

# CompTIA

## Exam Questions FC0-U61

CompTIA IT Fundamentals+ Certification Exam



#### NEW QUESTION 1

A programmer needs an element that will automatically store customer orders consecutively by order number every time a new order is placed. Which of the following elements should be used?

- A. Vector
- B. Sequence
- C. Array
- D. Constant

**Answer:** B

#### Explanation:

A sequence is an element that will automatically store customer orders consecutively by order number every time a new order is placed. A sequence is a database object that generates sequential numbers according to a specified rule. A sequence can be used to create unique identifiers for records in a table, such as order numbers or customer IDs. A vector is an element that can store multiple values of the same data type in an ordered sequence, but it does not automatically generate sequential numbers. A vector is a data structure that can be used in programming languages such as C++ or Java. An array is an element that can store multiple values of the same data type in an indexed sequence, but it does not automatically generate sequential numbers. An array is a data structure that can be used in programming languages such as C or Python. A constant is an element that can store a single value of any data type that does not change during the execution of a program, but it does not automatically generate sequential numbers. A constant is a variable that can be used in programming languages such as C# or JavaScript. References: The Official CompTIA IT Fundamentals (ITF+) Student Guide (Exam FC0-U61), Chapter 6: Database Fundamentals, Chapter 8: Software Development Concepts

#### NEW QUESTION 2

Which of the following actions is the FINAL step in the standard troubleshooting methodology?

- A. Document the solution and cause.
- B. Create a new theory of cause.
- C. Research the problem online.
- D. Implement preventive measures.

**Answer:** A

#### Explanation:

The final step in the standard troubleshooting methodology is to document the solution and cause of the problem. This step involves recording the details of the problem, the steps taken to resolve it, the outcome of the solution, and any preventive measures implemented to avoid future occurrences. Documenting the solution and cause can help to create a knowledge base for future reference, improve communication among IT professionals, and facilitate continuous improvement<sup>12</sup>. References:= CompTIA IT Fundamentals (ITF+) Study Guide, 2nd Edition, Chapter 7: Explain the Troubleshooting Methodology<sup>3</sup>; Troubleshooting Methodology | IT Support and Help Desk | CompTIA<sup>4</sup>

#### NEW QUESTION 3

For which of the following is a relational database management system MOST commonly used?

- A. Building flowcharts
- B. Storing information
- C. Generating reports
- D. Creating diagrams

**Answer:** B

#### Explanation:

A relational database management system (RDBMS) is most commonly used for storing information in a structured and organized way. A RDBMS stores data in tables, which consist of rows and columns. Each row represents a record or an entity, and each column represents an attribute or a property of the entity. A RDBMS allows users to create, update, delete, and query data using a standard language called SQL (Structured Query Language). A RDBMS also enforces rules and constraints to ensure data integrity and consistency<sup>3465</sup>.

References:= CompTIA IT Fundamentals (ITF+) Study Guide, 2nd Edition, Chapter 5: Database Fundamentals<sup>2</sup>; What is RDBMS (Relational Database Management System) - Javatpoint<sup>5</sup>; What is a Relational Database Management System? | Microsoft Azure

#### NEW QUESTION 4

Which of the following intellectual property concepts BEST represents a legally protected slogan of a business?

- A. Contract
- B. Patent
- C. Copyright
- D. Trademark

**Answer:** D

#### Explanation:

A trademark is a type of intellectual property that protects a word, phrase, symbol, or design that identifies and distinguishes the source of goods or services of one party from those of others. A slogan of a business is an example of a trademark that can be legally protected from unauthorized use by other parties. A trademark can be registered with the appropriate authority to obtain exclusive rights and benefits. References : The Official CompTIA IT Fundamentals (ITF+) Study Guide (FC0-U61), page 211.

#### NEW QUESTION 5

An online retailer experienced an outage. An investigation revealed that the server received more requests than it could handle, and customers could not log in as a result. Which of the following best describes this scenario?

- A. Hardware failure
- B. Denial of service
- C. On-path attack
- D. Social engineering

**Answer: B**

**Explanation:**

The scenario where an online retailer experienced an outage because the server received more requests than it could handle and customers could not log in as a result is best described as a denial of service. A denial of service is a type of attack that aims to disrupt or prevent the normal functioning or availability of a system or network by overwhelming it with excessive traffic or requests. A denial of service can cause performance degradation, slowdown, or outage for the system or network and its legitimate users. A denial of service can be performed by a single attacker or a group of attackers using multiple compromised devices, which is called a distributed denial of service (DDoS). A hardware failure is not the scenario that describes the online retailer's outage, but rather a possible cause or consequence of the outage. A hardware failure is a malfunction or breakdown of a physical component of a system or network, such as a disk, a memory, a CPU, a power supply, etc. A hardware failure can cause data loss, corruption, or interruption for the system or network and its users. A hardware failure can be caused by various factors, such as wear and tear, physical damage, overheating, power surge, etc. A hardware failure can also be induced by a denial of service attack that damages the hardware by overloading it. An on-path attack is not the scenario that describes the online retailer's outage, but rather a type of network attack that involves intercepting or modifying data packets that are transmitted between two parties on a network. An on-path attack can compromise the confidentiality, integrity, or authenticity of the data or communication between the parties. An on-path attack can be performed by an attacker who has access to the same network segment or device as one of the parties, such as a router, a switch, or a hub. An on-path attack can also be performed by an attacker who tricks one of the parties into sending data to them instead of the intended destination, which is called a man-in-the-middle attack. A social engineering attack is not the scenario that describes the online retailer's outage, but rather a type of attack that exploits human psychology and behavior to manipulate people into performing actions or revealing information that benefits the attacker. A social engineering attack can take various forms, such as phishing, vishing, baiting, quid pro quo, pretexting, or tailgating. References: The Official CompTIA IT Fundamentals (ITF+) Student Guide (Exam FC0-U61), Chapter 7: Security Concepts

**NEW QUESTION 6**

Employees of a large technology company are provided access to the internet as a work resource. Which of the following most likely represents the level of privacy employees should expect when utilizing this resource?

- A. Only the attempts to access unapproved URLs are logged.
- B. All internet usage is logged by a corporate server and may be monitored live.
- C. All internet browsing is private and anonymous.
- D. Only the attempts to access sites that include prohibited keywords are logged.

**Answer: B**

**NEW QUESTION 7**

Which of the following would be the best reason to implement a host firewall?

- A. To prevent external access
- B. To prevent hardware failures
- C. To prevent the removal of software
- D. To prevent wiretapping

**Answer: A**

**Explanation:**

A host firewall is a software program that runs on a computer or device and monitors and controls the incoming and outgoing network traffic based on predefined rules. A host firewall can help prevent external access from unauthorized or malicious sources, such as hackers, malware, or network worms. A host firewall can also block unwanted or unnecessary traffic from reaching the computer or device, which can improve performance and security. A host firewall can be configured to allow or deny traffic based on various criteria, such as port number, protocol, application, source address, destination address, or content. A host firewall can also log or alert the user about any suspicious or blocked activity.

**NEW QUESTION 8**

An administrator grants permission for a user to access data in a database. Which of the following actions was performed?

- A. Data correlation
- B. Data manipulation
- C. Data gathering
- D. Data definition

**Answer: D**

**Explanation:**

Data definition is the process of creating, modifying, or deleting the structure and objects of a database, such as tables, fields, indexes, and views. Data definition is performed using data definition language (DDL), which is a subset of SQL commands. An administrator can use DDL to grant or revoke permissions for a user to access data in a database. References : The Official CompTIA IT Fundamentals (ITF+) Study Guide (FC0-U61), page 144.

**NEW QUESTION 9**

Which of the following relational database constructs is used to ensure valid values are entered for a column?

- A. Schema
- B. Permissions
- C. Constraint
- D. Column

**Answer: C**

**Explanation:**

A constraint is a rule or a restriction that is applied to a column or a table in a relational database to ensure that only valid values are entered. Constraints help to maintain the integrity, accuracy, and consistency of the data. For example, a constraint can be used to specify that a column must not contain null values, or that a column must contain unique values, or that a column must match a value in another table<sup>12</sup>. References: = CompTIA IT Fundamentals (ITF+) Study Guide, 2nd Edition, Chapter 5: Database Fundamentals<sup>3</sup>; Constraints in Relational Database Model - Online Tutorials Library

**NEW QUESTION 10**

A technician overhears a systems administrator mention the term “IOPS”. To which of the following operating system functions would the term BEST apply?

- A. Disk management
- B. Process management
- C. Application management
- D. Service management

**Answer:** A

**Explanation:**

IOPS (Input/Output Operations Per Second) is a term that refers to the performance of a storage device or system. It measures how many read and write operations can be performed by the storage device or system in one second. IOPS would best apply to the operating system function of disk management, which involves managing how data is stored, accessed, and organized on disks. Process management, application management, and service management are not operating system functions that directly relate to IOPS. References: CompTIA IT Fundamentals+ Study Guide: Exam FC0-U61, Second Edition, Chapter 4: Programming Concepts and Data Structures, page 158.

**NEW QUESTION 10**

A systems administrator is setting up a new server using RAID technology. If one hard drive in the array fails, the data is stored on another drive, preventing data loss. Which of the following business continuity concepts does this explain?

- A. File backup
- B. Data restoration
- C. Fault tolerance
- D. Restoring access

**Answer:** C

**Explanation:**

Fault tolerance is the ability of a system to continue functioning even when one or more components fail. RAID (Redundant Array of Independent Disks) is a technology that uses multiple hard drives to store data in a way that improves performance and reliability. If one hard drive in the RAID array fails, the data can be recovered from another drive without losing any information. This is an example of fault tolerance.

References: CompTIA IT Fundamentals+ Study Guide: Exam FC0-U61, Second Edition, Chapter 6: Infrastructure Concepts, page 240.

**NEW QUESTION 11**

Which of the following database structures is the most granular?

- A. Column
- B. Field
- C. Record
- D. Table

**Answer:** B

**Explanation:**

A field is the most granular database structure among the options given. A field is a single unit of data that represents an attribute of an entity, such as name, age, or address. A field can have a specific data type, such as text, number, or date. A column is a collection of fields that share the same data type and name, such as the name column in a table. A record is a collection of fields that represent an instance of an entity, such as a person, a product, or an order. A record can be identified by a primary key, which is a unique value for each record. A table is a collection of records that represent the same type of entity, such as the customer table or the product table. References: CompTIA IT Fundamentals (ITF+) Study Guide: Exam FC0-U61, Second Edition, Chapter 5: Database Fundamentals and Security Concepts, page 156

**NEW QUESTION 12**

All users have access to an application at a company. The data from the application is stored on a centralized device located on the network. Which of the following devices would MOST likely be used to store the data?

- A. Server
- B. Tape library
- C. External HDD
- D. Workstation

**Answer:** A

**Explanation:**

A server is a device that provides services and resources to other devices on a network. A server can store data from an application and allow multiple users to access it simultaneously. A server is different from a tape library, an external HDD, or a workstation, which are devices that store data locally or offline and do not provide network services. References: The Official CompTIA IT Fundamentals (ITF+) Student Guide (Exam FC0-U61), Chapter 4, Section 4.1, Page 152.

**NEW QUESTION 13**

A user is trying to set up a new wireless access point. Which of the following should the user do first?

- A. Change the SSID to a unique name.
- B. Change the default password.
- C. Enable WPA2 encryption.
- D. Enable the highest available wireless standard.

**Answer:** B

**Explanation:**

A wireless access point (WAP) is a device that allows wireless devices to connect to a wired network using Wi-Fi or Bluetooth. A WAP usually has a default configuration that is set by the manufacturer, which may include a default password, SSID (service set identifier), encryption type, and wireless standard. The default password is often weak or well-known, which makes the WAP vulnerable to unauthorized access or hacking. Therefore, the first thing that a user should do when setting up a new WAP is to change the default password to a strong and unique one. This will help secure the WAP and prevent unwanted changes or attacks. Changing the SSID to a unique name, enabling WPA2 encryption, and enabling the highest available wireless standard are also important steps to improve the security and performance of the WAP, but they should be done after changing the default password.

**NEW QUESTION 17**

When editing a document, which of the following describes where the changes are located before they are saved to permanent storage?

- A. SSD
- B. CPU
- C. RAM
- D. GPU

**Answer:** C

**Explanation:**

RAM stands for Random Access Memory, which is where the changes are located before they are saved to permanent storage when editing a document. RAM is a type of volatile memory that stores data temporarily while the computer is running. RAM allows fast access and modification of data by the CPU, but it loses its contents when the power is turned off. SSD stands for Solid State Drive, which is a type of permanent storage that stores data persistently even when the power is turned off. SSD uses flash memory chips to store data, which offer faster performance and lower power consumption than traditional hard disk drives (HDDs). CPU stands for Central Processing Unit, which is the main component of a computer that executes instructions and performs calculations. CPU does not store data, but it uses registers and cache memory to hold data temporarily during processing. GPU stands for Graphics Processing Unit, which is a specialized component of a computer that handles graphics and image processing. GPU does not store data, but it uses dedicated memory to hold graphics data temporarily during rendering. References: The Official CompTIA IT Fundamentals (ITF+) Student Guide (Exam FC0-U61), Chapter 1: IT Fundamentals

**NEW QUESTION 21**

Which of the following would MOST likely prevent malware sent as compromised file via email from infecting a person's computer?

- A. Email previewing
- B. Patching
- C. Clear browsing cache
- D. Kill process

**Answer:** B

**Explanation:**

Patching would be the most likely way to prevent malware sent as a compromised file via email from infecting a person's computer. Patching is the process of applying updates or fixes to software or hardware to improve performance, security, or functionality. Patching can help prevent malware infections by closing the vulnerabilities or flaws that malware exploits to infect systems. Users should regularly patch their operating systems, applications, and antivirus software to protect their computers from malware attacks. References : The Official CompTIA IT Fundamentals (ITF+) Study Guide (FC0-U61), page 202.

**NEW QUESTION 24**

A systems administrator wants to return results for a time range within a database. Which of the following commands should the administrator use?

- A. SELECT
- B. INSERT
- C. DELETE
- D. UPDATE

**Answer:** A

**Explanation:**

A SELECT command is a SQL (Structured Query Language) statement that is used to return results for a time range within a database. A SELECT command can specify the columns and rows to be retrieved from one or more tables based on certain criteria or conditions. A SELECT command can also use functions or operators to manipulate or filter the data. For example, a SELECT command can use the BETWEEN operator to specify a time range for a date column<sup>89</sup>. References:= CompTIA IT Fundamentals (ITF+) Study Guide, 2nd Edition, Chapter 5: Database Fundamentals<sup>3</sup>; SQL SELECT Statement - W3Schools<sup>10</sup>

**NEW QUESTION 26**

Which of the following tasks is typically performed during the identification phase of the troubleshooting methodology?

- A. QUESTION NO: users.
- B. Verify functionality.
- C. Divide and conquer.
- D. Implement the solution.

**Answer:** A

**Explanation:**



users is a task that is typically performed during the identification phase of the troubleshooting methodology. QUESTION NO: users involves gathering information from the users who are experiencing the problem or who have reported the problem. This can help identify the symptoms, scope, frequency, and impact of the problem. Verify functionality, divide and conquer, and implement the solution are tasks that are typically performed in other phases of the troubleshooting methodology. References: CompTIA IT Fundamentals+ Study Guide: Exam FC0-U61, Second Edition, Chapter 9: Troubleshooting Methodology, page 333.

**NEW QUESTION 31**

A company will begin to allow staff to work from home by means of formal request. Which of the following is the BEST way for the company to document this change?

- A. Written procedure
- B. Written policy
- C. Written email
- D. Written memo

**Answer: B**

**Explanation:**

A written policy is the best way for a company to document a change that allows staff to work from home by means of formal request. A policy is a statement or guideline that defines the rules, standards, or procedures for an organization's actions, decisions, or behaviors. A policy can help an organization to achieve its objectives, comply with regulations, ensure consistency and quality, and communicate expectations and responsibilities. A written policy is a policy that is documented in a formal document that can be distributed, reviewed, updated, and enforced by the organization. A written policy can help a company to document a change that affects its staff, such as working from home, by specifying the criteria, process, benefits, limitations, and consequences of the change. References : The Official CompTIA IT Fundamentals (ITF+) Study Guide (FC0-U61), page 210.

**NEW QUESTION 34**

Which of the following would be the easiest component to upgrade on a laptop that is experiencing slow performance?

- A. Motherboard
- B. GPU
- C. RAM
- D. CPU

**Answer: C**

**Explanation:**

The easiest component to upgrade on a laptop that is experiencing slow performance is RAM. RAM stands for Random Access Memory, which is a type of volatile memory that stores data temporarily while the computer is running. RAM allows fast access and modification of data by the CPU, but it loses its contents when the power is turned off. Upgrading RAM can improve the performance of a laptop by increasing the amount of data that can be stored and processed at the same time, reducing the need for swapping or paging to the hard disk. Upgrading RAM on a laptop is usually easy, as it only requires opening a small panel on the back or side of the laptop and inserting or replacing the RAM modules into the slots. The motherboard is not the easiest component to upgrade on a laptop that is experiencing slow performance, but rather one of the most difficult components to upgrade. The motherboard is the main circuit board of a computer that connects and controls all the other components, such as the CPU, RAM, GPU, etc. Upgrading the motherboard can improve the performance of a laptop by supporting newer or faster components, but it is also very complex, costly, and risky. Upgrading the motherboard on a laptop may require replacing or reconfiguring many other components, as well as ensuring compatibility and stability with the operating system and drivers. The GPU is not the easiest component to upgrade on a laptop that is experiencing slow performance, but rather one of the most difficult components to upgrade. The GPU stands for Graphics Processing Unit, which is a specialized component of a computer that handles graphics and image processing. Upgrading the GPU can improve the performance of a laptop by increasing the speed and quality of rendering graphics, especially for gaming or video editing applications. However, upgrading the GPU on a laptop is usually very hard or impossible, as most laptops have integrated GPUs that are soldered to the motherboard or CPU and cannot be replaced or upgraded. The CPU is not the easiest component to upgrade on a laptop that is experiencing slow performance, but rather one of the most difficult components to upgrade. The CPU stands for Central Processing Unit, which is the main component of a computer that executes instructions and performs calculations. Upgrading the CPU can improve the performance of a laptop by increasing the speed and efficiency of processing data, especially for multitasking or complex applications. However, upgrading the CPU on a laptop is usually very hard or impossible, as most laptops have integrated CPUs that are soldered to the motherboard and cannot be replaced or upgraded. References: The Official CompTIA IT Fundamentals (ITF+) Student Guide (Exam FC0-U61), Chapter 1: IT Fundamentals

**NEW QUESTION 37**

A technician needs to install a wireless router for a client that supports speeds up to 11Mbps and operates on the 2.4GHz band. Which of the following should the technician select?

- A. 802.11a
- B. 802.11b
- C. 802.11g
- D. 802.11n

**Answer: B**

**Explanation:**

\* 802.11 b is the wireless standard that supports speeds up to 11Mbps and operates on the 2.4GHz band. 802.11b is one of the earliest versions of the IEEE 802.11 family of standards for wireless local area networks (WLANs). 802.11b uses direct-sequence spread spectrum (DSSS) modulation to transmit data over radio waves. 802.11b has a maximum theoretical data rate of 11Mbps and a typical range of up to 150 feet indoors or 300 feet outdoors. 802.11b operates on the same frequency band as some cordless phones, microwaves, and Bluetooth devices, which may cause interference or signal degradation. References : The Official CompTIA IT Fundamentals (ITF+) Study Guide (FC0-U61), page 171.

**NEW QUESTION 40**

Which of the following business continuity concepts is the best example of fault tolerance?

- A. Data restoration
- B. Redundant power
- C. Disaster recovery
- D. Restoring access

**Answer:** B

**Explanation:**

Redundant power is the best example of fault tolerance among the given business continuity concepts. Fault tolerance refers to the ability of a system to continue functioning despite failures or errors in some of its components. Redundant power provides backup sources of electricity in case of power outages or surges, ensuring uninterrupted operation of critical systems. Data restoration refers to the process of recovering lost or corrupted data from backups or other sources. Disaster recovery refers to the plan and procedures for restoring normal business operations after a major disruption, such as a natural disaster or a cyberattack. Restoring access refers to the process of granting users the ability to use systems or resources that were previously unavailable or inaccessible. References: The Official CompTIA IT Fundamentals (ITF+) Student Guide (Exam FC0-U61), Chapter 7: Security Concepts1

**NEW QUESTION 45**

A desktop administrator just connected a printer to a workstation, but the workstation does not recognize the printer. Which of the following does the workstation MOST likely need for the printer to function?

- A. Permission
- B. Ink cartridge
- C. USB cable
- D. Driver

**Answer:** D

**Explanation:**

A driver is a software component that enables a device, such as a printer, to communicate with the operating system of a computer. Without a proper driver, the workstation will not be able to recognize or use the printer. Therefore, the workstation most likely needs a driver for the printer to function. The other options are not relevant to the problem of device recognition.

**NEW QUESTION 46**

A developer is creating specific step-by-step instructions/procedures and conditional statements that will be used by a computer program to solve problems. Which of the following is being developed?

- A. Algorithm
- B. Software
- C. Pseudocode
- D. Flowchart

**Answer:** A

**Explanation:**

An algorithm is a set of specific step-by-step instructions/procedures and conditional statements that will be used by a computer program to solve problems. An algorithm defines the logic and sequence of actions that a computer program must follow to perform a task or achieve a goal. An algorithm can be expressed in various ways, such as pseudocode, flowchart, or natural language. References : The Official CompTIA IT Fundamentals (ITF+) Study Guide (FC0-U61), page 131.

**NEW QUESTION 49**

Which of the following internet service types is most susceptible to weather disruptions?

- A. Cable
- B. Satellite
- C. DSL
- D. Fiber

**Answer:** B

**Explanation:**

Satellite internet service is a type of internet service that uses satellites orbiting the earth to transmit and receive data signals from users' devices. Satellite internet service can provide internet access to remote or rural areas where other types of internet service are not available or reliable. However, satellite internet service is also more susceptible to weather disruptions than other types of internet service, such as cable, DSL (digital subscriber line), or fiber. Weather conditions such as rain, snow, clouds, wind, or storms can interfere with the signal quality and strength between the satellite and the user's device, causing slow speeds, latency (delay), packet loss (data loss), or connection drops. Therefore, satellite internet service users may experience poor or inconsistent internet performance during bad weather

**NEW QUESTION 52**

Which of the following should have the HIGHEST expectation of privacy?

- A. A picture posted to a social media website
- B. A presentation saved to a corporate file server
- C. A locally stored word processing document
- D. A spreadsheet emailed to a business client

**Answer:** C

**Explanation:**

A locally stored word processing document would have the highest expectation of privacy among the given options. Privacy is the right or ability of individuals or groups to control or limit the access or disclosure of their personal information by others. A locally stored word processing document is a file that contains text, images, or other data that is created and saved on a device's internal storage, such as a hard drive or SSD. A locally stored word processing document can have a higher level of privacy than a file that is shared, uploaded, or transmitted over the Internet or a network, because it is less exposed to potential threats or breaches. However, a locally stored word processing document may still require additional security measures, such as encryption, password protection, or backup, to ensure its privacy and integrity. References : The Official CompTIA IT Fundamentals (ITF+) Study Guide (FC0-U61), page 205.

**NEW QUESTION 54**

Which of the following storage types is MOST vulnerable to magnetic damage?

- A. Flash
- B. SSD
- C. Optical
- D. HDD

**Answer:** D

**Explanation:**

HDD (Hard Disk Drive) is a type of storage device that uses magnetic disks to store data. HDD is the most vulnerable to magnetic damage among the options given because magnetic fields can interfere with the read/write heads or the magnetic disks, causing data loss or corruption. Flash, SSD (Solid State Drive), and Optical are not types of storage devices that use magnetic disks to store data. Flash and SSD are types of storage devices that use flash memory chips to store data. Optical is a type of storage device that uses laser beams to read or write data on optical discs, such as CDs, DVDs, or Blu-ray discs. References: CompTIA IT Fundamentals+ Study Guide: Exam FC0-U61, Second Edition, Chapter 3: Computing Components, page 122.

**NEW QUESTION 59**

Which of the following creates multifactor authentication when used with something you have?

- A. Single sign-on
- B. Hardware token
- C. Geolocation
- D. Password

**Answer:** D

**Explanation:**

A password is something you know, which can be used to create multifactor authentication when used with something you have, such as a hardware token or a smart card. Multifactor authentication is a security method that requires two or more factors of authentication to verify a user's identity. Single sign-on is a feature that allows a user to access multiple applications or systems with one set of credentials, but it does not necessarily involve multifactor authentication. Geolocation is a feature that determines a user's physical location based on GPS or other methods, but it does not necessarily involve multifactor authentication. References: The Official CompTIA IT Fundamentals (ITF+) Student Guide (Exam FC0-U61), Chapter 7: Security Concepts

**NEW QUESTION 62**

Which of the following statements BEST describes binary?

- A. A notational system used to represent an "on" or "off" state
- B. A notational system used to represent media access control
- C. A notational system used to represent Internet protocol addressing
- D. A notational system used to represent a storage unit of measurement

**Answer:** A

**Explanation:**

Binary is a notational system used to represent an "on" or "off" state in digital devices or systems. Binary use only two symbols: 0 (off) and 1 (on). Binary is also known as base 2 notation, because each symbol represents a power of 2. Binary is the fundamental building block of all computer operations and data storage, as it can encode any type of information using sequences of bits (binary digits)1112. References  
:= CompTIA IT Fundamentals (ITF+) Study Guide, 2nd Edition, Chapter 2: Computing Basics3; What is Binary? - Definition from Techopedia

**NEW QUESTION 63**

A user is selecting software to use to prepare handouts for a presentation. The user would like the information to be easy to format and printer friendly. Which of the following software types should the user select?

- A. Word processing
- B. Spreadsheet
- C. Text editor
- D. Visual diagramming

**Answer:** A

**Explanation:**

The software type that the user should select to prepare handouts for a presentation that are easy to format and printer friendly is word processing. Word processing is a type of software that allows users to create, edit, format, and print text documents, such as letters, reports, resumes, etc. Word processing software provides features such as fonts, styles, margins, alignment, bullets, numbering, tables, images, etc., that enable users to customize the appearance and layout of their documents. Word processing software also provides features such as spell check, grammar check, word count, etc., that enable users to improve the quality and accuracy of their documents. Word processing software can also support various file formats and printing options that enable users to save and print their documents easily and conveniently. Examples of word processing software include Microsoft Word, Google Docs, LibreOffice Writer, etc. Spreadsheet is not the software type that the user should select to prepare handouts for a presentation that are easy to format and printer friendly, but rather a type of software that allows users to create, edit, format, and print numerical data in rows and columns, such as budgets, invoices, charts, etc. Spreadsheet software provides features such as formulas, functions, graphs, pivot tables, etc., that enable users to perform calculations, analysis, or visualization on their data. Spreadsheet software can also support various file formats and printing options that enable users to save and print their data easily and conveniently. Examples of spreadsheet software include Microsoft Excel, Google Sheets, LibreOffice Calc, etc. Text editor is not the software type that the user should select to prepare handouts for a presentation that are easy to format and printer friendly, but rather a type of software that allows users to create, edit, or view plain text files, such as code, scripts, notes, etc. Text editor software provides features such as syntax highlighting, search and replace, indentation, etc., that enable users to manipulate text easily and efficiently. Text editor software does not provide features such as fonts, styles, images, etc., that enable users to customize the appearance or layout of their documents. Text editor software can also support various file formats but not printing options that enable users to save but not print their files easily and conveniently. Examples of text editor software include Notepad++, Sublime Text, Vim, etc.



**NEW QUESTION 65**

Employee information is stored in a database. Which of the following BEST describes where all of an employee's information is stored?

- A. Record
- B. Report
- C. Column
- D. Procedure

**Answer:** A

**Explanation:**

A record is a collection of related fields or attributes that store information about a specific entity or object in a database. For example, an employee record would store information such as name, ID, department, salary, etc. A record would be the best description of where all of an employee's information is stored in a database. A report is a formatted presentation of data from a database, not a storage unit. A column is a vertical arrangement of fields or attributes that store the same type of information for different records, not all of an employee's information. A procedure is a set of instructions or commands that perform a specific task on a database, not a storage unit. References: CompTIA IT Fundamentals+ Study Guide: Exam FC0-U61, Second Edition, Chapter 5: Database Fundamentals, page 193.

**NEW QUESTION 66**

An IT manager wants to prevent end users from booting alternative operating systems on workstations. Which of the following security-related best practices would be used to accomplish this?

- A. Installing a host-based firewall
- B. Setting a BIOS password
- C. Patching the operating system
- D. Removing unnecessary software

**Answer:** B

**Explanation:**

Setting a BIOS password is a security-related best practice that would prevent end users from booting alternative operating systems on workstations. A BIOS password restricts access to the BIOS settings, which control the boot order and other hardware configurations of the computer. Installing a host-based firewall, patching the operating system, and removing unnecessary software are also security-related best practices, but they do not directly prevent booting alternative operating systems on workstations. References: The Official CompTIA IT Fundamentals (ITF+) Student Guide (Exam FC0-U61), Chapter 7: Security Concepts1

**NEW QUESTION 69**

Which of the following BEST describes a kilobyte?

- A. A kilobyte is a measurement of storage (e.g., 100KB).
- B. A kilobyte is a measurement of throughput (e.g., 100Kbps).
- C. A kilobyte is a measurement of power (e.g., 100KW).
- D. A kilobyte is a measurement of processor speed (e.g., 2.4KHz).

**Answer:** A

**Explanation:**

A kilobyte is a unit of digital information that equals 1,024 bytes. A byte is the smallest unit of data that can be stored or processed by a computer. A kilobyte can store a small amount of text, such as a few sentences or a paragraph. Storage devices, such as hard disks and flash drives, use kilobytes and other larger units, such as megabytes and gigabytes, to measure their capacity and performance. References: The Official CompTIA IT Fundamentals (ITF+) Study Guide (FC0-U61), page 38.

**NEW QUESTION 74**

Which of the following is the exact number of bytes in a gigabyte?

- A. 1,024 bytes
- B. 1,048,576 bytes
- C. 1,073,741,824 bytes
- D. 1,099,511,627,776 bytes

**Answer:** C

**Explanation:**

The exact number of bytes in a gigabyte is 1.073.741.824 bytes. A byte is a unit of digital information that consists of eight bits. A bit is a binary digit that can have one of two values: 0 or 1. A byte can store one character, such as a letter, a number, or a symbol. A gigabyte is a unit of digital information that consists of 1.073.741.824 bytes or 1.024 megabytes. A megabyte is a unit of digital information that consists of 1.048.576 bytes or 1.024 kilobytes. A kilobyte is a unit of digital information that consists of 1.024 bytes. These units are based on the binary system, which uses powers of two to represent values. However, there are also decimal units that use powers of ten to represent values, such as gigabyte (GB), megabyte (MB), and kilobyte (KB). These units are often used by storage devices and network services to measure capacity or speed. In this case, one gigabyte (GB) equals 1 billion bytes or 1.000 megabytes (MB). One megabyte (MB) equals 1 million bytes or 1.000 kilobytes (KB). One kilobyte (KB) equals 1 thousand bytes. References: The Official CompTIA IT Fundamentals (ITF+) Student Guide (Exam FC0-U61), Chapter 2: IT Concepts and Terminology

**NEW QUESTION 78**

A systems administrator wants to run a script at a certain time every day. Which of the following is the BEST way to achieve this?

- A. Perform process management.
- B. Perform task scheduling.
- C. Set the system date and time.
- D. Set a reminder to run the script.

**Answer:** B

**Explanation:**

Task scheduling is a function of an operating system that allows users to run a script or a program at a certain time or interval automatically. Task scheduling would be the best way for a systems administrator to run a script at a certain time every day without manual intervention. Perform process management, set the system date and time, and set a reminder to run the script are not options that would allow the systems administrator to run a script at a certain time every day automatically. References: CompTIA IT Fundamentals+ Study Guide: Exam FC0-U61, Second Edition, Chapter 3: Computing Components, page 128.

**NEW QUESTION 79**

A company has installed an application that only requires a workstation to function. Which of the following architecture types is this application using?

- A. One-tier
- B. Two-tier
- C. Three-tier
- D. n-tier

**Answer:** A

**Explanation:**

One-tier architecture is a type of architecture that uses only one layer or tier for an application or system. In one-tier architecture, the application logic, data, and user interface are all contained within the same layer or tier. One-tier architecture would be the best description of a technology that allows an application to run on a workstation without requiring any other components or layers. Two-tier, three-tier, and n-tier architectures are types of architectures that use more than one layer or tier for an application or system. In two-tier architecture, the application logic and data are separated into two layers or tiers. In three-tier architecture, the application logic, data, and user interface are separated into three layers or tiers. In n-tier architecture, the application logic, data, and user interface are separated into multiple layers or tiers. References: CompTIA IT Fundamentals+ Study Guide: Exam FC0-U61, Second Edition, Chapter 5: Database Fundamentals, page 198.

**NEW QUESTION 80**

A programmer needs to store output in a place that can be accessed as quickly as possible. The data does not need to remain persistent. Which of the following is the BEST option for storing the data?

- A. Flat file
- B. Memory
- C. Relational database
- D. Solid state drive

**Answer:** B

**Explanation:**

Memory is the component of a computer system that stores data temporarily for fast access by the processor. Memory does not need to remain persistent, which means it does not retain data when the power is turned off.

A programmer can use memory to store output in a place that can be accessed as quickly as possible by the processor. Memory is also known as RAM (random access memory). References : The Official CompTIA IT Fundamentals (ITF+) Study Guide (FC0-U61), page 36.

**NEW QUESTION 81**

The IT department has established a new password policy for employees. Specifically, the policy reads:

- Passwords must not contain common dictionary words
- Passwords must contain at least one special character.
- Passwords must be different from the last six passwords used.
- Passwords must use at least one capital letter or number.

Which of the following practices are being employed? (Select TWO).

- A. Password lockout
- B. Password complexity
- C. Password expiration
- D. Passwords history
- E. Password length
- F. Password age

**Answer:** BD

**Explanation:**

Password complexity and password history are two practices that are being employed by the IT department to establish a new password policy for employees.

Password complexity is the requirement that passwords must contain a combination of different types of characters, such as letters, numbers, and symbols.

Password complexity makes passwords harder to guess or crack by attackers. Password history is the record of the previous passwords used by a user. Password history prevents users from reusing the same passwords over and over again, which reduces the risk of compromise. References : The Official CompTIA IT Fundamentals (ITF+) Study Guide (FC0-U61), page 208.

**NEW QUESTION 86**

An employee's laptop does not connect to the Internet when it is used in a coffee shop. Which of the following is the MOST likely cause?

- A. Script blocker
- B. Proxy settings
- C. Private browsing
- D. Full browser cache

**Answer:** B

**Explanation:**

Proxy settings are the configuration options that determine how a computer or device connects to the Internet through a proxy server. A proxy server is an intermediary server that acts as a gateway between the computer or device and the Internet. Proxy servers can provide security, privacy, caching, filtering, or access control functions. Proxy settings can affect the Internet connectivity of a computer or device depending on the proxy server's availability, location, or rules. If an employee's laptop does not connect to the Internet when it is used in a coffee shop, the most likely cause is that the proxy settings are incorrect or incompatible with the coffee shop's network. The employee may need to disable or change the proxy settings to connect to the Internet through the coffee shop's network. Script blocker, private browsing, and full browser cache are not likely causes of Internet connectivity issues when using a laptop in a coffee shop. References: CompTIA IT Fundamentals+ Study Guide: Exam FC0-U61, Second Edition, Chapter 6: Infrastructure Concepts, page 234.

**NEW QUESTION 88**

A systems administrator uses a program that interacts directly with hardware to manage storage, network, and virtual machines. This program is an example of:

- A. a storage area network.
- B. an embedded OS.
- C. network attached storage.
- D. a Type 1 hypervisor.

**Answer:** D

**Explanation:**

A hypervisor is a software program that allows multiple operating systems (OS) to run on the same physical hardware as virtual machines (VMs). A hypervisor can be classified into two types: Type 1 and Type 2. A Type 1 hypervisor interacts directly with the hardware and does not need an underlying OS to function. A Type 1 hypervisor is also known as a bare-metal hypervisor or a native hypervisor. A Type 1 hypervisor can manage storage, network, and VMs more efficiently and securely than a Type 2 hypervisor<sup>89</sup>. References := CompTIA IT Fundamentals (ITF+) Study Guide, 2nd Edition, Chapter 3: IT Infrastructure<sup>3</sup>; What is Hypervisor? - Definition from Techopedia<sup>10</sup>

**NEW QUESTION 92**

A game developer is purchasing a computing device to develop a game and recognizes the game engine software will require a device with high-end specifications that can be upgraded. Which of the following devices would be BEST for the developer to buy?

- A. Laptop
- B. Server
- C. Game console
- D. Workstation

**Answer:** D

**Explanation:**

A workstation would be the best device for a game developer to buy if the game engine software requires high-end specifications and upgradability. A workstation is a computing device that is designed for professional or specialized applications that require high performance, reliability, and scalability. A workstation typically has more powerful components than a standard desktop computer, such as faster processors, larger memory, better graphics cards, and more storage options. A workstation can also be customized and upgraded to meet specific needs or preferences. References : The Official CompTIA IT Fundamentals (ITF+) Study Guide (FC0-U61), page 26.

**NEW QUESTION 94**

An attacker is using subversive tactics to gain the trust of a target in order to obtain entry to a location or access to confidential information. Which of the following best describes this scenario?

- A. Phishing attack
- B. Social engineering
- C. On-path attack
- D. Eavesdropping

**Answer:** B

**Explanation:**

The scenario where an attacker is using subversive tactics to gain the trust of a target in order to obtain entry to a location or access to confidential information is best described as social engineering. Social engineering is a type of attack that exploits human psychology and behavior to manipulate people into performing actions or revealing information that benefits the attacker. Social engineering can take various forms, such as phishing, vishing, baiting, quid pro quo, pretexting, or tailgating. Phishing attack is a type of social engineering attack that involves sending fraudulent emails or messages that appear to come from legitimate sources to trick recipients into clicking on malicious links or attachments, or providing personal or financial information.

On-path attack is a type of network attack that involves intercepting or modifying data packets that are transmitted between two parties on a network. Eavesdropping is a type of network attack that involves listening to or capturing data packets that are transmitted between two parties on a network. References: The Official CompTIA IT Fundamentals (ITF+) Student Guide (Exam FC0-U61), Chapter 7: Security Concepts<sup>1</sup>

**NEW QUESTION 99**

A large payment website was breached recently. A user is concerned that the breach will affect account security on other sites. Which of the following password best practices would mitigate this risk?

- A. Password history
- B. Password reuse
- C. Password expiration
- D. Password age

**Answer:** B

**Explanation:**

Password reuse is the practice of using the same password for multiple accounts or services. Password reuse would increase the risk of account security on other sites if a large payment website was breached recently. If the attackers obtained the user's password from the breached website, they could try to use it to access

the user's accounts on other sites. Password reuse should be avoided and different passwords should be used for different accounts or services. Password history, password expiration, and password age are not password best practices that would mitigate this risk. Password history is the record of previous passwords that a user has used for an account or service. Password expiration is the time limit for using a password before it needs to be changed. Password age is the length of time that a password has been in use. References: CompTIA IT Fundamentals+ Study Guide: Exam FC0-U61, Second Edition, Chapter 8: Security Concepts, page 308.

**NEW QUESTION 101**

A technician is troubleshooting an error message and tests the same program on a separate, identical machine. Which of the following troubleshooting methodology steps is this an example of?

- A. Duplicate the problem
- B. Gather information
- C. QUESTION NO: users
- D. Divide and conquer

**Answer:** A

**Explanation:**

Antivirus is a type of software that protects a computer or device from malicious software or malware, such as viruses, worms, trojans, spyware, ransomware, etc. Antivirus software requires the most frequent updating to remain effective because new malware threats are constantly emerging and evolving. Antivirus software needs to update its database of malware signatures or definitions, which are the patterns or characteristics that identify known malware. Antivirus software also needs to update its scanning engine or algorithm, which is the method or technique that detects and removes malware. Host firewall, web browser, and device drivers are not types of software that require the most frequent updating to remain effective. Host firewall is a type of software that monitors and controls the network traffic to or from a computer or device based on rules or policies. Web browser is a type of software that allows users to access and view web pages or web applications on the Internet. Device drivers are types of software that enable the communication and interaction between the operating system and the hardware devices. References: CompTIA IT Fundamentals+ Study Guide: Exam FC0-U61, Second Edition, Chapter 8: Security Concepts, page 305.

**NEW QUESTION 105**

Which of the following is a wireless communication that requires devices to be within 6in of each other to transfer information?

- A. Infrared
- B. NFC
- C. Bluetooth
- D. WiFi

**Answer:** B

**Explanation:**

NFC stands for near field communication, which is a wireless communication technology that allows devices to exchange data or perform transactions when they are within a few centimeters of each other. NFC uses radio frequency identification (RFID) to create a short-range wireless connection. NFC is commonly used for contactless payments, smart cards, and digital wallets. References : The Official CompTIA IT Fundamentals (ITF+) Study Guide (FC0-U61), page 174.

**NEW QUESTION 110**

Which of the following software license models allows a developer to modify the original code and release its own version of the application?

- A. Proprietary software
- B. Commercial software
- C. Open-source software
- D. Cross-platform software

**Answer:** C

**Explanation:**

Open source software is software that allows anyone to access, modify, and distribute its source code, which is the human-readable instructions that make up the software. Open source software encourages collaboration and innovation among developers and users. Examples of open source software include Linux, Firefox, and WordPress. Other types of software license models, such as proprietary and commercial software, restrict the access and modification of the source code. References : The Official CompTIA IT Fundamentals (ITF+) Study Guide (FC0-U61), page 122.

**NEW QUESTION 114**

A developer is writing a script to calculate a bank account balance within two decimal places. Which of the following data types should the developer select to store the balance?

- A. Boolean
- B. Integer
- C. Float
- D. Char

**Answer:** C

**Explanation:**

A float is a data type that can store decimal numbers, such as 3.14 or 0.01. This is suitable for calculating a bank account balance within two decimal places, as it can represent fractions of a dollar. A boolean is a data type that can only store true or false values, which is not useful for numerical calculations. An integer is a data type that can store whole numbers, such as 1 or 100, but not decimals. A char is a data type that can store a single character, such as 'a' or '9', but not multiple characters or decimals. References: CompTIA IT Fundamentals (ITF+) Study Guide: Exam FC0-U61, Second Edition, Chapter 4: Software Development Concepts, page 1371

**NEW QUESTION 119**

A business would like to create an employee portal that employees will have access to when they are at work. The employees will not be able to connect to the



portal from home without a VPN connection. Which of the following types of application does this describe?

- A. Local application
- B. Intranet application
- C. Extranet application
- D. Internet application

**Answer: B**

**Explanation:**

An intranet application is a type of application that is hosted on a private network and can only be accessed by authorized users within an organization. An intranet application would best describe an employee portal that employees can access when they are at work, but not from home without a VPN connection. A VPN (Virtual Private Network) is a technology that creates a secure and encrypted tunnel between a client device and a remote server over the Internet. A VPN can allow employees to access the intranet application from home by connecting to the private network of the organization. Local application, extranet application, and Internet application are not types of applications that describe an employee portal that employees can access when they are at work, but not from home without a VPN connection. References: CompTIA IT Fundamentals+ Study Guide: Exam FC0-U61, Second Edition, Chapter 5: Database Fundamentals, page 199.

**NEW QUESTION 124**

Joe, a user, finds out his password for a social media site has been compromised. Joe tells a friend that his email and banking accounts are probably also compromised. Which of the following has Joe MOST likely performed?

- A. Password reuse
- B. Snooping
- C. Social engineering
- D. Phishing

**Answer: A**

**Explanation:**

Password reuse is the practice of using the same password for multiple accounts or services. Password reuse is a bad security habit that can lead to compromise of multiple accounts if one of them is breached by an attacker. Joe has most likely performed password reuse if he thinks his email and banking accounts are also compromised after his password for a social media site was compromised. Joe should use different passwords for different accounts and change them regularly to prevent password reuse. References : The Official CompTIA IT Fundamentals (ITF+) Study Guide (FC0-U61), page 208.

**NEW QUESTION 125**

A computer technician is assigned a ticket to install a laptop for a new employee. Due to the arrangement of the workspace, the employee requests that the laptop be installed with the cover closed. Which of the following would be required to satisfy this request? (Choose two.)

- A. Printer
- B. Mouse
- C. Webcam
- D. External hard drive
- E. Speakers
- F. Display

**Answer: BF**

**Explanation:**

A mouse and a display would be required to satisfy the request of installing a laptop with the cover closed. A mouse is an input device that allows users to move a cursor and click on icons or buttons on the screen. A display is an output device that shows visual information on the screen. A mouse and a display would enable the user to interact with the laptop without opening the cover. A printer, a webcam, an external hard drive, and speakers are not devices that would be required to satisfy the request of installing a laptop with the cover closed. References: CompTIA IT Fundamentals+ Study Guide: Exam FC0-U61, Second Edition, Chapter 3: Computing Components, page 106.

**NEW QUESTION 130**

Which of the following filesystems is compatible with the greatest number of operating systems?

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

**Answer: B**

**Explanation:**

The filesystem that is compatible with the greatest number of operating systems is FAT32. FAT32 stands for File Allocation Table 32-bit, which is a filesystem that organizes data into clusters or groups of sectors on a storage device, such as a hard disk or a flash drive. FAT32 uses a 32-bit table to keep track of the location and status of each cluster. FAT32 can support volumes up to 2 TB and files up to 4 GB in size. FAT32 is compatible with most operating systems, such as Windows, Linux, Mac OS, Android, etc., as well as most devices, such as cameras, printers, game consoles, etc. FAT32 is one of the oldest and simplest filesystems, but it also has some limitations and drawbacks, such as fragmentation, waste of space, lack of security features, etc. ext4 is not the filesystem that is compatible with the greatest number of operating systems, but rather a filesystem that is mainly used by Linux operating systems. ext4 stands for Fourth Extended Filesystem, which is a filesystem that organizes data into blocks or groups of sectors on a storage device. ext4 uses an inode table to keep track of the location and attributes of each file or directory. ext4 can support volumes up to 1 EB and files up to 16 TB in size. ext4 has many features and advantages over FAT32, such as journaling, extents, subdirectories, encryption, etc., but it also has limited compatibility with other operating systems, such as Windows or Mac OS. NTFS is not filesystem that is compatible with greatest number of operating systems, but rather filesystem that is mainly used by Windows operating systems. NTFS stands for New Technology File System, which is filesystem that organizes data into clusters or groups of sectors on storage device. NTFS uses Master File Table (MFT) to keep track of location and attributes of each file or directory. NTFS can support volumes up to 256 TB and files up to 256 TB in size. NTFS has many features and advantages over FAT32, such as journaling, compression, encryption, security, etc., but it also has limited compatibility with other operating systems, such as Linux or Mac OS. HFS is not filesystem that is compatible with greatest number of operating systems, but rather filesystem that is mainly used by Mac OS operating systems. HFS stands for Hierarchical File System, which is filesystem that organizes data into blocks or groups of sectors on storage device. HFS uses

catalog file to keep track of location and attributes of each file or directory. HFS can support volumes up to 2 TB and files up to 2 GB in size. HFS has some features and advantages over FAT32, such as resource forks, aliases, etc., but it also has some limitations and drawbacks, such as fragmentation, waste of space, lack of security features, etc. HFS also has limited compatibility with other operating systems, such as Windows or Linux. References: The Official CompTIA IT Fundamentals (ITF+) Student Guide (Exam FC0-U61), Chapter 4: Operating System Fundamentals<sup>1</sup>

**NEW QUESTION 133**

Which of the following is both an input and output device?

- A. Microphone
- B. Speaker
- C. Touch-screen monitor
- D. Keyboard

**Answer:** C

**Explanation:**

A touch-screen monitor is a device that can function as both an input and output device. An input device is a device that allows users to enter data or commands into a computer or system. An output device is a device that displays or produces data or information from a computer or system. A touch-screen monitor can function as an input device by detecting the touch or gesture of the user on the screen and sending the corresponding signal to the computer or system. A touch-screen monitor can also function as an output device by showing visual information on the screen. A microphone, a speaker, and a keyboard are not devices that can function as both an input and output device. A microphone is an input device that allows users to record sound or voice into a computer or system. A speaker is an output device that plays sound or voice from a computer or system.

A keyboard is an input device that allows users to type text or characters into a computer or system. References: CompTIA IT Fundamentals+ Study Guide: Exam FC0-U61, Second Edition, Chapter 3: Computing Components, page 106.

**NEW QUESTION 137**

An IP address is 32 bits long. If converted to bytes, it would be:

- A. 4 bytes
- B. 8 bytes
- C. 16 bytes
- D. 64 bytes

**Answer:** A

**Explanation:**

A byte is a unit of information that consists of eight bits. A bit is a binary digit that can have a value of either 0 or 1. An IP address is 32 bits long, which means it is composed of four groups of eight bits each. Therefore, if converted to bytes, an IP address would be four bytes long. For example, the IP address 192.168.1.1 in binary form is: 11000000.10101000.00000001.00000001

This IP address has four groups of eight bits each, which are equivalent to four bytes. References: CompTIA IT Fundamentals+ Study Guide: Exam FC0-U61, Second Edition, Chapter 6: Infrastructure Concepts, page 221.

**NEW QUESTION 138**

For a disaster recovery exercise, a company wants to ensure customer data is recovered before operational data. This is an example of:

- A. redundancy.
- B. replication.
- C. prioritization.
- D. fault tolerance.

**Answer:** C

**Explanation:**

Prioritization is the example of a disaster recovery exercise that involves ensuring customer data is recovered before operational data. Prioritization is the process of ranking or ordering the importance or urgency of tasks, goals, or resources. In disaster recovery, prioritization helps to determine which data, systems, or functions should be restored first based on their criticality or impact on the business continuity. For example, a company may prioritize customer data over operational data because customer data is more valuable or essential for the business operations. References : The Official CompTIA IT Fundamentals (ITF+) Study Guide (FC0-U61), page 200.

**NEW QUESTION 143**

A company executive wants to view company training videos from a DVD. Which of the following components would accomplish this task?

- A. Optical drive
- B. Hard disk drive
- C. Solid state drive
- D. Flash drive

**Answer:** A

**Explanation:**

An optical drive is a component that can accomplish the task of viewing company training videos from a DVD. An optical drive is a device that can read and write data from optical discs, such as CDs, DVDs, or Blu-ray discs. An optical drive uses a laser beam to access the data stored on the disc. An optical drive can play video or audio files from optical discs, as well as install software or store data.

A hard disk drive (HDD) is a component that can store large amounts of data on magnetic platters, but it cannot read or write data from optical discs. A solid state drive (SSD) is a component that can store data on flash memory chips, but it cannot read or write data from optical discs. A flash drive is a component that can store data on flash memory chips and connect to a USB port, but it cannot read or write data from optical discs.

**NEW QUESTION 147**

When following the troubleshooting methodology, which of the following should be performed last?

- A. Document findings.
- B. Establish a plan.
- C. Determine the cause.
- D. Verify functionality.

**Answer:** A

**Explanation:**

The troubleshooting methodology is a systematic process of identifying and resolving problems with computers or other devices. The troubleshooting methodology consists of six steps: identify the problem, establish a theory of probable cause, test the theory to determine cause, establish a plan of action to resolve the problem and implement the solution, verify full system functionality and if applicable implement preventive measures, document findings/actions/outcomes. The last step of the troubleshooting methodology is to document findings/actions/outcomes. This step involves recording what was done to solve the problem, what was learned from the process, what preventive measures were taken (if any), and any feedback from the customer or user. Documenting findings/actions/outcomes is important for several reasons: it helps keep track of what was done and why; it helps avoid repeating the same steps or mistakes in the future; it helps share knowledge and best practices with others; it helps improve customer satisfaction and trust; it helps comply with organizational policies or regulations

**NEW QUESTION 149**

A technician has verified full system functionality. Which of the following actions should the technician take next?

- A. Question the users.
- B. Determine if anything has changed.
- C. Document the findings.
- D. Gather Information.

**Answer:** C

**Explanation:**

Documenting the findings is the last step in the troubleshooting process, after verifying full system functionality. Documenting the findings helps to create a record of the problem and the solution, which can be useful for future reference or training purposes. Questioning the users, determining if anything has changed, and gathering information are steps that precede verifying full system functionality in the troubleshooting process. References: The Official CompTIA IT Fundamentals (ITF+) Student Guide (Exam FC0-U61), Chapter 2: IT Concepts and Terminology1

**NEW QUESTION 152**

Which of the following is an example of a compiled language?

- A. C++
- B. SQL
- C. Python
- D. XML

**Answer:** A

**Explanation:**

C++ is an example of a compiled language. A compiled language is a programming language that requires a compiler to translate the source code into executable code before running the program. A compiler is a program that converts the entire source code into machine code or intermediate code that can be executed by the processor or another program. A compiled language usually offers faster performance and lower memory usage than an interpreted language, but it also requires more time and effort to compile and debug the code. SQL is not a programming language, but a query language that is used to interact with databases. SQL statements are usually executed by a database management system (DBMS) that interprets and processes them. Python is an example of an interpreted language. An interpreted language is a programming language that does not require compilation before running the program. An interpreter is a program that reads and executes the source code line by line at runtime. An interpreted language usually offers more flexibility and portability than a compiled language, but it also requires more memory and CPU resources to run the program. XML is not a programming language either, but a markup language that is used to define and structure data in a human-readable and machine-readable format. XML documents are usually parsed by another program that uses them for data exchange or presentation. References: CompTIA IT Fundamentals (ITF+) Study Guide: Exam FC0-U61, Second Edition, Chapter 4: Software Development Concepts, pages 134-135

**NEW QUESTION 154**

Which of the following WiFi security options would create the MOST need for a VPN connection on the client device?

- A. Open
- B. WEP
- C. WPA
- D. WPA2

**Answer:** A

**Explanation:**

Open is a WiFi security option that does not use any encryption or authentication to protect the wireless network from unauthorized access or eavesdropping. Open would create the most need for a VPN connection on the client device because VPN (Virtual Private Network) is a technology that creates a secure and encrypted tunnel between the client device and a remote server over the Internet. VPN would provide an additional layer of security and privacy for the wireless communication that is not provided by the open WiFi network. WEP (Wired Equivalent Privacy), WPA (WiFi Protected Access), and WPA2 (WiFi Protected Access II) are WiFi security options that use encryption and authentication to protect the wireless network from unauthorized access or eavesdropping. WEP, WPA, and WPA2 would create less need for a VPN connection on the client device than open because they already provide some level of security and privacy for the wireless communication. References: CompTIA IT Fundamentals+ Study Guide: Exam FC0-U61, Second Edition, Chapter 8: Security Concepts, page 311.

**NEW QUESTION 156**

Which of the following would be considered the BEST method of securely distributing medical records?

- A. Encrypted flash drive
- B. Social networking sites
- C. Fax
- D. FTP file sharing

**Answer:** A

**Explanation:**

An encrypted flash drive would be the best method of securely distributing medical records among the given options. An encrypted flash drive is a portable storage device that uses encryption to protect the data stored on it. Encryption is a process of transforming data into an unreadable form that can only be restored with a key or password. Encryption can prevent unauthorized access or disclosure of sensitive or confidential data, such as medical records, if the flash drive is lost or stolen. An encrypted flash drive can also be used to transfer data between different devices or locations securely. References : The Official CompTIA IT Fundamentals (ITF+ Study Guide (FC0-U61), page 203.

**NEW QUESTION 159**

Which of the following are benefits of a security awareness training program9 (Select two).

- A. Enhances overall security
- B. Provides information on how to avoid phishing
- C. Lowers the incidence of hardware failures
- D. Increases the availability of computers
- E. Advances end users' technical skills
- F. Creates IT security opportunities for end users

**Answer:** AB

**Explanation:**

The benefits of a security awareness training program are enhancing overall security and providing information on how to avoid phishing. Enhancing overall security is a benefit of a security awareness training program because it helps users understand the importance and value of security for themselves and their organization. It also helps users develop good security habits and behaviors, such as choosing strong passwords, locking their devices, reporting incidents, etc., which can prevent or reduce security risks and threats. Providing information on how to avoid phishing is a benefit of a security awareness training program because it helps users recognize and respond to phishing attacks, which are one of the most common and effective types of social engineering attacks. Phishing attacks involve sending fraudulent emails or messages that appear to come from legitimate sources to trick recipients into clicking on malicious links or attachments, or providing personal or financial information. A security awareness training program can teach users how to identify phishing signs, such as spelling errors, generic greetings, urgent requests, etc., and how to verify the sender, the URL, or the attachment before opening or responding. Lowering the incidence of hardware failures is not a benefit of a security awareness training program, but rather a benefit of a hardware maintenance program. A hardware maintenance program involves performing regular checks and repairs on the physical components of a system or network, such as disks, memory, CPU, power supply, etc., to ensure their proper functioning and performance. A hardware maintenance program can prevent or reduce hardware failures, which can cause data loss, corruption, or interruption for the system or network and its users. Increasing the availability of computers is not a benefit of a security awareness training program, but rather a benefit of a backup and recovery program. A backup and recovery program involves creating and restoring copies of data or systems in case of data loss, corruption, or disaster. A backup and recovery program can increase the availability of computers by ensuring that users can access their data or systems from alternative sources or locations in case of an emergency. Advancing end users' technical skills is not a benefit of a security awareness training program, but rather a benefit of a technical training program. A technical training program involves teaching users how to use various technologies or applications effectively and efficiently. A technical training program can advance end users' technical skills by increasing their knowledge, competence, and productivity with the technologies or applications they use. Creating IT security opportunities for end users is not a benefit of a security awareness training program, but rather a benefit of a career development program. A career development program involves providing users with guidance and resources to help them achieve their professional goals and aspirations. A career development program can create IT security opportunities for end users by exposing them to different IT security roles, paths, or certifications that they can pursue or obtain. References: The Official CompTIA IT Fundamentals (ITF+) Student Guide (Exam FC0-U61), Chapter 7: Security Concepts

**NEW QUESTION 161**

Which of the following is used to protect intellectual property while requiring the owner to provide the public with working details?

- A. Patent
- B. Trademark
- C. License
- D. Copyright

**Answer:** A

**Explanation:**

A patent is used to protect intellectual property while requiring the owner to provide the public with working details of an invention or a process. A patent grants the owner the exclusive right to make, use, or sell the invention or process for a limited period of time, usually 20 years. A trademark is used to protect a name, symbol, logo, or slogan that identifies a product or service. A trademark grants the owner the exclusive right to use the mark to distinguish their product or service from others. A license is used to grant permission to use intellectual property under certain terms and conditions. A license does not transfer ownership of the intellectual property, but only grants limited rights to use it. A license can be revoked by the owner if the terms and conditions are violated. A copyright is used to protect original works of authorship, such as books, music, movies, or software. A copyright grants the owner the exclusive right to reproduce, distribute, perform, display, or create derivative works based on their original work. References: The Official CompTIA IT Fundamentals (ITF+) Student Guide (Exam FC0-U61), Chapter 8: Software Development Concepts

**NEW QUESTION 166**

A user needs to enter text and numbers to produce charts that demonstrate sales figures. Which of the following types of software would BEST complete this task?

- A. Text editing software
- B. Visual diagramming software
- C. Spreadsheet software
- D. Web browsing software

**Answer:** C



**Explanation:**

Spreadsheet software is a type of software that allows users to enter text and numbers in a grid of cells and perform calculations and analysis on the data. Spreadsheet software can also produce charts that demonstrate sales figures or other trends. Examples of spreadsheet software are Microsoft Excel, Google Sheets, and LibreOffice Calc.

References: CompTIA IT Fundamentals+ Study Guide: Exam FC0-U61, Second Edition, Chapter 7: Software Installation and Functions, page 266.

**NEW QUESTION 168**

A corporate network just implemented a 60-day password-warning banner. Which of the following is most likely going to happen in 60 days?

- A. Password reset
- B. Password expiration
- C. Password reuse
- D. Password Implementation

**Answer: B**

**Explanation:**

The most likely thing that will happen in 60 days after implementing a 60-day password-warning banner is password expiration. A password-warning banner is a message that appears on the screen when a user logs in to a system or network, informing them of how many days are left before their password expires. A password expiration policy is a security measure that requires users to change their passwords periodically, usually every 30 to 90 days. This policy helps to prevent unauthorized access or compromise of passwords by hackers or malicious insiders. Password reset is the process of changing or creating a new password for a user account when the user forgets their password or wants to change it for security reasons. Password reset can be done by the user themselves or by an administrator, depending on the system or network settings. Password reset does not necessarily happen in 60 days after implementing a 60-day password-warning banner, unless the user forgets their password or chooses to change it before it expires. Password reuse is the practice of using the same password for multiple user accounts or systems. Password reuse is not recommended as it increases the risk of compromise if one of the accounts or systems is breached by hackers or malicious insiders. Password reuse does not necessarily happen in 60 days after implementing a 60-day password-warning banner, unless the user chooses to use their old password for their new password after it expires. Password implementation is not a term used in security, but it may refer to the process of creating or enforcing password policies for user accounts or systems. Password implementation does not necessarily happen in 60 days after implementing a 60-day password-warning banner, unless there are changes in the password policies that require users to comply with them. References: The Official CompTIA IT Fundamentals (ITF+) Student Guide (Exam FC0-U61), Chapter 7: Security Concepts1

**NEW QUESTION 173**

Which of the following actions is most likely associated with database use?

- A. Creating diagrams
- B. Querying
- C. File sharing
- D. Printing

**Answer: B**

**Explanation:**

The action that is most likely associated with database use is querying. Querying is the process of retrieving data from a database based on certain criteria or conditions. Querying allows users to access specific information from large amounts of data stored in tables. Querying can be done using SQL (Structured Query Language), which is a standard language for interacting with relational databases. SQL queries can perform various operations, such as selecting, inserting, updating, deleting, or joining data from tables. Creating diagrams is not an action that is associated with database use, but rather with software development or design. Creating diagrams can help visualize the structure, logic, or flow of a program or an algorithm. Examples of diagrams include flowcharts, UML diagrams, ER diagrams, etc. File sharing is not an action that is associated with database use, but rather with network use. File sharing is the process of allowing users to access or transfer files over a network. File sharing can be done using various protocols, such as FTP, SMB, NFS, etc. Printing is not an action that is associated with database use, but rather with output device use. Printing is the process of producing hard copies of documents, images, or other data on paper or other media using a printer. References: The Official CompTIA IT Fundamentals (ITF+) Student Guide (Exam FC0-U61), Chapter 6: Database Fundamentals1

**NEW QUESTION 176**

A help desk technician loads a browser-based ticketing system, but when navigating to the queue, the technician realizes that another employee's queue is being accessed. Which of the following explains the issue?

- A. The previous user's session is cached.
- B. The proxy settings were misconfigured.
- C. The application is not compatible with the browser.
- D. The browser was opened in private mod

**Answer: A**

**Explanation:**

The issue that explains why the technician is accessing another employee's queue is that the previous user's session is cached. Caching is the process of storing data temporarily in a memory or disk for faster access or reuse. Caching can improve the performance and efficiency of a browser-based application, but it can also cause security or privacy issues if the data is not cleared or updated properly. The previous user's session may have been cached by the browser or the application, and the technician may have accessed the same URL or credentials without logging out or clearing the cache. The proxy settings were not misconfigured, as this would not affect the access to another employee's queue, but rather the access to the internet or the application server. The proxy settings are the configuration options that determine how a browser connects to a proxy server, which is an intermediary server that acts as a gateway between the browser and the internet or the application server. The proxy server can provide security, anonymity, or caching functions for the browser. The application is not incompatible with the browser, as this would not affect the access to another employee's queue, but rather the functionality or appearance of the application. The application compatibility is the degree to which an application works correctly and efficiently with a specific browser or operating system. The browser was not opened in private mode, as this would not affect the access to another employee's queue, but rather prevent the caching of data. The private mode is a feature that allows a browser to browse the internet without storing any browsing history, cookies, cache, or other data on the device. References: The Official CompTIA IT Fundamentals (ITF+) Student Guide (Exam FC0-U61), Chapter 5: Infrastructure Concepts1

**NEW QUESTION 181**

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### FC0-U61 Practice Exam Features:

- \* FC0-U61 Questions and Answers Updated Frequently
- \* FC0-U61 Practice Questions Verified by Expert Senior Certified Staff
- \* FC0-U61 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* FC0-U61 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The FC0-U61 Practice Test Here](#)**