of requests at a service desk. A support portal provides a centralized platform where users can submit and track their requests, access self-help resources, and find relevant information. It streamlines the request management process, making it more efficient and organized.

While creating a ticketing system and submitting tickets through email are components of a support portal, a dedicated support portal often includes additional features, such as knowledge bases, FAQs, and user forums. These features empower users to find solutions independently and reduce the workload on the service desk. Automated callback systems may help with communication but may not address the root cause of the volume issue.

ChatGPT source

upvoted 1 times

Mango7 11 months ago

Selected Answer: A

I confirmed its A guys.

upvoted 1 times

extrarefe 10 months, 4 weeks ago

Where is it confirmed?

upvoted 1 times

Hail_Stoneface 1 year ago

Selected Answer: B

Hass to be B

upvoted 1 times

Footieprogrammer 1 year ago

Selected Answer: B

Ticketing system is in this case.

upvoted 1 times

Mehsotopes 1 year, 1 month ago

Selected Answer: A

You can open a case/help ticket using a support portal. Ticketing systems require a support portal.

upvoted 4 times

dcv1337 1 year, 1 month ago

Selected Answer: B

A ticketing system allows service desk staff to track, prioritize, and manage incoming requests in an organized and efficient manner. This can help the department handle a high volume of requests and ensure that each request is addressed in a timely and effective manner.

upvoted 1 times

Nabilrrhmn 1 year, 1 month ago

Selected Answer: B

B. Creating a ticketing system: A ticketing system is a support tool that helps track, manage, organize, and prioritize customer requests. A ticketing system can provide features such as automatic ticket creation, intelligent routing, status tracking, reporting, and analytics. A ticketing system can also integrate with other tools such as chatbots, self-service portals, call center automation, and email to provide omnichannel support. A ticketing system can improve customer satisfaction, reduce response time, increase efficiency, and streamline workflows¹.

The other solutions are not suitable for this task because:

A. Implementing a support portal: A support portal is a website or an app that provides customers with information and resources to help them solve their issues. A support portal can include FAQs, knowledge base articles, forums, videos, and other content. A support portal can reduce the number of requests by enabling customers to find answers themselves, but it does not help manage the requests that still come in

upvoted 1 times

Wildhunt37 1 year, 3 months ago

Selected Answer: A

I think the important part to focus on is "volume". A ticketing system might make it more organized but it doesn't cut down on the volume. Even if you don't believe in a support portal, I would argue for testing purposes that A would seem like what Comptia is looking for.

upvoted 3 times

Rafid51 1 year, 6 months ago

Selected Answer: B

A ticketing system allows the service desk to efficiently manage and prioritize incoming requests.

upvoted 1 times

1Abel1 1 year, 7 months ago

Selected Answer: A

The volume of requests is too much for the service desk so therefore "Implementing a support portal" will reduce the workload because customers can go to the support portal to browse through their FAQ and also check for answers to their problem. This will indeed reduce the volume of

request at least to me extent.
upvoted 4 times

Question #141

Topic 1

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

- A. yum
- B. grep
- C. ls
- D. sudo

Correct Answer: A

NotAHackerJustYet Highly Voted 1 year, 7 months ago

Answer: A. yum. Yum is a Linux command used to install and manage packages from a repository. It is the most commonly used command for installing applications in Linux. Grep is a command used to search for a specific string in a file or set of files, ls is a command used to list the contents of a directory, and sudo is a command used to elevate privileges to perform administrative tasks.

upvoted 8 times

Raffaello Most Recent 8 months, 4 weeks ago

Selected Answer: A

YUM is a package manager for RPM-based Linux distributions such as Fedora, CentOS and Red Hat Enterprise Linux. It allows users to install, update, remove and search for software packages from various repositories. YUM also resolves dependencies and handles configuration files automatically

upvoted 1 times

KnowYourPorts 11 months, 3 weeks ago

Selected Answer: A

The dnf (or yum) command is a front-end for the RPM packaging system.
It's A

upvoted 1 times

ScorpionNet 1 year, 5 months ago

Yum for RPM and apt, or apt-get for debian based

upvoted 1 times

cecegilbert 1 year, 7 months ago

Selected Answer: A

Yellowdog Updater, Modified (yum) -
Install, delete, update

upvoted 4 times

quintusca 1 year, 8 months ago

Selected Answer: A

yum for redhat package management

upvoted 1 times

alexandrsexy 1 year, 8 months ago

Selected Answer: A

yum is the primary tool for getting, installing, deleting, querying, and managing Red Hat Enterprise Linux RPM software packages from official Red Hat software repositories, as well as other third-party repositories. yum is used in Red Hat Enterprise Linux versions 5 and later.

upvoted 1 times

Dido1963 1 year, 8 months ago

[https://en.wikipedia.org/wiki/Yum_\(software\)](https://en.wikipedia.org/wiki/Yum_(software))

upvoted 1 times

[Removed] 1 year, 9 months ago

Selected Answer: A

The yum command is used to install applications for Red Hat Enterprise Linux editions. The other install command is called apt-get.

upvoted 2 times

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.

Correct Answer: A

[-]  **Alvar_Hanso** Highly Voted 1 year, 4 months ago

Note that the question is asking what BEST describes the security benefits; it also mentions that a "client certificate" is being deployed. C and D could be prevented with other measures, they also would not label the BEST benefits. Regarding B, the client certificate would not encrypt ALL data, only the authentication mechanism or "digital handshake" for the session. Therefore A best describes the method and best security benefit gained, a multifactor authentication method. Best choice: A

upvoted 11 times

[-]  **TacosInMyBelly** 10 months, 3 weeks ago

Agreed. Also the wording makes it evident: "The certificate will be used IN CONJUNCTION with the user's existing username and password." That's textbook MFA. Answer is A

upvoted 3 times

[-]  **ChattyKathy222** Most Recent 4 months, 3 weeks ago

encryption in transit is always a VPN and it said nothing about that

upvoted 1 times

[-]  **RyeBread** 7 months ago

Selected Answer: A

The answer is A. A. Multifactor authentication will be forced for Wi-Fi. Think about what multifactor authentication is. MFA is something you know (your password) and something you have (your client certificate). Once this is verified, a server certificate will be issued to the hostname at which point traffic will be encrypted.

So technically, it will lead to encryption from the server certificate, the user will first have to input their password (something you know) then the client certificate will be shared (something you have). Multifactor authorization since it states "Client certificate".

upvoted 3 times

[-]  **Thwiseman** 7 months, 2 weeks ago

Advantages of Certificate Authentication

Using certificate authentication has many benefits that all involve making the network safer and improving the user experience.

Strong Encryption

Certificates use encryption keys to secure data between devices and the network. This level of security makes it much less likely that someone with malicious intent will be able to read the message.

upvoted 1 times

[-]  **Raffaello** 9 months ago

Selected Answer: A

First, the client performs a "client hello", wherein it introduces itself to the server and provides a set of security-related information.

upvoted 2 times

[-]  **MissJovana** 9 months, 3 weeks ago

Selected Answer: A

I believe A is correct.

In the official CompTIA book, it states: "Another advantage of EAP is support for more advanced authentication methods than simple usernames and passwords. Strong EAP methods use a digital certificate on the server and/or client machines. These certificates allow the machines to establish a trust relationship and create a secure tunnel to transmit the user credential or to perform smart card authentication without a user password. This means the system is using strong multifactor authentication."

upvoted 2 times

[-]  **haibrecol** 1 year ago

I came across this in CompTIA's CertMaster in regards to WAP's 802.1X and EAP(Extensible Authentication Protocol).

For example, EAP with Transport Layer Security (EAP-TLS) is one of the strongest types of multifactor authentication:

- 1.Both the server and the wireless supplicant are issued with an encryption key pair and digital certificate.
- 2.On the wireless device, the private key is stored securely in a trusted platform module (TPM) or USB key. The user must authenticate with the

device using a PIN, password, or bio gesture to allow use of the key. This is the first factor.

3. When the device associates with the network and starts an EAP session, the server sends a digital signature handshake and its certificate.

4. The supplicant validates the signature and certificate and if trusted, sends its own handshake and certificate. This is the second factor.

5. The server checks the supplicant's handshake and certificate and authenticates it if trusted.

upvoted 1 times

  **maggie22** 1 year ago

The answer is B. 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 password

upvoted 2 times

  **rick2461** 1 year, 1 month ago

The use of a cert alongside username and pass is related to EAP and WPA3, which encrypts the traffic. While certs might be considered multifactor, I've never seen it referenced as a multifactor option. Unclear on this one

upvoted 1 times

  **rocistuff** 1 year, 1 month ago

Selected Answer: A

Forgot to vote "A".

upvoted 4 times

  **rocistuff** 1 year, 1 month ago

I am fairly certain this is A.

Even in the imagined scenario where there's no encryption on the wifi, having a client-side certificate won't magically make the connection between the client and the router encrypted.

The client-side certificate is something installed by the admin to ensure the device itself is trusted. Without the cert, even if someone had a valid user/pass, they wouldn't be able to connect. In other words, connecting with only the certificate or only the user/pass is insufficient: therefore answer is A, multi-factor.

upvoted 2 times

  **orsopdx** 1 year, 3 months ago

Selected Answer: B

B. All Wi-Fi traffic will be encrypted in transit.



A client certificate can be used in conjunction with the user's existing username and password to establish a secure Wi-Fi connection. This method of authentication is known as mutual authentication and provides additional security by ensuring that both the client and server authenticate each other's identities. Once authenticated, all Wi-Fi traffic will be encrypted in transit, which provides additional security against eavesdropping attempts.

upvoted 2 times

  **otoshikami** 1 year, 5 months ago



A client certificate is what the user has, and the username and password are what the user knows, so it could be A. Multifactor authentication will be forced for Wi-Fi, right?

upvoted 2 times

  **Olddie** 1 year, 5 months ago

Client certificates do not encrypt or decrypt any data, unlike server certificates that encode and decode the information shared between a user and a web server. So Client Certificate+Username+Password would be MFA. IS it not?

upvoted 1 times

  **EddyNL** 1 year, 5 months ago

Selected Answer: B

Deploying a client certificate for Wi-Fi access provides two main security benefits. First, it provides cryptographically-backed assurance to the visitor that the device they're connecting to genuinely belongs to the organization they think they're connecting with. Second, it serves to encrypt the connection between the client device and the server/host end


upvoted 4 times

  **Ace_of_Spaded** 1 year, 6 months ago

Selected Answer: B

I'm going B, the SSL certificate should encrypt the traffic. Password and username isn't MFA. Certificates won't stop Rogue AP's. I think the certificate will help against eavesdropping attacks but won't fully prevent them.

upvoted 2 times

  **minx98** 1 year, 6 months ago

I'm sure this is wrong. I would go D or possible B

upvoted 1 times

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

- A. The user is not connected to the VPN.
- B. The file server is offline.
- C. A low battery is preventing the connection.
- D. The log-in script failed.

Correct Answer: A

  **Calebdames** Highly Voted  1 year, 4 months ago

Selected Answer: D

D because it says " A user in a Corporate office" they don't need to vpn into the office in order to access the network resources.
upvoted 7 times

  **RoPsur** Highly Voted  1 year, 2 months ago

Selected Answer: A

I've had to deal with many associates who had this problem and turning on the VPN turned was the solution.
upvoted 6 times

  **354fcf1** Most Recent  1 month, 3 weeks ago

I can see D, but I *HAVE* seen this situation at my work, where users are connected to a backup wi-fi and need VPN. D uses actual A+ material though
upvoted 1 times

  **StudyWithXeno** 5 months ago

As of April 2024 answer D has been changed to "files on the server are encrypted"

Correct answer is A not connected to correct VPN

Guaranteed pass CompTIA exams, AWS etc as well, Telegram @XenoMD
upvoted 1 times

  **crazymonkeh** 6 months ago

Selected Answer: D

Many corporations use a "login script" which auto-runs upon windows login. It primarily maps the network drives based on the user's access level. It also maps network printers based on facility location.

One would think the answer would be "A" as you must be on the company network to connect to company shared resources, however the user is at a "Corporate Office" already. They're connected to the corp network by default. They don't require VPN unless they're at a remote location.

The answer is obviously "D"
upvoted 2 times

  **dlittle** 9 months, 3 weeks ago

The answer given here is confusing. If a user is in the office, why would he/she need to connect to the VPN?
upvoted 4 times

  **ComPCertOn** 1 year ago

Selected Answer: D

D is correct
upvoted 2 times

  **ronniehaang** 1 year, 6 months ago

Selected Answer: D



The most likely reason the user is having this issue is that the log-in script failed. A log-in script is a set of instructions that execute when a user logs into a computer. The log-in script can be used to map network drives to the user's computer, so the user has access to the files on the network. If the log-in script fails to execute, then the network drives will not be mapped, and the user will be unable to connect to them.

It is less likely that the user is not connected to the VPN since other users have not reported any issues, and the file server is offline since other users would also be unable to access the network drives. A low battery is also an unlikely reason as it would not affect the user's ability to connect to network drives. Therefore, the failed log-in script is the most probable reason for the issue. The technician should troubleshoot the log-in script to resolve the issue.
upvoted 5 times

  **NotAHackerJustYet** 1 year, 7 months ago

The most likely reason the user is having this issue is D. The log-in script failed. Login scripts are used to perform specific tasks when a user logs into a computer or network. These scripts allow users to access network resources such as network drives. When the login script fails, the user will not be able to access these network resources. The other choices are not as likely because the user being connected to the VPN or having a low battery would not prevent them from accessing network resources, and the file server being offline would prevent all users from accessing the network drives, not just one.

upvoted 4 times

  **jtmonster** 1 year, 8 months ago

Can someone answer why it would be a vpn?

upvoted 1 times

  **quintusca** 1 year, 8 months ago

Selected Answer: D

in office no need vpn, so choose D

upvoted 2 times

  **alexandrasexy** 1 year, 8 months ago

Selected Answer: D

D. The log-in script failed.

upvoted 1 times

  **Dido1963** 1 year, 8 months ago

Selected Answer: D

He is in the Office. A VPN-Problem can only avoid him from connect to the Network drives, if he is remote (at home or f.e. in a hotel)

upvoted 3 times

  **aisling** 1 year, 9 months ago

Selected Answer: D

They are in the office

upvoted 2 times

  **Bogardinc** 1 year, 9 months ago

The answer is "A"

<https://www.wccnet.edu/mywcc/faculty-staff/its/user-services/map-drive.php>

upvoted 1 times

  **joe_sol_arch** 1 year ago

That link is dead.

upvoted 1 times

  **JohnAcc** 1 year, 9 months ago

Selected Answer: D

Has to be D. It says that the user is in the office.

upvoted 1 times

  **Paradox_Walnut** 1 year, 9 months ago

Selected Answer: D

Strange, it doesn't mention a VPN at all, or the user being away from the office, I was assume it be "D".

upvoted 1 times

A user reports a PC is running slowly. The technician suspects high disk I/O. Which of the following should the technician perform NEXT?

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

Correct Answer: C

[-]  **NotAHackerJustYet** Highly Voted 1 year, 7 months ago

The correct answer is D. msinfo32.exe. This is because msinfo32.exe is a utility that can be used to monitor the system's performance and resource usage, including I/O usage. This can be used to identify any excessive I/O activities that may be causing the slow performance. The other options are not relevant to this situation, as resmon.exe is for monitoring system resource usage, msconfig.exe is for configuring startup programs and services, and dfrgui.exe is for managing disk defragmentation.

upvoted 7 times

[-]  **ropea** 11 months, 3 weeks ago

I don't believe what this guy says half the time. Careful.


It's either Resmon or defragging. It's so close. This question is BS.

upvoted 3 times

[-]  **ropea** 11 months, 3 weeks ago

I'm going defrag just because it says what should you PERFORM next.

upvoted 2 times

[-]  **igorclapa** 5 months, 3 weeks ago

The technician SUSPECTS high disk I/O usage. He would need to verify that this is actually the case with resmon.exe to confirm suspicions. Why would he defrag anything???

upvoted 1 times

[-]  **[Removed]** 1 year ago

no msinfo32 displays a detailed list of the systems hardware and specs, resource monitor would provide you with what you just stated.

upvoted 2 times

[-]  **ollie93** Most Recent 3 months, 2 weeks ago

Selected Answer: A

To diagnose high disk I/O and understand which processes or activities are causing it, the technician should perform the following:

A. resmon.exe

Resource Monitor (resmon.exe) provides detailed real-time data about the system's resource usage, including CPU, memory, disk, and network activity. It will allow the technician to identify which processes are generating high disk I/O, helping to diagnose the cause of the slow performance.

upvoted 2 times

[-]  **GongRoca** 11 months ago

The key into this question is the technician is "suspecting" so, he has a theory and he needs to prove it. So the best way to do it is through RASMON

upvoted 4 times

[-]  **DeckardCain** 11 months, 1 week ago

Selected Answer: A

If a technician suspects high disk I/O, the technician should use the Resource Monitor (resmon.exe) to identify the process that is causing the high disk I/O.

Resource Monitor provides detailed information about the system's resource usage, including disk I/O. The technician can use this information to identify the

process that is causing the high disk I/O and take appropriate action.

upvoted 2 times

[-]  **Magdycom** 11 months, 3 weeks ago

The technician suspect vs the technician found .

If I'm the technician and I Suspect, I'll go to check resources monitor first , if I found , I'll go to defragmentation.

upvoted 2 times

[-]  **Mehsotopes** 1 year, 1 month ago

Answer could be C (dfrgui.exe) because this defragments the drive to allow disk reader find the data stored on this disk which could decrease read time that might translate to I/O. Other than that, resource monitor will keep you informed.

You can check I/O subsystems under msinfo32.exe (system information), however this only tells you statuses & does not measure performance.
upvoted 1 times

  **dcv1337** 1 year, 1 month ago

Selected Answer: A

Resmon.exe (Resource Monitor) is a tool in Windows that provides real-time information about system resource usage, including disk I/O. By running resmon.exe, the technician can monitor disk activity and determine if high disk I/O is indeed the cause of the slow performance.
upvoted 3 times

  **Maruf91** 1 year, 4 months ago

Selected Answer: A

1. resmon.exe > Disk
2. click on the Disk activity and expand
3. Go to I/O tab and you will see all applications running
upvoted 3 times

  **Brightside** 1 year, 4 months ago

Selected Answer: C

Defrag because I suspect resmon.exe and others have possibly already been run ?
The wording is doing its best to de clarify the scenario .
upvoted 1 times

  **Calebdames** 1 year, 4 months ago

Selected Answer: A

The question is definitely a confusing one, D. msinfo32.exe (System Information) does show I/O disk but not how much usage just what is using it and if it is Ok or not. A.resmon.exe (resource monitor) shows where the disk is being, and what is using it and gives a Graph so I believe its A.
upvoted 2 times

  **Oxolane** 1 year, 6 months ago

According to BING AI.
Msinfo32.exe can be used to read system information for local and remote computers¹², but it cannot be used to monitor I/O directly. You can use other tools such as Task Manager, Resource Monitor, or Performance Monitor to monitor I/O for processes.
upvoted 3 times

  **Rafid51** 1 year, 6 months ago

Selected Answer: A

Resmon.exe (Resource Monitor) is a Windows system utility that provides real-time performance data on CPU, memory, disk, and network usage. It is an effective tool for diagnosing issues related to high disk I/O, as it provides detailed information on the processes and services that are causing the high I/O.
upvoted 3 times

  **quintusca** 1 year, 8 months ago

Selected Answer: A

resmon for resource monitor application
upvoted 2 times

  **Dido1963** 1 year, 8 months ago

Selected Answer: A

At first he should use the resmon to verify, if the Disk is really the reason. If yes: the defragmentation would be the second step.
upvoted 3 times

  **Dido1963** 1 year, 8 months ago

At first he should use the resmon to verify, if the Disk is really the reason. If yes: the defragmentation would be the second step.
upvoted 1 times

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

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

Correct Answer: D

  **[Removed]** 1 year, 5 months ago

Selected Answer: D

it's D

upvoted 2 times

  **minx98** 1 year, 6 months ago



C makes most sense but I would go with D specifically to the question

upvoted 1 times

Which of the following is MOST likely contained in an EULA?

- A. Chain of custody
- B. Backup of software code
- C. Personally identifiable information
- D. Restrictions of use

Correct Answer: D

  **Raffaello** 8 months, 4 weeks ago

Selected Answer: D

It specifies the scope of the license, including whether it is perpetual or time-limited and whether it permits installation on multiple devices. The EULA may also address any limitations on usage, such as non-commercial use or restrictions on the number of users

upvoted 1 times

  **[Removed]** 1 year, 5 months ago

Selected Answer: D

EULA=End User Lease Agreement.

upvoted 2 times

  **[Removed]** 1 year, 5 months ago

end-user license agreement

upvoted 3 times

A junior administrator is responsible for deploying software to a large group of computers in an organization. The administrator finds a script on a popular coding website to automate this distribution but does not understand the scripting language. Which of the following BEST describes the risks in running this script?

- A. The instructions from the software company are not being followed.
- B. Security controls will treat automated deployments as malware.
- C. The deployment script is performing unknown actions.
- D. Copying scripts off the internet is considered plagiarism.

Correct Answer: C

  **lilbuu** Highly Voted 1 year, 7 months ago

C. The deployment script is performing unknown actions.

When an administrator does not understand the scripting language and is not familiar with the script, there is a risk that the script may be performing unknown or unintended actions on the computers. This could include unintended changes to system configurations, or the installation of malware or other malicious software. It's important to thoroughly review and test the script to ensure it performs the intended actions before deploying it in a production environment.

upvoted 6 times

  **Mamad66** Most Recent 5 months ago

Selected Answer: C

C is correct.

upvoted 1 times

  **Raffaello** 9 months ago

Selected Answer: C

Correct Answer: C

Explanation

The risks in running this script are that the deployment script is performing unknown actions. Running the script blindly could cause unintended actions, such as deploying malware or deleting important files, which could negatively impact the organization's network and data

upvoted 1 times

  **ronniehaang** 1 year, 6 months ago

Selected Answer: C

C. The deployment script is performing unknown actions.

As the junior administrator does not understand the scripting language, they cannot accurately assess what the script does or any potential risks associated with it. Running the script blindly could cause unintended actions, such as deploying malware or deleting important files, which could negatively impact the organization's network and data. It is essential to ensure that any scripts or code deployed on organizational systems are fully understood and trusted.

upvoted 4 times

A user opened a ticket regarding a corporate-managed mobile device. The assigned technician notices the OS is several versions out of date. The user is unaware the OS version is not current because auto-update is turned on. Which of the following is MOST likely the cause of the issue?

- A. The device does not have enough free space to download the OS updates.
- B. The device needs user confirmation to update to a major release.
- C. The device is not compatible with the newest version of the OS.
- D. The device is restricted from updating due to a corporate security policy.

Correct Answer: D

  **jackjack007** Highly Voted 1 year, 9 months ago

Selected Answer: A

A. The device does not have enough free space to download the OS updates = can be true
 B. The device needs user confirmation to update to a major release = because it is managed by corporate it does not require user confirmation to update, so = false
 C. The device is not compatible with the newest version of the OS. = false because it is under management of corporate and they know all devices. also the mobile is several version out of date, here it says only with the newest version
 D. The device is restricted from updating due to a corporate security policy= false. corporate security policy should update devices regularly to improve security not to prevent several versions from updating

I go with "A"
 upvoted 26 times

  **Yomijohnson** 11 months, 1 week ago

I love your explanation, thank you
 upvoted 1 times

  **GRONDBOTTER** Highly Voted 9 months, 2 weeks ago

i dont like this question
 upvoted 6 times

  **YukonV** 9 months, 1 week ago

I dont like you.
 upvoted 6 times

  **YukonV** 9 months, 1 week ago

joke tee hee
 upvoted 4 times

  **JanakPatel** Most Recent 2 months, 2 weeks ago

A corporate security policy can restrict a corporate-managed mobile device from updating its OS automatically, even if the auto-update feature is turned on. This can be done to prevent compatibility issues, security risks or performance problems caused by untested or unwanted updates. The device administrator can control when and how the updates are applied to the device. The device not having enough free space, needing domain administrator confirmation or being incompatible with the newest version of the OS are not likely Exams Prep CompTIA - 220-1102 Top IT Certification Prep Material 233 of 395 A. B. C. D. E. F. A. B. C. D. causes of the issue, since the user would receive an error message or a notification in those cases.
 upvoted 1 times

  **bobby** 5 months, 3 weeks ago

Seriously is this a real question? if OS is several generations out of date there a high chance that the phone doesn't support the newer version. Generations are a year apart and that make this phone 4~7 years out of date. except for high end phones most phones only get a couple years. this is a question that the correct answer should be to followed up with more research before jumping to the "most likely cause of the issue"
 upvoted 1 times

  **bobzilla96** 9 months, 4 weeks ago

if read through the notes, you will know that the answer is A.
 upvoted 1 times

  **DeckardCain** 11 months, 1 week ago

Selected Answer: A

With a corporate managed device using most likely using MDM (Mobile Device Manager) having a device out of date poses a unnecessary security risk to the agency.
 upvoted 1 times

  **JBSecurity101** 1 year ago

Selected Answer: A

If you studied, you'd know it's A.

upvoted 1 times

  **Walide0** 1 year ago

Selected Answer: A

Its a trick question the user will never submits a ticket because its outdated according to "several versions out of date" even more he's unaware the OS version is not current, so he must be submits it because something is wrong with his device that preventing him from doing his tasks so A is making more sense to me IMO. Please advice if i missed something.

upvoted 2 times

  **alexkeung** 1 year ago

Selected Answer: D

It is D

upvoted 1 times

  **maggie22** 1 year ago

D. because it's a corporate managed mobile device.

upvoted 1 times

  **ComPCertOn** 1 year ago

Selected Answer: D

it is D

upvoted 2 times

  **SaralITHub** 1 year ago

According to CHATGPT

Answer is B. The device needs user confirmation to update to a major release.

The most likely cause of the issue with the corporate-managed mobile device running an outdated OS despite having auto-update turned on is that the device needs user confirmation to update to a major release (option B).

upvoted 1 times

  **Mehsotopes** 1 year, 1 month ago

Selected Answer: D

The device is restricted by corporate-management from updating due to a corporate security policy, update was set to automatically start, user has not mentioned issues running, or installing other programs. A mobile phone & PC should warn you about low storage space at all times.

upvoted 2 times

  **Mehsotopes** 1 year, 1 month ago

The device is restricted by corporate-management from updating due to a corporate security policy, update was set to automatically start, user has not mentioned issues running, or installing other programs. A mobile phone & PC should warn you about low storage space at all times.

upvoted 1 times

  **HQvRuss** 1 year, 1 month ago

Selected Answer: D

just google it and look

If the user is unaware that the mobile device's OS version is not current despite auto-update being turned on, the most likely cause of the issue is that the device is restricted from updating due to a corporate security policy, option D. Corporate-managed mobile devices are often subject to specific security policies and configurations set by the organization to protect sensitive data and resources.

upvoted 2 times

  **[Removed]** 1 year, 5 months ago

Selected Answer: D

If the user is unaware that the mobile device's OS version is not current despite auto-update being turned on, the most likely cause of the issue is that the device is restricted from updating due to a corporate security policy, option D. Corporate-managed mobile devices are often subject to specific security policies and configurations set by the organization to protect sensitive data and resources. It is possible that the corporate security policy restricts OS updates to ensure compatibility with the organization's security protocols and prevent unauthorized access.



Option A, not enough free space, could cause problems with downloading and installing updates, but it would not cause the user to be unaware of the outdated OS version.

upvoted 3 times

  **Kordrakka** 1 year, 4 months ago

The assigned technician notices the OS is several versions out of date. Which would mean the device is restricted from updating due to a corporate security policy is the incorrect answer. As the technician knows the company's policies.

upvoted 1 times

  **fiela1** 1 year, 5 months ago

Surely if there was not enough free space the user would have a notification saying this?

upvoted 1 times

Question #149

Topic 1

A technician receives a ticket indicating the user cannot resolve external web pages. However, specific IP addresses are working. Which of the following does the technician MOST likely need to change on the workstation to resolve the issue?

- A. Default gateway
- B. Host address
- C. Name server
- D. Subnet mask

Correct Answer: C

  **Mehsotopes** Highly Voted  1 year, 1 month ago

Selected Answer: C

Name server is a DNS record that contains other DNS records, this being corrupted would cause you to be unable to connect to other websites. We know Subnet Mask and Host Address works because IP addresses are functional.

Your Default Gateway is your TCP/IP router address that links the host's subnet to other networks, when a host attempts to communicate with another device using TCP/IP, it performs comparison processing using desired subnet mask & destination host IP address versus it's own subnet mask and IP address, result tells computer whether destination is a local host, or a remote host.

For good information on how Subnet Masks and Host addresses work:

<https://www.youtube.com/watch?v=eHV1aOnu7oM>



upvoted 6 times

  **ConfigNique** Most Recent  1 year, 3 months ago

Selected Answer: C

Name Server

upvoted 1 times

  **kevgjo** 1 year, 5 months ago

Anybody can explain this one?

upvoted 2 times

  **deverser** 1 year, 5 months ago

DNS (Domain Name Server) is not resolving. DNS turns an IP address into a name. Since IP addresses are working but typing in a url isn't it has to be the Name Server.

upvoted 2 times

  **deverser** 1 year, 5 months ago

System* not server.

upvoted 2 times

  **DerekM** 1 year, 4 months ago

When a user enters a website name or URL into a web browser, the computer sends a request to a DNS server to resolve the domain name into an IP address that the computer can use to connect to the server hosting the website. This process is called DNS resolution.

If a user can access specific IP addresses but cannot resolve external web pages, it could indicate a problem with the DNS server settings on the user's workstation. The DNS server settings on the workstation could be incorrect or pointing to an invalid DNS server.

In this scenario, the technician would need to change the name server settings on the workstation to point to a valid DNS server that can correctly resolve domain names into IP addresses. The default gateway, host address, and subnet mask settings are not typically related to DNS resolution and would not resolve the issue of not being able to resolve external web pages.

upvoted 7 times

An administrator has received approval for a change request for an upcoming server deployment. Which of the following steps should be completed NEXT?

- A. Perform a risk analysis.
- B. Implement the deployment.
- C. Verify end user acceptance.
- D. Document the lessons learned.

Correct Answer: B

  **glenpharmd** Highly Voted  1 year, 2 months ago

Look at the order of change management phases. C= END USER ACCEPTANCE.

1. Request forms
2. Purpose of change
3. Scope of the change
4. Date and Time of the change
5. Affective systems/ impact
6. Risk analysis
7. Change board approval
8. Finally end user acceptance.

upvoted 25 times

  **Fannan** Highly Voted  1 year ago

Selected Answer: C

7. Change board approval
8. Finally end user acceptance.

upvoted 13 times

  **b27480c** Most Recent  2 months, 2 weeks ago

Selected Answer: C

Cannot implement without end user acceptance.
Upon approval the final step is end user acceptance so the answer is C.

upvoted 1 times

  **Sleezyglizzy** 3 months, 2 weeks ago

Selected Answer: C

based on glenpharmd, ,makes sense.



upvoted 1 times

  **Mr_Tension** 5 months, 1 week ago

Selected Answer: C

1. Request forms
2. Purpose of change
3. Scope of the change
4. Date and Time of the change
5. Affective systems/ impact
6. Risk analysis
7. Change board approval
8. Finally end user acceptance.


upvoted 1 times

  **jsmthy** 5 months, 2 weeks ago

Selected Answer: B

When will you implement your changes? Seriously starting to think some sysadmins never implement anything and just schedule meetings.

upvoted 1 times

  **yutface** 5 months, 1 week ago

HAHA, exactly. "Implement the deployment" is not one the steps. What?...

upvoted 1 times

  **Avengers_inc** 5 months, 2 weeks ago

POV: Dont bother asking Chat GPT because you will be further confused! 😂 It said the next step is to perform risk analysis, so what exactly was the board approving in the first place?? 😂 😂

upvoted 2 times

  **newbytechy** 6 months, 1 week ago

I think it's B. Now I know the change management phases and I dislike that Implementing isn't include in the order but it's just "implied" but this is word from word from Professor Messer.

"Once you receive this approval, the administrative part of the change control process is over, and now you have to actually implement the change. And one of the last steps of the change control process is having the end users confirm that the change was successful."

<https://www.professormesser.com/free-a-plus-training/220-1102/220-1102-video/change-management-220-1102/#>


upvoted 3 times

  **RyeBread** 7 months ago

Selected Answer: B

How do you get end user acceptance if you haven't implemented the change? End user acceptance is confirming the change was successful. You cannot determine if it was successful unless you implement it. I am going with B. Implement the change.

upvoted 3 times

  **yutface** 7 months, 1 week ago

Weird as it is, Implement the change is actually NOT one of the official steps. Very strange that it is not a step - but it isn't.

upvoted 1 times

  **Chavozamiri** 9 months, 1 week ago

Selected Answer: C

8. Finally end user acceptance.

upvoted 1 times

  **Mozzy83** 10 months ago

Selected Answer: B

I watched the professor's video again and he says the next step after board approval is to implement the change. It makes sense to me that you would have to implement the change before any end user acceptance can happen. I say B.

upvoted 3 times

  **CaptainCJ** 10 months, 1 week ago

Selected Answer: C

1. Request forms
2. Purpose of change
3. Scope of the change
4. Date and Time of the change
5. Affective systems/ impact
6. Risk analysis
7. Change board approval
8. Finally end-user acceptance



upvoted 1 times

  **Nater6969** 10 months, 2 weeks ago

Selected Answer: C

Definitely C

upvoted 1 times

  **ropea** 11 months, 3 weeks ago

You wouldn't need end user acceptance if no changes happened.

so you need changes to happen right? so you implement the changes

upvoted 3 times

  **Andylove** 11 months, 3 weeks ago

Selected Answer: B

The next step after receiving approval for a change request for an upcoming server deployment is to implement the deployment. So the answer is (B).

The other options are important steps in the deployment process, but they should be completed in the following order:

Perform a risk analysis: This should be done before the deployment to identify and assess any potential risks.

Implement the deployment: This is the step where the server is actually deployed.

Verify end user acceptance: This should be done after the deployment to ensure that the server is working as expected and meeting the needs of the end users.

Document the lessons learned: This should be done after the deployment to capture any knowledge gained during the process that can be used to improve future deployments.

upvoted 2 times

  **Iddio** 12 months ago

"Once you receive this approval, the administrative part of the change control process is over, AND NOW YOU HAVE TO ACTUALLY IMPLEMENT THE CHANGE. And one of the last steps of the change control process is having the end user confirm that the change was successful." - Professor Messer

So the next step is implement the deployment.

Answer - B

upvoted 3 times

A user calls the help desk to report that Windows installed updates on a laptop and rebooted overnight. When the laptop started up again, the touchpad was no longer working. The technician thinks the software that controls the touchpad might be the issue. Which of the following tools should the technician use to make adjustments?

- A. eventvwr.msc
- B. perfmon.msc
- C. gpedit.msc
- D. devmgmt.msc



Correct Answer: D

  **Alizade** 1 year, 3 months ago

Selected Answer: D

To make adjustments to the software that controls the touchpad on a laptop after Windows installed updates and the touchpad stopped working, the technician should use:

D. devmgmt.msc (Device Manager).
upvoted 3 times

  **kevgjo** 1 year, 5 months ago

this correct?
upvoted 2 times

  **nonzerocrowd** 1 year, 4 months ago

yes, device manager is where you find the hardware drivers.
upvoted 5 times

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

Correct Answer: A

  **carl0gima** Highly Voted  1 year, 4 months ago

Selected Answer: A

A because it say what shoud be done FIRST, so power off the pc, remove LAN card, then perform antivirus scan
upvoted 7 times

  **Yomijohnson** Most Recent  11 months, 1 week ago

This question is just about what to be done after confirming virus on the laptop,. Next step is to quarantine the system by taking it out of the network which will be best done in this provided answer options as shutting down the system
upvoted 1 times

  **oatmealturkey** 1 year, 5 months ago

Selected Answer: C

The question is saying that the ransomware itself cannot be quarantined within the system; there is no reason you can't disconnect the system from the network. Remove the LAN card.
upvoted 1 times

  **deverser** 1 year, 5 months ago

Power off the pc FIRST, then remove the LAN card, no?
upvoted 6 times

  **oatmealturkey** 1 year, 4 months ago

Good point!! You're right
upvoted 4 times

A technician has been tasked with troubleshooting audiovisual issues in a conference room. The meeting presenters are unable to play a video with sound. The following error is received:

The Audio Driver is not running.

Which of the following will MOST likely resolve the issue?



- A. compmgmt.msc
- B. regedit.exe
- C. explorer.exe
- D. taskmgr.exe
- E. gpmsc.msc
- F. services.msc

Correct Answer: F

  **Mehsotopes** 1 year, 1 month ago

Selected Answer: F

Windows Audio most likely crashed. You can find that exact service under the Services Management tab (services.msc).
upvoted 1 times

  **mr_reyes** 1 year, 3 months ago

Selected Answer: F

F. services.msc

The most likely solution to resolve the audio driver error received in the conference room would be to restart the audio-related services on the computer. This can be done using the Services console (services.msc).
upvoted 1 times

  **Crezzki** 1 year, 4 months ago

Selected Answer: F

The error message "The Audio Driver is not running" suggests that the audio driver on the computer may have stopped working or failed to start. Therefore, the most likely solution to resolve the issue is to check the status of the audio driver and restart it if necessary.

The best tool to use for this task is the "Services" management console (services.msc) which allows you to manage and control system services, including the audio driver. Therefore, the correct answer is F. services.msc.

Using the Services management console, the technician can check if the audio driver service is running, and if not, restart it.

- Chat GPT

upvoted 2 times

  **carl0gima** 1 year, 4 months ago


Selected Answer: F

In this scenario Windows Audio Service would be responsible for audio issues if it were stopped. So F services.msc
upvoted 1 times

  **lordcheekklappur** 1 year, 5 months ago

can someone please explain

upvoted 2 times

  **kevgjo** 1 year, 4 months ago

yeah same

upvoted 1 times

  **Tonielo** 11 months, 1 week ago

KKK JJJ PPP

upvoted 1 times

  **nonzerocrowd** 1 year, 4 months ago

<https://softwarekeep.com/help-center/how-to-fix-the-audio-services-not-responding-error-in-windows-10>

upvoted 2 times

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

Correct Answer: A

  **Hoshi1215** Highly Voted  1 year, 5 months ago

To edit the Path Environment Variable, the technician can follow these steps:

1. Open the Control Panel and select the "System" utility.
2. Click on the "Advanced system settings" link.
3. In the System Properties window, click on the "Environment Variables" button.
4. Under "System Variables," scroll down and select the "Path" variable, and click the "Edit" button.
5. Add the new directory where the application executables are located, and click "OK" to save the changes.

Source from ChatGPT

upvoted 9 times

  **LePecador** 1 year, 2 months ago

I tested it in my computer and it's correct

Answer: A) System

upvoted 3 times

  **Rixon** Most Recent  2 weeks, 2 days ago

Selected Answer: A

Windows 11: System > About > Advanced system settings > Environment variables

Windows 10: Same but start in Control Panel



upvoted 1 times

  **sam3210** 7 months ago

Selected Answer: A

System (Option A): The System utility in the Control Panel allows access to various system-related settings, including the Environment Variables. To add an application to the Path Environment Variable, the technician can navigate to "Advanced system settings" and then click on the "Environment Variables" button.

upvoted 4 times

  **Raffaello** 8 months, 4 weeks ago

Selected Answer: A

The PATH is the system variable that your operating system uses to locate needed executables from the command line or Terminal window. The PATH system variable can be set using System Utility in control panel on Windows, or in your shell's startup file on Linux and Solaris.

upvoted 2 times

  **lordcheekklappur** 1 year, 5 months ago

can someone please explain this?

upvoted 3 times

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

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

Correct Answer: A

  **saraperales** 3 weeks, 3 days ago

Selected Answer: A

it's A

upvoted 1 times

  **b27480c** 2 months, 2 weeks ago

Selected Answer: A

This question is designed specifically so the answer can be Power User. "Least Access"

upvoted 1 times

  **Julio_T** 3 months, 1 week ago

Selected Answer: A

It's in the exam objectives. What else is a power user, if not this description?

Admin > Power User > Standard User..... plus bruh it's in the objectives

upvoted 1 times

  **Mamad66** 5 months ago

Selected Answer: A

The user will need a A. Power user account. In a Windows environment, a Power User account is a type of user account that has more permissions than a standard user account but fewer than an Administrator account.

upvoted 1 times

  **Mr_Tension** 5 months, 1 week ago

Selected Answer: A



just imagine, if the user need don't need access to advanced features & configuration ,which account you gonna create for him? guest account? of course not. we will create a simple standard account for that user. but in given scenario when the user need access to some advanced features & configuration, we have to crate a power user account. power user account holder has more power to some specific features and configuration than a standard user but less power compare to an administrator account. hope it's clear now.

upvoted 1 times

  **jsmthy** 5 months, 2 weeks ago

Power user accounts haven't been really relevant in Windows since Windows 7. Just use a Standard account unless your org doesn't mind a user-space Administrator account and expects the user computer to detonate (meaning a user-space backup tool would be a good idea.)

upvoted 1 times

  **hafiz871111** 6 months ago

require the least administrative control. Answer is A.


upvoted 2 times

  **newbytechy** 6 months, 1 week ago

I'm leaning towards A. Power User.

My reasoning is, a power user uses advanced features of computer hardware, operating systems, programs, or websites which are not used by the average user. Since an average user falls under a standard account that eliminates B. Guest accounts are temporary so that eliminates C. And lastly the questions basically implies the user will have access to features and configuration settings for "several" applications not ALL applications which eliminates Administrative Account since that account has Access to make changes to the FULL system.

upvoted 1 times

  **aqeras** 9 months, 1 week ago

Selected Answer: B

standard

upvoted 1 times

Andylove 11 months, 3 weeks ago

Selected Answer: B

B. Standard account

A standard user account provides restricted access compared to an administrator account but allows users to use most software and make some system changes that don't affect the overall system configuration. It's a suitable choice for users who need to perform advanced tasks within the boundaries of their applications but should not have full control over the system's settings or security.

upvoted 2 times

glenpharmd 1 year ago

Given that the user needs to access advanced features and configuration settings for several applications, but also considering the need for a least privilege environment, the best choice here would be:

ANSWER= Standard account

upvoted 2 times

Mehsotopes 1 year, 1 month ago

Selected Answer: A

You can make a user account & put it under the Power Users group in Windows 10 & 11 Pro. Access this setting by going to Local Users and Groups (lusrmgr.msc). You can give the created user account access to advanced features & configuration settings for applications (to read, write, execute & modify) while eliminating access to mess with the Command Line Interface (CLI).

upvoted 2 times

dcv1337 1 year, 1 month ago

Selected Answer: B

A standard account provides the user with the necessary access to use most software and change system settings that do not affect other users or the security of the computer. If the user needs to perform tasks that require administrative privileges, such as accessing advanced features and configuration settings for several applications, they can do so by providing the credentials of an administrator account when prompted by User Account Control (UAC).

upvoted 1 times

RoPsur 1 year, 2 months ago

Selected Answer: B

It's either standard user or admin account for this one as the guest account should be disabled and power user is deprecated due to privilege escalation issues. The scenario presented indicates the user will not need access to everything an administrator has access to, and for that reason, I pick Standard User. Sure you could make the user part of a group with proper permissions.

upvoted 1 times

DerekM 1 year, 4 months ago

Selected Answer: B

Based on the information provided, the user will need access to advanced features and configuration settings for several applications. However, corporate policy requires a least privilege environment. Therefore, the BEST account access level for the user would be a Standard account.

A Standard account provides a basic level of permissions to the user, allowing them to run applications and perform tasks that do not require administrative privileges. This helps to minimize the risk of unauthorized changes to the system and protects against malicious software.

upvoted 2 times

Thunder_Cat 1 year, 4 months ago

Selected Answer: D

It doesn't mention legacy applications, so it's not a power user.

upvoted 1 times

Crezzki 1 year, 4 months ago

Selected Answer: D

The user will need an account with administrative access level. While corporate policy requires a least privilege environment, some applications and advanced configuration settings may require administrative access to function properly. However, it is recommended to limit administrative access to only the necessary tasks and revoke the access when it is no longer needed to maintain security.

-ChatGPT

upvoted 1 times

A technician downloads a validated security tool and notes the vendor hash of a11e11a1. When the download is complete, the technician again validates the hash, but the value returns as 2a222a2b2. 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

Correct Answer: C

  **DerekM** Highly Voted  1 year, 4 months ago

Selected Answer: C

Based on the information provided, the most likely cause of the issue is a modified file. The fact that the hash value has changed from the expected value suggests that the file has been modified in some way. This could be due to a number of factors, such as a virus or malware infecting the file, or the file being intercepted and modified during transmission.

upvoted 7 times

  **TacosInMyBelly** Most Recent  10 months, 4 weeks ago

Selected Answer: C

If you modify a file the hash will change representing changes done to that file.

upvoted 1 times

A company needs to securely dispose of data stored on optical discs. Which of the following is the MOST effective method to accomplish this task?

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

Correct Answer: D



  **ScorpionNet** Highly Voted  1 year, 4 months ago

Selected Answer: D

D is correct because optical disks can be shredded when the disk is no longer needed. Degaussing only applies to the HDD.
upvoted 6 times

  **Pythagorean** Most Recent  1 year, 3 months ago

low-level formatting since its data disposal
upvoted 1 times

  **kevgjo** 1 year, 5 months ago

wouldn't this be degaussing since its an optical disk?
upvoted 1 times

  **Thunder_Cat** 1 year, 4 months ago

an optical disk is a CD/DVD.
upvoted 3 times

  **Hoshi1215** 1 year, 5 months ago

I go with D.
Degaussing is a method used to erase data from magnetic media, such as hard drives. So it is not effective for optical discs.
upvoted 2 times

  **ScorpionNet** 1 year ago

No, because unlike HDDs, optical disks are not magnetic. So shredding it would work, breaking in half can work too.
upvoted 2 times

  **oatmealturkey** 1 year, 5 months ago

Degaussing does not work on optical disks.
upvoted 3 times

A mobile phone user has downloaded a new payment application that allows payments to be made with a mobile device. The user attempts to use the device at a payment terminal but is unable to do so successfully. The user contacts a help desk technician to report the issue. Which of the following should the technician confirm NEXT as part of the troubleshooting process?

- A. If airplane mode is enabled
- B. If Bluetooth is disabled
- C. If NFC is enabled
- D. If Wi-Fi is enabled
- E. If location services are disabled

Correct Answer: C

[-]  **Bioka** Highly Voted 1 year, 4 months ago

NFC(New File Communicaton) is the right answer.

method of wireless data transfer that allows smartphones, laptops, tablets and other devices to share data when in close proximity. NFC technology powers contactless payments via mobile wallets like Apple Pay and Google Pay, as well as contactless cards.

upvoted 6 times

[-]  **brewersmurf** 1 year, 3 months ago


Near Field Communication (NFC)

upvoted 7 times

[-]  **Rixon** Most Recent 2 weeks, 2 days ago

How would you verify if NFC is enabled?

upvoted 1 times

[-]  **Sunree** 7 months, 2 weeks ago

Selected Answer: C

Near Field Communication (NFC)

upvoted 1 times

A Chief Executive Officer has learned that an exploit has been identified on the web server software, and a patch is not available yet. Which of the following attacks MOST likely occurred?

- A. Brute force
- B. Zero day
- C. Denial of service
- D. On-path

Correct Answer: B

  **S5Networking** Highly Voted  1 year, 5 months ago

More like zero bitches... ahhh I'm failing this exam
upvoted 27 times

  **Hogslayer** 10 months, 3 weeks ago

Let me know if you passes lol
upvoted 2 times

  **DerekM** 1 year, 3 months ago

I needed this.
upvoted 6 times

  **jacob2125** Most Recent  5 months, 2 weeks ago

Which attack most likely occurred? It doesn't say any attack occurred, just that it is vulnerable to an attack. Who tf writes these questions?
upvoted 2 times

  **Tochukwu424** 6 months, 2 weeks ago

The CEO's situation most likely involves a Zero day attack.
upvoted 1 times

  **Raffaello** 9 months ago

Selected Answer: B

A zero-day (0day) exploit is a cyber attack targeting a software vulnerability which is unknown to the software vendor or to antivirus vendors. The attacker spots the software vulnerability before any parties interested in mitigating it, quickly creates an exploit, and uses it for an attack.
upvoted 3 times

  **dcv1337** 1 year, 1 month ago

Selected Answer: B

A zero-day attack exploits a vulnerability in software that is unknown to the vendor and for which no patch is available yet. This is a SY0-601 question.
upvoted 2 times

  **lordcheekklappur** 1 year, 4 months ago

Based on the information provided, it is not possible to determine which specific attack occurred. However, the situation described suggests that the web server may be vulnerable to a zero-day exploit, which is a type of attack that targets a previously unknown vulnerability in software before a patch or fix is available.

A zero-day exploit can be extremely dangerous because it can be used by attackers to gain unauthorized access to a system or steal sensitive information without being detected. When a vulnerability is discovered, software vendors typically work to create and release a patch or update to address the issue. However, in some cases, a patch may not be available for some time, leaving the system vulnerable to attack.

source chat GPT 3.5

upvoted 2 times

  **lordcheekklappur** 1 year, 5 months ago

can someone explain?
upvoted 1 times

A user has a license for an application that is in use on a personal home laptop. The user approaches a systems administrator about using the same license on multiple computers on the corporate network. Which of the following BEST describes what the systems administrator should tell the user?

- A. Use the application only on the home laptop because it contains the initial license.
- B. Use the application at home and contact the vendor regarding a corporate license.
- C. Use the application on any computer since the user has a license.
- D. Use the application only on corporate computers.

Correct Answer: B

  **lordcheekklappur** Highly Voted  1 year, 4 months ago

It is generally not appropriate to use a personal license for an application on multiple computers in a corporate network without confirming the terms of the license agreement. Each software vendor has different licensing terms and conditions, and using the same license on multiple machines may not be allowed. Additionally, the corporate network may have its own software requirements and policies that need to be followed.

Option B suggests the most appropriate course of action. The user should continue using the application on their personal home laptop, which is already licensed, and then contact the software vendor to inquire about the proper licensing for use on the corporate network. By doing this, the user ensures compliance with the software's licensing terms and the company's policies, avoiding potential legal issues or violation of corporate guidelines.

Source Chat GPT

upvoted 7 times

  **sam3210** Most Recent  7 months ago

Selected Answer: B

Typically, a license for software is valid for a specific number of installations or users. If a user has a license for personal use on their home laptop, they should adhere to the terms of the license agreement. In this case, it's important for the user to use the application only on the home laptop as per the initial license terms.

If the user wants to use the application on multiple computers on the corporate network, they should contact the vendor to inquire about obtaining a corporate license that allows for such usage. Using the application on corporate computers without the appropriate licensing could violate the terms of the license agreement and may result in legal and compliance issues.

upvoted 2 times

A technician needs to interconnect two offices to the main branch while complying with good practices and security standards. Which of the following should the technician implement?

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

Correct Answer: C

  **DerekM** Highly Voted  1 year, 4 months ago

Selected Answer: C

To interconnect two offices to the main branch while complying with good practices and security standards, the technician should implement a VPN (Virtual Private Network).

A VPN is a secure and encrypted connection between two networks or devices, which provides a secure tunnel through which data can be transmitted. This ensures that data is protected from interception and tampering by unauthorized third parties.

upvoted 5 times

A user receives a notification indicating the data plan on the user's corporate phone has reached its limit. The user has also noted the performance of the phone is abnormally slow. A technician discovers a third-party GPS application was installed on the phone. Which of the following is the MOST likely cause?

- A. The GPS application is installing software updates.
- B. The GPS application contains malware.
- C. The GPS application is updating its geospatial map data.
- D. The GPS application is conflicting with the built-in GPS.

Correct Answer: D

  **oatmealturkey** Highly Voted 1 year, 4 months ago

Selected Answer: B

This question was on my exam and I did not get anything wrong in this objective, so B is the right answer.
upvoted 19 times

  **crazymonkeh** 6 months ago

This individual doesn't seem to understand the grading scheme of the Comptia A+ exam.

The grading scale goes up to 900 for full marks. There's only 70-90 questions per core tests (My Core 1 had 70). Don't tell me you honestly believe every correct answer is worth 10+ marks each? If that was the case, why didn't they just grade it from 0%-100% instead of an odd scale to 900?

It works like this:

The test questions have a "Most Correct" answer, a "semi-correct" answer, a "Mostly Wrong" and a "Completely Wrong" answer.

I don't know the exact numbers, but a completely wrong answer would likely give you 0 pts. Mostly wrong would probably be around 3 pts, semi correct around half marks, and fully correct would grant full marks. (Don't quote me on this, I don't know the exact mechanics)

My point is, just because you didn't get the question wrong, doesn't mean it was completely correct either.

upvoted 2 times

  **MikeNg98** 1 year, 4 months ago

Man I trusted you since you already took the exam and got this one right lol

upvoted 7 times

  **kekejon** 9 months ago

this guy wrote this for like 90% of these questions. Even though he is right sometimes I would watch out

upvoted 7 times

  **Mr_Tension** Most Recent 5 months, 1 week ago

I don't trust chatgpt but here he got a point.

"The GPS application is updating its geospatial map data," is a plausible explanation for increased data usage, but it's less likely to directly cause the abnormal slowdown of the phone. While updating map data could indeed consume data from the user's data plan, it typically shouldn't significantly impact the performance of the device unless the update process is particularly resource-intensive. However, in most cases, map data updates occur in the background and are designed to minimize disruption to the user's experience.

upvoted 2 times

  **Mr_Tension** 5 months, 1 week ago

On the other hand, malware is known to consume data in the background, potentially leading to both increased data usage and degraded performance as it may be performing additional malicious activities beyond data consumption. Given the combination of symptoms described—reaching the data plan limit, abnormal slow performance, and the presence of a third-party GPS application—the presence of malware is a more likely explanation for the observed issues. Therefore, option B, "The GPS application contains malware," is the most probable cause.

upvoted 1 times

  **crazymonkeh** 6 months ago

Selected Answer: C

Shouldn't the answer be C?

Updating Geographical data constantly on a GPS whether it's 3rd part or not, takes up a colossal amount of cellular Data.

As for running slow, depending on how much resources the app is using, it could cause overheating, thus slowing down the performance.

upvoted 2 times

  **Footieprogrammer** 1 year ago

Selected Answer: B

B is the most logical answer here, dataplan is used up AND the device is slow

upvoted 2 times

  **Mehsotopes** 1 year, 1 month ago

Two GPS software programs conflicting with each other might cause an increase in data usage.

upvoted 1 times

  **Mehsotopes** 1 year, 1 month ago

Selected Answer: D

Test says GPS application is conflicting with the built-in GPS application, considering this is causing phone's performance to be slow, most would consider this malware.



upvoted 1 times

  **dcv1337** 1 year, 1 month ago

Selected Answer: B

The most likely cause of the data plan reaching its limit and the phone's performance being abnormally slow is that the third-party GPS application contains malware. Malware is malicious software that can harm the device or steal data. In this case, the malware may be using the phone's data connection to transmit data, causing the data plan to reach its limit. It may also be using the phone's resources, causing it to slow down.

upvoted 2 times

  **racononice12** 1 year, 4 months ago

Selected Answer: B

its B guys.

upvoted 2 times

  **DerekM** 1 year, 4 months ago

Selected Answer: B

Based on the information provided, the MOST likely cause of the slow performance and data usage on the user's corporate phone is that the third-party GPS application installed on the phone contains malware.

Malware is a type of malicious software that is designed to cause harm to a device or network. Malware can be installed on a device through a variety of methods, such as downloading and installing an infected application or clicking on a malicious link. Once installed, malware can use up system resources and data usage, as well as cause the device to slow down or crash.

upvoted 3 times

  **1337Minty** 1 year, 5 months ago

Selected Answer: C

The answer is def C.

upvoted 2 times

  **oatmealturkey** 1 year, 5 months ago

Sum total of third-party application + used up all of user's data + device is abnormally slow = malware is most likely issue



upvoted 4 times

  **Joshuaau** 1 year, 5 months ago

Selected Answer: C

If the GPS keeps refreshing, it will use more data than a GPS app that does not

upvoted 2 times

  **kevgjo** 1 year, 5 months ago

I think it could be A

upvoted 1 times

A technician needs to document who had possession of evidence at every step of the process. Which of the following does this process describe?

- A. Rights management
- B. Audit trail
- C. Chain of custody
- D. Data integrity

Correct Answer: C

  **Sunree** 7 months, 2 weeks ago

Selected Answer: C

Chain of custody
upvoted 1 times

  **Footieprogrammer** 1 year ago

Selected Answer: C

Chain of custody describes who has possessed the unit previously
upvoted 1 times

A malicious file was executed automatically when a flash drive was plugged in. Which of the following features would prevent this type of incident?

- A. Disabling UAC
- B. Restricting local administrators
- C. Enabling UPnP
- D. Turning off AutoPlay

Correct Answer: A



  **LayinCable** Highly Voted  1 year, 5 months ago

Selected Answer: D

UAC most definitely NEEDS TO STAY ON. This is exactly what UAC is for, therefore making this a WRONG answer.

The correct answer is D. As turning off autoplay wont allow any kind of external objects, LIKE USB DRIVES, to run or install any kind of software or codes that could purposely or accidentally harm a computer or network.

upvoted 20 times

  **Bioka** 1 year, 4 months ago

Sure, you are right.

upvoted 1 times

  **Philco** Most Recent  2 days, 10 hours ago

Selected Answer: D

Disable AutoRun

Disabling AutoRun prevents programs from automatically executing when a USB device is connected

upvoted 1 times

  **crazymonkeh** 6 months ago

Selected Answer: D

LMAO disabling User Account Control, wouldn't that make things worse?!

The answer is obviously D: Disabling Autoplay for external devices.

upvoted 1 times

  **ddholla** 1 year ago

Please someone explain to me why A is the "correct" answer

upvoted 1 times

  **sillylilguy** 8 months, 3 weeks ago

I read from another user that this website will sometimes mark incorrect answers to avoid copyright or like test leakage. Using the discussion it beneficial for questions like these

upvoted 1 times

  **dcv1337** 1 year, 1 month ago

Selected Answer: D

Turning off AutoPlay would prevent this type of incident from occurring. AutoPlay is a feature in Windows that automatically runs a program or opens a file when a removable media device, such as a flash drive, is inserted into the computer. If a malicious file is present on the flash drive, it could be executed automatically when the drive is plugged in. By turning off AutoPlay, the user will have to manually open the flash drive and choose which files to run, preventing the automatic execution of any malicious files.



upvoted 2 times

  **lordcheekklappur** 1 year, 4 months ago

AutoPlay is a feature in Windows that automatically launches applications or opens files when a removable device, like a flash drive, is connected to the computer. If a malicious file is present on the flash drive, AutoPlay could potentially execute it without any user intervention, leading to a security breach.

Turning off AutoPlay helps prevent this type of incident by requiring users to manually open or execute files on the flash drive. Without AutoPlay, the malicious file will not be executed automatically upon plugging in the flash drive, reducing the risk of infection. Users can then scan the flash drive with antivirus software before accessing any files, further improving security.

upvoted 3 times

  **1337Minty** 1 year, 5 months ago

Selected Answer: D

Answer is def D.
upvoted 1 times

Question #165

Topic 1

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

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

Correct Answer: D

  **Mehsotopes** **Highly Voted**  1 year, 1 month ago

Selected Answer: D

In order to analyze risks, you need to test methods in a sandbox environment.
upvoted 5 times

  **racononice12** **Most Recent**  1 year, 4 months ago

Is this correct?
upvoted 4 times

  **NadirM_18** 1 year, 3 months ago

Yes it is
upvoted 4 times

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.

Correct Answer: C

  **EddyNL** Highly Voted 1 year, 5 months ago

Selected Answer: B

it is B

upvoted 7 times

  **ScorpionNet** Highly Voted 1 year, 5 months ago

Selected Answer: B

B is correct

upvoted 5 times

  **yutface** Most Recent 5 months, 3 weeks ago


Another useless question. You can literally hit the windows key and type "wallpaper" and it takes you there.

upvoted 3 times

  **max12553** 1 week, 3 days ago

And yet navigation is apart of CompTIA test. Be careful what you regard as useless. Test will bite you.

upvoted 1 times

  **Raffaello** 8 months, 4 weeks ago

Selected Answer: B

Select Start > Settings > Personalization. The preview window gives you a sneak peek of your changes as you make them. In Background, you can select a picture or solid color, or create a slideshow of pictures

upvoted 1 times

  **Footieprogrammer** 1 year ago

Selected Answer: B

B definately, try it.

upvoted 2 times

  **HQvRuss** 1 year ago

Selected Answer: B

B is the correct answer

upvoted 2 times

  **Mehsotopes** 1 year, 1 month ago

Test says display, but that don't make sense, it's under Personalization.

upvoted 1 times

  **dcv1337** 1 year, 1 month ago

Selected Answer: B

To change the desktop wallpaper using a Windows 10 Settings tool, the user should open Settings, select Personalization, then select Background. From there, the user can choose a picture from the list of available images or click Browse to locate and open an image from their computer to use as the wallpaper.

upvoted 2 times

  **Promagane** 1 year, 2 months ago

Selected Answer: B

B is the correct answer

upvoted 2 times

  **Calebdames** 1 year, 4 months ago

Selected Answer: B

B is correct b33947e.

upvoted 4 times

  **LayinCable** 1 year, 5 months ago

Selected Answer: B

It is most definitely B. Not C.

upvoted 4 times

  **[Removed]** 1 year, 5 months ago

Select Start > Settings > Personalization. The preview window gives you a sneak peek of your changes as you make them. In Background, you can select a picture or solid color, or create a slideshow of pictures.

upvoted 3 times

Question #167

Topic 1

A macOS user needs to create another virtual desktop space. Which of the following applications will allow the user to accomplish this task?

- A. Dock
- B. Spotlight
- C. Mission Control
- D. Launchpad

Correct Answer: C

  **kekejon** 9 months ago

C , Mission Control is a macOS feature that allows you to view all open windows on a single interface on your Mac. The feature is great if you're bad at keeping your windows organized and find yourself losing things all of the time. Be aware that if you have minimized a window, then it won't show up in Mission Control.


upvoted 1 times

  **DonnieDuckoe** 1 year, 4 months ago

Selected Answer: C

C actually is correct on this one.

upvoted 4 times

  **loki33** 10 months, 2 weeks ago



thanks

upvoted 1 times

A user lost a company tablet that was used for customer intake at a doctor's office. Which of the following actions would BEST protect against unauthorized access of the data?


- A. Changing the office's Wi-Fi SSID and password
- B. Performing a remote wipe on the device
- C. Changing the user's password
- D. Enabling remote drive encryption

Correct Answer: B

  **6809276** 6 months, 3 weeks ago

Selected Answer: B

remote wipe is in Professor Messer study guide.
upvoted 1 times

  **FT786** 11 months, 3 weeks ago

B. Performing a remote wipe on the device

The best action to protect against unauthorized access to the data on the lost company tablet is to perform a remote wipe on the device. This action will erase all data and settings on the tablet, rendering it useless to anyone who finds it. Changing the office's Wi-Fi SSID and password, changing the user's password, and enabling remote drive encryption are important security measures, but they won't completely protect the data on the lost tablet. Remote wiping is specifically designed to address situations like this and is the most effective way to ensure that sensitive data doesn't fall into the wrong hands.

upvoted 3 times

A desktop engineer is deploying a master image. Which of the following should the desktop engineer consider when building the master image? (Choose two.)

- A. Device drivers
- B. Keyboard backlight settings
- C. Installed application license keys
- D. Display orientation
- E. Target device power supply
- F. Disabling express charging

Correct Answer: AE

AyeGodly Highly Voted 1 year, 5 months ago

Selected Answer: AC

"A & C" make the most sense
upvoted 12 times

FT786 Most Recent 11 months, 3 weeks ago

A & C

A. Device drivers: Ensuring that the necessary device drivers are included in the master image is crucial for compatibility and proper functioning of hardware components on target devices.

C. Installed application license keys: If the master image includes licensed software applications, it's important to manage and document license keys or activations to ensure compliance and prevent issues with software licensing on the target devices.

The other options (B, D, E, F) are not typically critical considerations when building a master image, as they are more related to individual device settings and power management, which can usually be configured after deploying the master image to target devices.

upvoted 2 times

Footieprogrammer 1 year ago

Selected Answer: AC

it's AC
upvoted 1 times

HQvRusss 1 year ago

Selected Answer: AC

A AND C is the correct answer
upvoted 2 times

Mehsotopes 1 year, 1 month ago

Selected Answer: AE

Depending on the use of the computers running off of this Golden/Master image, you would want to make sure they have the correct power output for the intended use for both the drives and processing units.

To create a Master Image (Golden Image, Ghost Image, or Base Image), an administrator first sets up the computing environment with the exact specifications needed & then saves the disk image as a pattern for future copies & use. It is a template for a virtualized computing system.

upvoted 1 times

dcv1337 1 year, 1 month ago

Selected Answer: AC

Device drivers are software components that enable the operating system to communicate with hardware devices. The master image should include the appropriate device drivers for the target hardware to ensure that all devices function properly after deployment.

Installed application license keys are used to activate licensed software. If the master image includes licensed software, the desktop engineer should ensure that the appropriate license keys are included in the image and that the licensing terms allow for deployment on multiple devices.

upvoted 1 times

rah555 1 year, 4 months ago

Selected Answer: AC

A. Device drivers: The master image should contain all the necessary device drivers for the hardware components that will be used on the target devices. This ensures that the devices function properly and optimally.

C. Installed application license keys: If the master image includes any licensed software, the license keys should be either excluded from the image

or activated before deploying the image to the target devices. This prevents license key conflicts and ensures that the licensed software is properly activated on each device.

upvoted 4 times

  **electro1989** 1 year, 5 months ago

yes The right answer should be A and C

upvoted 3 times

Question #170

Topic 1

A technician installed an application on a user's desktop and received an error message. Which of the following tools can the technician use to research the error?

- A. Resource Monitor > CPU > Services
- B. Task Manager > Processes > Apps
- C. Event Viewer > Windows Logs > Application
- D. Device Manager > Computer

Correct Answer: C

  **lordcheekklappur** Highly Voted  1 year, 4 months ago

Selected Answer: C

C. Event Viewer > Windows Logs > Application

upvoted 7 times

  **Raffaello** Most Recent  8 months, 4 weeks ago

Selected Answer: C

Use Event Viewer to Troubleshoot System Freezes

To open Event Viewer, click Start > Run and then type eventvwr

After Event Viewer opens, in the left-hand column, click Windows Logs > Application. ...

On the right-hand side, click Filter and then check the boxes for Critical, Warning, and Error.

upvoted 1 times

  **Raffaello** 9 months ago

Selected Answer: C

How to identify the cause of the Player or Editor crashing?



Click the Windows Start button.

Search for Event Viewer and open it.

Click Windows Logs and click Application.

Find the error you are looking for and check the Date and Time, Source, Event ID, etc.

upvoted 1 times

  **FT786** 11 months, 3 weeks ago

C. Event Viewer > Windows Logs > Application

upvoted 1 times

A technician is configuring a new Windows laptop. Corporate policy requires that mobile devices make use of full disk encryption at all times. Which of the following encryption solutions should the technician choose?

- A. Encrypting File System
- B. File Vault
- C. BitLocker
- D. Encrypted LVM

Correct Answer: C



  **RyeBread** 7 months ago

Selected Answer: C

Since it specifically says a Windows laptop, the answer I would think is best is Bitlocker which is proprietary to Microsoft.
upvoted 1 times



  **Aa_Min_a** 8 months, 3 weeks ago

BitLocker To Go, is BitLocker Drive Encryption on removable data drives
upvoted 1 times

  **mohdAj** 9 months, 3 weeks ago

Selected Answer: C

FDE is especially useful for desktops, laptops and mobile devices that can be physically lost or stolen. FDE is often installed on computing devices at the time of manufacturing. For example, FDE is enabled through features like BitLocker, which is included in certain Microsoft Windows versions or FileVault, which is built into the macOS.
upvoted 1 times

  **FT786** 11 months, 3 weeks ago

C. BitLocker

BitLocker is a full disk encryption solution provided by Microsoft for Windows operating systems.

The other options mentioned (A. Encrypting File System, B. File Vault, D. Encrypted LVM) are encryption solutions, but they do not provide full disk encryption at the same level as BitLocker on Windows systems.
upvoted 2 times

  **kevij** 11 months, 3 weeks ago

A. Encrypting File System
upvoted 1 times

  **Ily5031** 12 months ago

It's A
upvoted 2 times

A small business owner wants to install newly purchased software on all networked PCs. The network is not configured as a domain, and the owner wants to use the easiest method possible. Which of the following is the MOST efficient way for the owner to install the application?

- A. Use a network share to share the installation files.
- B. Save software to an external hard drive to install.
- C. Create an imaging USB for each PC.
- D. Install the software from the vendor's website.

Correct Answer: A

  **Raffaello** 9 months ago

Selected Answer: A

File sharing is the public or private sharing of files or folders on a computer connected to a network. Files can easily be shared outside a network via removable media, but the term file sharing almost always refers to sharing files on a network. File sharing allows several people to use the same file data

upvoted 1 times

  **DerekM** 1 year, 4 months ago

Selected Answer: A

Option A is the correct answer. Using a network share allows the owner to copy the installation files to a central location on the network, from which all networked PCs can access them. The owner can then run the installation on each PC by simply navigating to the shared folder and double-clicking on the setup file. This method avoids the need to copy the installation files to each PC or create an imaging USB for each PC, which would be more time-consuming.

upvoted 2 times

  **oatmealturkey** 1 year, 4 months ago

Selected Answer: A

This question was on my exam and I did not get anything wrong in this objective, so A is the right answer.

upvoted 4 times

  **Mr_Tension** 5 months, 1 week ago

I'm wondering if you pass actually not . because I can , you just telling the same thing in everywhere

upvoted 1 times

  **rah555** 1 year, 4 months ago

Selected Answer: A

Using a network share to share the installation files allows the owner to install the software on all networked PCs simultaneously. This eliminates the need to manually install the software on each individual PC, saving time and effort.

upvoted 2 times

  **lordcheekklappur** 1 year, 4 months ago

Using a network share to share the installation files is the most efficient way for the small business owner to install the newly purchased software on all networked PCs without a domain configuration. By creating a network share, the owner can place the software's installation files in a centralized location that is accessible to all PCs on the network.

upvoted 1 times

  **2FkinBored** 1 year, 5 months ago

Selected Answer: D



It's not a domain environment so I don't see how it can be A. C wouldn't be the most efficient. B would take more steps than D.

upvoted 1 times

  **BinMcGrin** 1 year, 4 months ago

It doesn't have to be a domain environment to use a network share. It can be a workgroup environment, which is probably what you have at home. Think about sharing a folder or printer between two laptops running Windows Home on your home network - that is a network share without use of a domain.

upvoted 4 times

  **kevgjo** 1 year, 5 months ago

Selected Answer: C

Would this be C?

upvoted 1 times

A user reports that text on the screen is too small. The user would like to make the text larger and easier to see. Which of the following is the BEST way for the user to increase the size of text, applications, and other items using the Windows 10 Settings tool?

- A. Open Settings, select Devices, select Display, and change the display resolution to a lower resolution option.
- B. Open Settings, select System, select Display, and change the display resolution to a lower resolution option.
- C. Open Settings, select System, select Display, and change the Scale and layout setting to a higher percentage.
- D. Open Settings, select Personalization, select Display, and change the Scale and layout setting to a higher percentage.

Correct Answer: C

Wiz_tech101 Highly Voted 1 year, 4 months ago

Selected Answer: C

C. Open Settings, select System, select Display, and change the Scale and layout setting to a higher percentage.

By following these steps will take exactly to the display settings and increase the scale to a higher percentage will increase the size of the text, apps and other items

upvoted 8 times

Raffaello Most Recent 8 months, 4 weeks ago

Selected Answer: C

Open Start, select Settings > System > Display.

Under Scale and layout, check the setting under Change the size of text, apps, and other items. We suggest you use the percentage marked "(Recommended)."

If that doesn't solve your problem, under Resolution, select a new value

upvoted 1 times

ph12 1 year, 2 months ago

C is correct

upvoted 1 times

tepek 1 year, 3 months ago

Selected Answer: C

It is C

upvoted 2 times

DerekM 1 year, 4 months ago

Selected Answer: D

D. Open Settings, select Personalization, select Display, and change the Scale and layout setting to a higher percentage.

upvoted 2 times

DMC71 1 year, 2 months ago

You dont personalise it so its c .

upvoted 2 times

A user is being directed by the help desk to look up a Windows PC's network name so the help desk can use a remote administration tool to assist the user. Which of the following commands would allow the user to give the technician the correct information? (Choose two.)


- A. ipconfig /all
- B. hostname
- C. netstat /?
- D. nslookup localhost
- E. arp -a
- F. ping ::1

Correct Answer: AB

  **EddyNL** Highly Voted 1 year, 5 months ago

Selected Answer: AB

Tried it. A and B.
upvoted 7 times

  **kevgjo** 1 year, 5 months ago


what about nslookup
upvoted 1 times

  **DerekM** 1 year, 4 months ago

nslookup in cmd did not provide the information needed by just that command. AB did.
upvoted 2 times


  **6809276** Most Recent 6 months, 3 weeks ago

This question was on the exam words for words
upvoted 3 times



  **6809276** 6 months, 3 weeks ago

Selected Answer: AB

I got this exact same worded questions on the actual exam.
upvoted 2 times

  **yutface** 7 months, 1 week ago

How about just >whoami
upvoted 1 times



  **Raffaello** 8 months, 4 weeks ago

Selected Answer: AB

ipconfig /all: Displays detailed information about all adapters, including the IP address, subnet mask, default gateway, DHCP server, and DNS servers.

A hostname is a unique label assigned to a device connected to a computer network. It serves as a human-readable identifier for that device, allowing you to easily distinguish it from other devices on the network. You can think of it as the name of your computer or other network-enabled devices

upvoted 1 times

  **FT786** 11 months, 3 weeks ago

The commands that would provide the network name of the Windows PC are:

A. ipconfig /all: This command provides detailed information about the network configuration of the computer, including the hostname, which is the network name of the PC.

B. hostname: This command directly displays the hostname (the network name) of the PC.

Both of these commands will provide the necessary information for the user to provide the network name to the help desk for remote assistance.
upvoted 3 times

  **orsopdx** 1 year, 3 months ago

what do we think of B & E, ChatGPT:

The two commands that would allow the user to give the technician the correct information for a Windows PC's network name are:

- B. hostname
- E. arp -a