FC0-U51.exam.145q

Number: FC0-U51
Passing Score: 800
Time Limit: 120 min

FC0-U51

CompTIA IT Fundamentals Certification Exam

Sections
1. Software
2. Hardware
3. Security
4. Networking
5. Basic IT Literacy
6. Mix Questions

Exam A

QUESTION 1
Which of the following is considered an optical storage medium?

A. SSD
B. Blu-Ray
C. Flash drive
D. Memory card

Correct Answer: B
Section: Hardware
Explanation

Explanation/Reference:

QUESTION 2
Which of the following are examples of keyboard connectors? (Select TWO).

A. USB
B. RJ-11
C. Serial
D. FireWire
E. PS/2

Correct Answer: AE
Section: Hardware
Explanation

Explanation/Reference:

QUESTION 3
Which of the following is the function of a CPU?

A. Encrypts data for remote transmission
B. Performs data computation
C. Supplies electricity to components
D. Provides storage location for files

Correct Answer: B
Section: Hardware
Explanation

Explanation/Reference:

QUESTION 4
Several users want to share a common folder with high availability. Which of the following devices is BEST to use for this requirement?

A. Large USB flash drive connected to a PC
B. Medium capacity SATA hard drive
C. Network attached storage appliance
D. Firewall with security management

Correct Answer: C
Section: Hardware
Explanation

Explanation/Reference:

QUESTION 5
Which of the following is a 15-pin video connection?

A. DVI
B. S-video
C. Component
D. HDMI
E. VGA

Correct Answer: E
Section: Hardware
Explanation

Explanation/Reference:

QUESTION 6
Which of the following are considered input devices for a computer? (Select TWO).

A. Mouse
B. Printer
C. Speakers
D. Microphone
E. Monitor

Correct Answer: AD
Section: Hardware
Explanation

Explanation/Reference:

QUESTION 7
Which of the following is required to have a multimedia conversation with someone across the Internet? (Select THREE).

A. Network connection
B. Microphone
C. Modem
D. Firewall
E. Webcam
F. Cable connection
G. Wired NIC

Correct Answer: ABE
Section: Hardware
Explanation

Explanation/Reference:

QUESTION 8
Which of the following components is required to send faxes via POTS?

A. NIC
B. Power supply
C. Modem
D. Wireless adapter

Correct Answer: C
Section: Hardware
Explanation

Explanation/Reference:

QUESTION 9
A technician sets up a new computer system and connects the keyboard and mouse to the PS/2 ports. When the computer boots, the BIOS gives a keyboard and mouse error. Both devices are connected. Which of the following is the solution?

A. Swap the mouse and keyboard to the other PS/2 ports.
B. Remap the mouse and keyboard in the BIOS.
C. Update the BIOS to recognize the newer keyboard and mouse.
D. Configure the keyboard localization settings.

Correct Answer: A
Section: Hardware
Explanation

Explanation/Reference:

QUESTION 10
A user is browsing the Internet when suddenly a threatening message appears on screen demanding a payment in order to avoid the system being disabled. Which of the following BEST describes this type of malware infection?

A. Ransomware
B. Adware
C. Spyware
D. Virus

Correct Answer: A
Section: Security
Explanation

Explanation/Reference:

QUESTION 11
Which of the following is an example of ransomware?

A. A user is asked to pay a fee for a password to unlock access to their files.
B. A user receives an email demanding payment for a trial application that has stopped working.
C. A user has opened an Internet browser and is taken to a site that is not the normal home page.
D. A user is asked to open an attachment that verifies the price of an item that was not ordered.

Correct Answer: A
Section: Security
Explanation

Explanation/Reference:

QUESTION 12
An employee, Joe, forgot his laptop at the airport. Joe is worried about unauthorized access. Which of the following BEST protects against data theft in this instance?

A. Security software
B. Full disk encryption
C. Cable lock
D. Username and password
E. Patching the OS and third party software

Correct Answer: B
Section: Security
Explanation

Explanation/Reference:

QUESTION 13
Multiple laptops that contain confidential data are stolen from a company. Which of the following is a likely policy change resulting from this incident?

A. Enabling full disk encryption
B. Requiring screensaver password
C. Disabling Bluetooth adapters
D. Adding multifactor authentication

Correct Answer: A
Section: Security
Explanation

Explanation/Reference:

QUESTION 14
A user receives an email formatted to appear as if the bank sent it. The email explains that the user must confirm the name, address, and social security number listed on the bank account. Which of the following BEST describes the security threat taking place?

A. Shoulder surfing
B. Social engineering
C. Spam
D. Phishing

Correct Answer: D

Section: Security
Explanation

Explanation/Reference:

QUESTION 15
A user, Ann, is concerned about theft of her laptop and does not want a thief to have easy access to all of her banking and email. Which of the following precautions could be taken to mitigate this issue?

A. Only browse the Internet on WiFi connections that use WPA2
B. Turn off the guest account in the operating system
C. Disable autofill functionality within the web browser
D. Remove any legacy browsers from the computer

Correct Answer: C
Section: Security
Explanation

Explanation/Reference:

QUESTION 16
A user is configuring a new wireless router. Which of the following should be done to ensure that unauthorized changes cannot be made?

A. Change the SSID
B. Change the router's address
C. Change the administrator password
D. Change the encryption key

Correct Answer: C
Section: Security
Explanation

Explanation/Reference:

QUESTION 17
Which of the following would BEST be described as password best practices? (Select THREE).

A. Use of long passwords
B. Sharing passwords with a trusted source
C. Limiting password reuse
D. Keeping default passwords
E. Use of special characters
F. Writing down difficult passwords

Correct Answer: ACE
Section: Security
Explanation

Explanation/Reference:

QUESTION 18

A user, Ann, receives a call asking for her password to troubleshoot a problem. Which of the following describes this type of security threat?

A. Malware
B. Social engineering
C. Spam
D. Physical security

Correct Answer: B
Section: Security
Explanation

Explanation/Reference:

QUESTION 19
Malware that has an embedded keylogger to capture all of the keystrokes and steal logins is considered:

A. adware
B. spyware
C. ransomware
D. phishing

Correct Answer: B
Section: Security
Explanation

Explanation/Reference:

QUESTION 20
Which of the following security threats occurs when a user receives an email from an illegitimate source asking for login information?

A. Hacking
B. Phishing
C. Spam
D. Cracking

Correct Answer: B
Section: Security
Explanation

Explanation/Reference:

QUESTION 21
Which of the following are best practices when it comes to using a computer in a public location? (Select TWO).

A. Notify the administrator when finished.
B. Use strong passwords.
C. Turn off the computer when finished.
D. Disable the save password function on web pages.
E. Make sure to clean the keyboard when finished.

F. Make sure to log out of websites when done.

Correct Answer: DF
Section: Security
Explanation

Explanation/Reference:

QUESTION 22
Joe, a user, wishes to allow his roommate to access his personal computer for Internet browsing, but does not want his roommate to have the ability to make changes to the system. Which of the following BEST describes the type of account Joe should create for his roommate?

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

Correct Answer: B
Section: Security
Explanation

Explanation/Reference:

QUESTION 23
A user is configuring a SOHO wireless router. The user should change the router's default administrator password for which of the following reasons?

A. To prevent improper data transmission encryption
B. To prevent unauthorized configuration changes
C. To prevent social engineering attacks
D. To increase wireless signal strength

Correct Answer: B
Section: Security
Explanation

Explanation/Reference:

QUESTION 24
Ann, a user, is doing her daily job on her company laptop at a coffee shop. She opens an Internet browser and tries to go to her home page. Instead, she is sent to an unfamiliar website. She clears all temporary files and deletes the history, but this continues to occur. Which of the following is the cause of the problem?

A. The company has configured a policy on her computer that forces her to stay on their website.
B. Her computer is infected with adware and is redirecting her browser to another site.
C. The memory of the browser is corrupt, and she needs to have the browser reinstalled.
D. She did not reboot her computer after clearing the temporary files.

Correct Answer: B
Section: Security
Explanation

Explanation/Reference:

QUESTION 25
An attacker cracks a user's password for all social media, email, and bank accounts. The user needs to change the passwords for all these accounts. Which of the following should the user do in the future to prevent this from happening?

A. Disable unused browser toolbars.
B. Clear the browser cache.
C. Avoid credential reuse.
D. Delete tracking cookies.

Correct Answer: C
Section: Security
Explanation

Explanation/Reference:

QUESTION 26
While browsing the Internet, a user receives a warning regarding the display of mixed content. The address bar includes https, and the lock symbol is showing. Which of the following does this warning indicate about the website?

A. It stores data in cache or cookies, but not both.
B. It requires login credentials for some sections.
C. It contains both secure and non-secure parts.
D. It is best viewed with a different browser.

Correct Answer: C
Section: Security
Explanation

Explanation/Reference:

QUESTION 27
A technician is typing the password to logon to a system. A user is standing in close proximity to the technician and is able to see the password being typed. Which of the following BEST describes this situation?

A. Dumpster diving
B. Shoulder surfing
C. Phishing
D. Social engineering

Correct Answer: B
Section: Security
Explanation

Explanation/Reference:

QUESTION 28
Joe, a user, has just installed his first home wireless router. Which of the following tasks should be considered to help secure the unit from any confirmed exploits?

A. Change the router administrator username.
B. Change the router's broadcasting channel.
C. Update the unit's firmware.
D. Use a complex administrator password.

Correct Answer: C
Section: Networking
Explanation

Explanation/Reference:

QUESTION 29
Which of the following is the BEST security practice to use when configuring the management options of a wireless router?

A. Disable DHCP
B. Change the admin password
C. Enable SSID
D. Enable remote administration

Correct Answer: B
Section: Networking
Explanation

Explanation/Reference:

QUESTION 30
When operating under optimal network conditions, which of the following has the HIGHEST reliability?

A. Bluetooth
B. Wired
C. Cellular
D. WiFi

Correct Answer: B
Section: Networking
Explanation

Explanation/Reference:

QUESTION 31
A user needs to download tax documents from a financial website. Which of the following is the website MOST likely to use for transmission of the tax document to the user's browser?

A. HTTP
B. HTTPS
C. SFTP
D. FTP

Correct Answer: B
Section: Networking
Explanation