Free Questions for FC0-U61 by ebraindumps

Shared by Pearson on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

A customer is looking for a device that uses tap to pay when making purchases. Which of the following technologies should the customer use?

Options:

A- Wi-Fi

B- IR

C- Bluetooth

D- NFC

Answer:

D

Explanation:

NFC (Near Field Communication) is a wireless technology that allows devices to communicate and exchange data within a short range, typically a few centimeters. NFC is commonly used for tap to pay transactions, where a customer can use a contactless card or a smart device (such as a smartphone or a smartwatch) to make payments by tapping or hovering over a compatible terminal. NFC is different from other wireless technologies, such as Wi-Fi, IR (Infrared), and Bluetooth, because it does not require pairing, authentication, or network access to work. NFC is also faster, more secure, and more convenient than other payment methods, such as inserting or swiping a card.Reference:CompTIA IT Fundamentals (ITF+) Certification Guide, page 25;What is Tap to Pay and How Does It Work?

Question 2

Question Type: **MultipleChoice**

A technician needs to install and configure a wireless SOHO network. Which of the following should the technician configure to reduce Wi-Fi interference from other household appliances?

Options:

A- 2.4GHz

B- 5GHz

C- 802.11b

D- 802.11g

Answer:

B

Explanation:

The 5GHz frequency band is less prone to interference from other household appliances, such as microwaves, cordless phones, and Bluetooth devices, than the 2.4GHz band. The 5GHz band also offers more non-overlapping channels and higher data rates than the 2.4GHz band. However, the 5GHz band has a shorter range and lower penetration than the 2.4GHz band, so the technician should consider the size and layout of the SOHO network before choosing the frequency band. 802.11b and 802.11g are wireless standards that operate in the 2.4GHz band, while 802.11a, 802.11n, and 802.11ac can operate in both the 2.4GHz and 5GHz bands.Reference:

Basic Wired/Wireless SOHO Network | CompTIA A+ 220-1001 | 2.3

Installing a SOHO Network -- CompTIA A+ 220-1001 -- 2.3

Installing and Configuring a SOHO Network - CompTIA A+ Complete: Review ...

Question 3

Question Type: **MultipleChoice**

A network technician needs to ensure data on a network drive is fully backed up. Which of the following backups should the technician implement?

Options:

A- Database

B- Webserver

C- File

D- Operating system

Answer:

C

Explanation:

A file backup is a type of backup that copies individual files or folders from a source to a destination. A file backup can be used to back up data on a network drive, as it allows the technician to select the specific files or folders that need to be backed up. A file backup can also be performed incrementally or differentially, which means that only the files that have changed since the last backup are copied, saving time and space. A file backup can be restored easily, as it does not require any special software or hardware to access the backed up files.

A database backup is a type of backup that copies the entire database or parts of it from a source to a destination. A database backup is used to back up data that is stored in a structured format, such as tables, records, and indexes. A database backup can be performed using the native tools of the database management system, such as SQL Server or Oracle, or using third-party software. A database backup can be restored using the same tools that performed the backup, and it may require some additional steps, such as restoring the transaction logs or applying the differential backups.

A webserver backup is a type of backup that copies the files and folders that are related to a webserver, such as HTML, CSS, JavaScript, PHP, images, and so on. A webserver backup is used to back up data that is used to host a website or a web application. A webserver backup can be performed using the file backup method, or using specialized software that can backup the webserver configuration, settings, and permissions. A webserver backup can be restored by copying the files and folders back to the webserver, or using the software that performed the backup.

An operating system backup is a type of backup that copies the entire operating system or parts of it from a source to a destination. An operating system backup is used to back up data that is essential for the functioning of the computer, such as the system files, the registry, the drivers, the applications, and the user settings. An operating system backup can be performed using the native tools of the operating system, such as Windows Backup or Time Machine, or using third-party software. An operating system backup can be restored by booting from a recovery media, such as a CD, DVD, or USB, or using the software that performed the backup.

Question 4

Question Type: MultipleChoice

Which of the following notational systems uses the most characters to represent the decimal number 10?

Options:

A- Octal

B- Hexadecimal

C- Decimal

D- Binary

Answer:

D

Explanation:

A notational system is a way of writing numbers using symbols or digits. The base or radix of a notational system is the number of symbols or digits it uses to represent numbers. For example, the decimal system uses 10 symbols (0 to 9) and has a base of 10. The octal system uses 8 symbols (0 to 7) and has a base of 8. The hexadecimal system uses 16 symbols (0 to 9 and A to F) and has a base of 16. The binary system uses 2 symbols (0 and 1) and has a base of 2.

To represent the decimal number 10 in different notational systems, we need to convert it to the corresponding base. This can be done by dividing the number by the base repeatedly and writing the remainders in reverse order. For example:

To convert 10 to octal, we divide 10 by 8 and get a quotient of 1 and a remainder of 2. Then we divide 1 by 8 and get a quotient of 0 and a remainder of 1. The remainders in reverse order are 12, so 10 in octal is 12.

To convert 10 to hexadecimal, we divide 10 by 16 and get a quotient of 0 and a remainder of 10. The remainder is 10, which is represented by the symbol A in hexadecimal, so 10 in hexadecimal is A.

To convert 10 to binary, we divide 10 by 2 and get a quotient of 5 and a remainder of 0. Then we divide 5 by 2 and get a quotient of 2 and a remainder of 1. Then we divide 2 by 2 and get a quotient of 1 and a remainder of 0. Then we divide 1 by 2 and get a quotient of 0 and a remainder of 1. The remainders in reverse order are 1010, so 10 in binary is 1010.

The notational system that uses the most characters to represent the decimal number 10 is the binary system, which uses 4 characters (1010). The octal system uses 2 characters (12), the hexadecimal system uses 1 character (A), and the decimal system uses 2 characters (10).

Question 5

Question Type: MultipleChoice

Which of the following file extensions is used for a consolidated group of files?

Options:

A- .bat

B- .avi

C- .rar

D- .rtf

Answer:

C

Explanation:

A file extension is a suffix that indicates the type, format, or content of a file. Different file extensions are associated with different applications, programs, or functions. For example, .bat is a file extension for a batch file, which is a script that contains a series of commands to be executed by the command-line interpreter. .avi is a file extension for an audio video interleave file, which is a multimedia container format that stores video and audio data. .rtf is a file extension for a rich text format file, which is a document format that supports text formatting, such as fonts, colors, and styles.

A consolidated group of files is a collection of files that are compressed or archived into a single file, usually to reduce the file size, save disk space, or facilitate file transfer. A consolidated group of files can be created or extracted by using a compression or archiving software, such as WinRAR, 7-Zip, or WinZip. One of the most common file extensions for a consolidated group of files is .rar, which stands for Roshal Archive. .rar is a proprietary file format that supports data compression, error recovery, encryption, and splitting.For example, in the following image1, a folder named Documents contains four files: resume.docx, report.pdf, budget.xlsx, and presentation.pptx. The folder is compressed into a single file named Documents.rar, which has a smaller file size and can be easily attached to an email or uploaded to a cloud storage.

Therefore, the correct answer is C. .rar, as it is the file extension that is used for a consolidated group of files.

CompTIA IT Fundamentals+ (ITF+) Certification Exam Objectives, page 15, section 3.5

CompTIA IT Fundamentals+ (ITF+) Study Guide, page 191, section 7.4

CompTIA IT Fundamentals+ (ITF+) All-in-One Exam Guide, Second Edition, page 287, chapter 8

Using File Systems | CompTIA IT Fundamentals+ (FC0-U61) | Part 25 of 38

Question 6

Question Type: **MultipleChoice**

Which of the following best describes the differences between data and information?

Options:

A- Data is a result of the analytical processing of information.

B- Information is raw unstructured or uncorrected data.

C- Information can exist without data.

D- Data can be facts, figures, or events that can be processed to create information.

Answer:

D

Explanation:

Data and information are related but distinct concepts in IT. Data refers to the raw, unorganized, and uninterpreted facts, figures, or events that can be collected, stored, or transmitted by various means. Information refers to the meaningful, organized, and interpreted output that is derived from data by applying some form of analysis, processing, or logic. Data can be processed to create information, but information cannot exist without data. The other options are incorrect because they either confuse the roles of data and information, or imply that information can be independent of data.Reference:

CompTIA IT Fundamentals FC0-U61 Certification Study Guide, page 18, section 1.1: "Data is the raw, unorganized, and uninterpreted facts, figures, or events that can be collected, stored, or transmitted by various means. Information is the meaningful, organized, and interpreted output that is derived from data by applying some form of analysis, processing, or logic."

CompTIA ITF+ Practice Test, question 239: "Data can be facts, figures, or events that can be processed to create information is the correct answer."

Question 7

Question Type: MultipleChoice

A technician reading workstation security logs notices that an unidentified device is plugged into a USB port several hours a day but is never plugged in when the technician goes to check the machine. File audits reveal nothing unexpected. Which of the following devices is most likely causing this message?

Options:

A- Mobile phone

B- Mouse

C- Scanner

D- External hard drive

Answer:

A

Explanation:

A mobile phone is the most likely device that is causing this message, because it can be plugged into a USB port for charging or data transfer, and then unplugged when the user leaves the workstation. A mobile phone may also not be detected by the file audits, as it may not have any files stored on the workstation or may use encryption or password protection. A mouse, a scanner, and an external hard drive are less likely to be plugged and unplugged frequently, and they would also leave traces of their presence in the file audits or device manager.Reference:CompTIA IT Fundamentals+ FC0-U61 Cert Guide, Chapter 3: Device Ports and Peripherals, page 77;CompTIA IT Fundamentals+ (Exam FC0-U61) Module 4 / Unit 2 / Connecting to a Network, page 6;How to identify USB Ports in Device Manager?

Question 8

Question Type: MultipleChoice

Which of the following interfaces is best for viewing database performance information?

Options:

A- Direct

B- Programmatic

C- Query

D- Utility

Answer:

D

Explanation:

A utility interface is a type of interface that provides tools and features for managing, monitoring, and optimizing a database system. A utility interface can help users view database performance information, such as resource usage, query execution time, error logs, backup status, and optimization suggestions. A utility interface can also help users perform tasks such as backup, restore, repair, export, import, and migrate data. A utility interface is best suited for viewing database performance information, because it can provide a comprehensive and graphical overview of the database system's health and efficiency.

Some examples of utility interfaces for databases are:

MySQL Workbench1: A GUI tool for MySQL that provides data modeling, SQL development, server administration, backup and migration, and performance tuning features.

Oracle Enterprise Manager: A web-based tool for Oracle that provides database management, cloud control, application performance management, and data warehouse management features.

Microsoft SQL Server Management Studio: A GUI tool for SQL Server that provides database design, development, administration, analysis, and reporting features.

The Official CompTIA IT Fundamentals (ITF+) Student Guide (Exam FC0-U61), Chapter 5: Database Fundamentals, pages 5-15 to 5-16.

CompTIA IT Fundamentals Certification Training, Module 5: Database Fundamentals, Lesson 3: Methods Used to Interface with Databases.

Interfaces in DBMS

Question 9

Question Type: **MultipleChoice**

Which of the following is most appropriate to list on a social media site about an employer?

Options:

A- Work email

B- Job title

C- Hire date

D- Customers served

E- Contract

Answer:

B

Explanation:

A system usage agreement is a document that defines the rules and expectations for using a company's IT resources, such as computers, networks, intranets, software, and data. A system usage agreement typically covers topics such as acceptable use, security, privacy, monitoring, ownership, and consequences of violations. A system usage agreement helps to protect the company's assets, reputation, and legal compliance, as well as the users' rights and responsibilities. Privacy expectations on a company intranet should be limited to what is stated in the system usage agreement, as the company has the right and the duty to monitor and control the intranet for business purposes. Users should not assume that their activities on the intranet are private or confidential, unless the system usage agreement explicitly guarantees such privacy. The other options, such as precedents, HR policy, and word of mouth, are not reliable or consistent sources of privacy expectations, as they may vary, change, or conflict with the system usage agreement or the law.Reference:CompTIA IT Fundamentals (ITF+) Certification Guide, page 100;10 Intranet Best Practices for a Successful Intranet in 2021, point 7.

Question 10

Question Type: MultipleChoice

Privacy expectations on a company intranet should be limited to:

Options:

A- precedents.

B- HR policy.

C- word of mouth.

D- system usage agreements.

Answer:

D

Explanation:

A system usage agreement is a document that defines the rules and expectations for using a company's IT resources, such as computers, networks, intranets, software, and data. A system usage agreement typically covers topics such as acceptable use, security, privacy, monitoring, ownership, and consequences of violations. A system usage agreement helps to protect the company's assets, reputation, and legal compliance, as well as the users' rights and responsibilities. Privacy expectations on a company intranet should be limited to what is stated in the system usage agreement, as the company has the right and the duty to monitor and control the intranet for business purposes. Users should not assume that their activities on the intranet are private or confidential, unless the system usage agreement explicitly guarantees such privacy. The other options, such as precedents, HR policy, and word of mouth, are not reliable or consistent sources of privacy expectations, as they may vary, change, or conflict with the system usage agreement or the law.Reference:CompTIA IT Fundamentals (ITF+) Certification Guide, page 100;10 Intranet Best Practices for a Successful Intranet in 2021, point 7.

Question 11

Question Type: **MultipleChoice**

A hacker was able to obtain a user's password for email, social media, and bank accounts. Which of the following should the user do to prevent this type of attack in the future?

Options:

A- Delete the tracking cookies.

B- Avoid password reuse.

C- Use a complex password.

D- Clear the browser cache.

Answer:

B

Explanation:

Password reuse is a common practice that makes users vulnerable to credential stuffing attacks, where hackers use stolen passwords from one site to access other accounts of the same user. This can lead to identity theft, financial loss, and privacy breaches. To prevent this type of attack in the future, the user should avoid password reuse and create unique and strong passwords for each account. The user should also use a password manager to store and generate passwords securely, and enable multi-factor authentication whenever possible.Reference:

Chapter 32 Explain Password Best Practices - CompTIA IT Fundamentals+ FC0-U61 Cert Guide

Cybersecurity and End User Passwords | Cybersecurity | CompTIA

Managing Password Policies -- CompTIA Security+ SY0-401: 5.3

CompTIA IT Fundamentals+ Certification Exam Test Questions With Answers ...