FC0-U11 comptia

Number: FC0-U11
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

Exam A

QUESTION 1

You are working with a team that will be bringing in new computers to a sales department at a company. The sales team would like to keep not only their old files, but system settings as well on the new PC's. What should you do?

A. Do a system backup (complete) on each old machine, then restore it onto the new machines.

B. Copy the files and the Windows Registry to a removable media then copy it onto the new machines.

C. Use the User State Migration tool to move the system settings and files to the new machines.

D. Use the Disk Management tool to move everything to the new computer.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The User State Migration Tool is made specifically for this purpose. Large scale migrations require not only files but system settings to be moved to new machines and Microsoft created this tool for this purpose.

QUESTION 2

Which of the following is designed to infiltrate or damage a computer without the consent of the owner?

A. Shareware

B. Malware

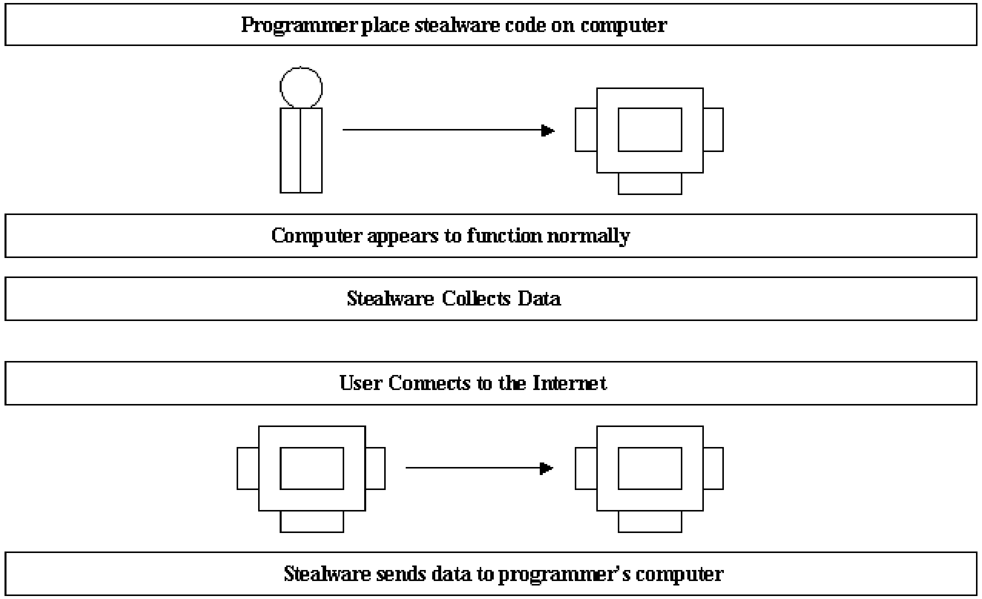
C. Freeware

D. Stealware

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The term malware refers to malicious software, which is a broad class of malicious viruses, including spyware. Malware is designed to infiltrate

or damage a computer without the consent of the owner.
Answer: D is incorrect. Stealware is associated with Web bugs or spyware. It is used by Web sites to affiliate marketing programs. Stealware attributes can be present in peer-to-peer software applications. Spyware, adware, and stealware are similar types of malicious code.
Some Websites are advertised as free and allow information to be downloaded. However, a pop-up window with a disclaimer should appear. The disclaimer discloses information of possible charges or rerouting of the Web site. The users should read the disclaimer to learn what charges are applicable before clicking the advertisement. Otherwise, they will be liable to pay a large sum of money. The working procedure of stealware is shown in the figure below:


Programmer place stealware code on computer
Computer appears to function normally
Stealware Collects Data
User Connects to the Internet
Stealware sends data to programmer's computer

Answer: A is incorrect. Shareware is software designed to use freely or for a limited period available on the Internet. After completing the given time, the user can either purchase it or legally remove it. These types of products are usually offered either with certain features only available when the user has purchased the product, or as a full version but for a limited trial period of time.
Answer: C is incorrect. Freeware is computer software that can be used without paying for it.

QUESTION 3
Which of the following is a circuit board that is used to extend slots for expansion cards and provides the ability to connect additional expansion cards to the computer?

A. Audio/modem riser
B. Secure Digital (SD) card
C. Riser card
D. Communication and Networking Riser (CNR)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Riser card is a circuit board that is used to extend slots for expansion cards and provides the ability to connect additional expansion cards to the computer. These cards are used with LPX motherboards. With the introduction of ATX motherboards, riser cards are rarely used. In ATX motherboards, the expansion cards connect directly to the computer motherboard instead of using riser cards.
Answer: A is incorrect. The audio/modem riser (AMR), also known as an AMR slot, is an expansion slot. It is found on the motherboards of some Pentium III, Pentium 4, and Athlon personal computers. It was designed by Intel to interface with chipsets and provide analog functionality, such as sound cards and modems, on an expansion card. It has two rows of 23 pins each, making a total of 46 pins.
Answer: D is incorrect. Communication and Networking Riser (CNR) is a hardware device developed by Intel. It plugs into the motherboard and holds chips for the functioning of devices such as modems and audio devices. It supports V.90 analog modem, multi-channel audio, phone-line-based networking, and 10/100 Ethernet-based networking. CNR also minimizes electrical noise interference through the physical separation of noise-sensitive elements from the motherboard's communication systems.
Answer: B is incorrect. Secure Digital (SD) card is a non-volatile memory card format used in portable devices such as mobile phones, digital cameras, and handheld computers. SD cards are based on the older MultiMediaCard (MMC) format, but they are a little thicker than MMC cards. Generally an SD card offers a write-protect switch on its side. SD cards generally measure 32 mm x 24 mm x 2.1 mm, but they can be as thin as 1.4 mm. The devices that have SD card slots can use the thinner MMC cards, but the standard SD cards will not fit into the thinner MMC slots. Some SD cards are also available with a USB connector. SD card readers allow SD cards to be accessed via many connectivity ports such as USB, FireWire, and the common parallel port.

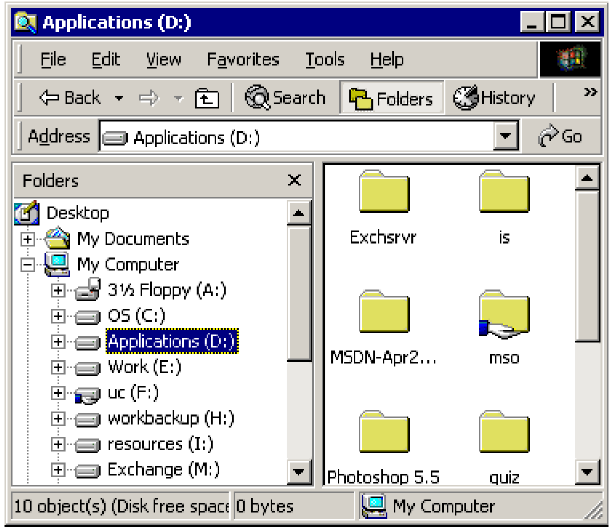
QUESTION 4
Which of the following is a file management tool?

A. Windows Explorer
B. Device Manager
C. MSCONFIG
D. Defrag

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Windows Explorer is a file management tool.
Windows Explorer is a dual-pane window that can be used for file management. File management includes copying, moving, renaming, and searching files and folders. Windows Explorer displays the resources on the system and the tools available in the operating system in a

hierarchical form, in its left window-pane. It displays the contents of the folder that is selected in the left window-pane, in its right window-pane. Windows Explorer can also be used for starting programs or accessing system resources such as a printer.



It can be accessed in Windows through the Start menu as follows:
Start>Programs>Accessories>Windows Explorer
Answer: B and C are incorrect. Device Manager and MSCONFIG are system management tools.

QUESTION 5
Which of the following parts of the computer is built-in to the motherboard?

A. Joystick
B. Mouse
C. Sound card
D. CD-ROM drive

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Sound cards are built-in to the motherboard.
Sound card enables the computer to output sound to audio devices, as well as accept input from a microphone. Most modern computers have sound cards built-in to the motherboard, though it is common for a user to install a separate sound card as an upgrade.

Answer: D is incorrect. CD-ROM is a device used for reading data from a CD. This device is not built-in to the mother board.
Answer: B is incorrect. Mouse is a pointing device that detects two dimensional motion relative to its supporting surface. This device is not built-in to the mother board.
Answer: A is incorrect. Joystick is a device mostly used in gaming. It consists of a handheld stick that pivots around one end, to detect angles in two or three dimensions.

QUESTION 6
You are selecting memory to put in to a laptop. Which of the following types of RAM chips would you most likely select?

A. 72 PIN
B. 240 PIN
C. 184 PIN
D. 144 PIN

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Both MicroDIMM and SO-DIMM come in a 144 pin configuration, and are used for laptops.

QUESTION 7
Which of the following statements does the UK Parliament state in the Computer Misuse Act 1990?
Each correct answer represents a complete solution. Choose two.

A. Unauthorized access to the computer material is punishable by 6 months imprisonment or a fine "not exceeding level 5 on the standard scale".
B. Personal data shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which they are processed.
C. Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage
D. Unauthorized modification of computer material is subject to the same sentences as section 2 offences.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The Computer Misuse Act 1990 is an act of the UK Parliament which states the following statement:
Unauthorized access to the computer material is punishable by 6 months imprisonment or a fine "not exceeding level 5 on the standard scale" (currently 5000).
Unauthorized access with the intent to commit or facilitate commission of further offences is punishable by 6 months/maximum fine on summary conviction or 5 years/fine on indictment.
Unauthorized modification of computer material is subject to the same sentences as section 2 offences.
Answer: B and C are incorrect. These two statements are stated in the Data Protection Act 1998.

QUESTION 8
Which of the following types of parental controls is used to limit access to the Internet contents?

A. Monitoring control
B. Usage management tool
C. Content filter control
D. Bandwidth control

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Content filter control is a type of parental control that is used to limit access to the Internet content.
Answer: A is incorrect. Monitoring control is a type of parental control that is used to track locations nd activities when using the device.
Answer: B is incorrect. Usage management tool is a type of parental control that allows parents to enforce learning time into child computing time.
Answer: D is incorrect. There is no parental control such as bandwidth control.

QUESTION 9
You are working in a Windows network environment. Which of the following accounts/groups have many advanced permissions not needed by occasional users?
Each correct answer represents a part of the solution. Choose two.

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

Correct Answer: CD
Section: (none)

Explanation

Explanation/Reference:
Explanation:
An Administrator user account has full permissions on the computer.
The Power Users group has many advanced permissions not needed by occasional users. Power users can perform any tasks except those reserved for administrators.
Answer: B is incorrect. A Standard user account has a minimal set of permissions. Each account in standard user mode is designed to store a separate set of settings for users. The users are allowed to launch applications, create new documents, and modify basic system configurations.
Answer: A is incorrect. A Guest account is designed to provide temporary access to computers. It does not store user-specific profile settings permanently. This account is disabled by default.

QUESTION 10
You need to alter disk partitions in Windows XP prior to upgrade to Windows Vista. Which Windows utility should you use for this?

A. Disk Defragmenter
B. The Registry
C. Disk Management
D. System Configuration Utility

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Disk Management tool is used to alter, adjust, and configure partitions.

QUESTION 11
Which of the following is used by Wi-Fi Protected Access (WPA) to provide data encryption?

A. IDEA
B. TKIP
C. RSA

D. RC4

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
TKIP (Temporal Key Integrity Protocol) is an encryption protocol defined in the IEEE 802.11i standard for wireless LANs (WLANs). It is designed to provide more secure encryption than the disreputably weak Wired Equivalent Privacy (WEP). TKIP is the encryption method used in Wi-Fi Protected Access (WPA), which replaced WEP in WLAN products.
TKIP is a suite of algorithms to replace WEP without requiring the replacement of legacy WLAN equipment. TKIP uses the original WEP programming but wraps additional code at the beginning and end to encapsulate and modify it. Like WEP, TKIP uses the RC4 stream encryption algorithm as its basis.

QUESTION 12
Mark works as a Network Administrator for NetTech Inc. The company has a Windows 2000 domain-based network. A user working on a Windows 2000 Professional client computer reports that he is unable to access some files on the hard disk. However, he is able to successfully log on and access other files. What should Mark do to resolve the issue?

A. Instruct the user to log off and log on again.
B. Enable the user account on the computer.
C. Check the file permissions on the hard disk drive.
D. Check the hard disk drive using the SCANDISK utility.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In order to resolve the issue, Mark should check the file permissions for the user on the hard disk drive. According to the question, the user is able to access other files on the hard disk. Hence, the most likely cause of the issue is that the user does not have sufficient privileges on those files.
Answer: A is incorrect. Logging off and then logging on will not help resolve the issue.
Answer: D is incorrect. Checking the hard disk drive using the SCANDISK utility will not help, as the issue is related to permissions.
Answer: B is incorrect. According to the question, the user is able to successfully log on to the computer. This indicates that his user account is already enabled. Hence, there is no need to enable it.

QUESTION 13
Which of the following refers to the data rate supported by a network connection or interface?

A. Spam

B. Preboot Execution Environment (PXE)

C. Bandwidth

D. Branding

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Bandwidth is a term that refers to the data rate supported by a network connection or interface.
Bandwidth (or digital bandwidth) is a measurement of how much data can be sent in a period of time. It is a data rate measured in bits. The standard unit of digital bandwidth is bits per second (bps). In radio communication, bandwidth (analogue bandwidth) is the range of frequencies occupied by the radio signals. The standard unit of analogue bandwidth is Hertz (Hz).
Answer: D is incorrect. In Web site designing, branding refers to the look and feel of a Web site. Branding helps in differentiating a site from its competitors and also helps the customer to develop a relationship with the Web site. The look and feel of a Web site comes through logo, fonts, color schemes, and symbols used in the Web site. The overall look of the Web site should be consistent.
Answer: B is incorrect. Preboot Execution Environment (PXE) is an environment to boot computers using a network interface independently of available data storage devices like hard disks or installed operating systems. PXE is also known as Pre-Execution Environment.
Answer: A is incorrect. Spam is a term that refers to the unsolicited e-mails sent to a large number of e-mail users. The number of such e-mails is increasing day by day, as most companies now prefer to use e-mails for promoting their products. Because of these unsolicited e-mails, legitimate e-mails take a much longer time to deliver to their destination. The attachments sent through spam may also contain viruses. However, spam can be stopped by implementing spam filters on servers and e-mail clients.

QUESTION 14
Which of the following slots on a motherboard are best for a video card? Each correct answer represents a complete solution. Choose two.

A. PCI

B. PCIe

C. EISA

D. AGP

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

Explanation:
AGP and PCIe are the best slots for a video card.
PCI Express (PCIe), also known as 3rd Generation I/O (3GIO), is a type of computer bus. It is a new I/O bus technology that has more bandwidth than PCI and AGP slots. It uses two low-voltage differential pairs, at 2.5Gb/s in each direction. It is designed to replace PCI and AGP expansion slots. The bus is available in several different bus widths: x1, x2, x4, x8, x12, x16, and x32. PCIe is able to transfer data in both directions at a time. PCIe hardware will work on operating systems that support PCI.
AGP is a high speed 32-bit bus designed for high performance graphics and video support. It allows a video card to have direct access to a computer's RAM, which enables fast video performance. AGP provides a bandwidth of up to 2,133 MB/second.
Answer: C is incorrect. The Extended Industry Standard Architecture (EISA) is a 32-bit PC expansion bus designed as a superset of a 16-bit ISA bus. The EISA bus is designed to increase the speed and expand the data width of the legacy expansion bus while still supporting older ISA cards. EISA slots are obsolete now.
Answer: A is incorrect. PCIe and AGP slots are better than PCI slot for a video card.

QUESTION 15
Which of the following statements about a smart card are true? Each correct answer represents a complete solution. Choose two.

A. It is a device that contains a microprocessor and permanent memory.

B. It is used to securely store public and private keys for log on , e-mail signing and encryption, and file encryption.

C. It is a device that routes data packets between computers in different networks.

D. It is a device that works as an interface between a computer and a network.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A smart card is a credit card-sized device that contains a microprocessor and permanent memory. It is used to securely store public and private keys for log on, e-mail signing and encryption, and file encryption. To use a smart card, a computer must have a smart card reader attached with it.

QUESTION 16
A customer has come to you wanting upgrade the video card in his laptop. What would you recommend?

A. A PCI Express card

B. Upgrade is not possible

C. A PCMCIA card

D. An AGP Card

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:
Video cards in laptops are built into the motherboard and cannot be upgraded.
Answer: D is incorrect. An AGP card is an older type of video card for PC's.

QUESTION 17
Which of the following cache levels are implemented on microprocessors? Each correct answer represents a complete solution. Choose two.

A. Level 5 (L5) cache
B. Level 2 (L2) cache
C. Level 0 (L0) cache
D. Level 1 (L1) cache

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Level 1 (L1) cache is implemented on microprocessors. The L1 cache is a type of memory implemented inside the microprocessor chip. It is the fastest memory in the computer. It contains the current working set of data and code. Cache memory is used to store frequently used information, so that the processor can access this information without delay.
Level 2 (L2) cache is employed between main memory and L1 cache. The L2 cache contains additional data and code. In old architecture, L2 cache is mounted on the motherboard, which means that it runs at the motherboard's speed. In modern architecture, L2 caches are built directly into the microprocessor.
Answer: A and C are incorrect. There are no such cache levels as level 0 and level 5.

QUESTION 18
You work as a Network Administrator for NetTech Inc. The company has a wireless local area network (WLAN). You want to prevent your wireless access point from being accessed by intruders. What will you do to accomplish the task?

A. Implement auditing.
B. Implement WEP.
C. Implement SSL.
D. Implement IPSec.

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:
In order to prevent your wireless access point from being accessed by intruders, you will have to implement Wired Equivalent Privacy (WEP) on the network. WEP is a security protocol for wireless local area networks (WLANs). It is the most commonly and widely accepted security standard. Almost all the available operating systems, wireless access points, and wireless bridges support this security standard. It has two components, authentication and encryption. It provides security that is equivalent to wired networks for wireless networks. WEP encrypts data on a wireless network by using a fixed secret key. WEP incorporates a checksum in each frame to provide protection against the attacks that attempt to reveal the key stream.
Answer: C is incorrect. Secure Sockets Layer (SSL) is a protocol used to transmit private documents via the Internet. SSL uses a combination of public key and symmetric encryption to provide communication privacy, authentication, and message integrity. Using the SSL protocol, clients and servers can communicate in a way that prevents eavesdropping and tampering of data on the Internet. Many Web sites use the SSL protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with https: instead of http:. By default, SSL uses port 443 for secured communication.
Answer: A is incorrect. Auditing is used to track user accounts for file and object access, logon attempts, system shutdown etc. This enhances the security of the network. Before enabling auditing, the type of event to be audited should be specified in the Audit Policy in User Manager for Domains.
Answer: D is incorrect. Internet Protocol Security (IPSec) is a standard-based protocol that provides the highest level of VPN security.
IPSec can encrypt virtually everything above the networking layer. It is used for VPN connections that use the L2TP protocol. It secures both data and password.
IPSec cannot be used with Point-to-Point Tunneling Protocol (PPTP).

QUESTION 19
What is the maximum cable length to connect a device to an IEEE 1394a port?

A. 12 meters
B. 5 meters
C. 4.5 meters
D. 10 meters

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The maximum cable length to connect a device to an IEEE 1394a port is 4.5 meters.

QUESTION 20

Which of the following identifies a wireless network and is sometimes referred to as a "network name"?

A. BSSID
B. SSID
C. BSS
D. IBSS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
SSID stands for Service Set Identifier. It is used to identify a wireless network. SSIDs are case sensitive text strings and have a maximum length of 32 characters. All wireless devices on a wireless network must have the same SSID in order to communicate with each other.
The SSID on computers and the devices in WLAN can be set manually and automatically. Configuring the same SSID as that of the other Wireless Access Points (WAPs) of other networks will create a conflict.
A network administrator often uses a public SSID that is set on the access point. The access point broadcasts SSID to all wireless devices within its range. Some newer wireless access points have the ability to disable the automatic SSID broadcast feature in order to improve network security. An SSID is sometimes referred to as a "network name." It allows stations to connect to the desired network when multiple independent networks operate in the same physical area.
Answer: A is incorrect. BSSID (Basic Service Set Identifier) is an identifier used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Medium Access Control) address of the wireless protected access point (WPA), whereas in Independent BSS or ad hoc networks, the BSSID is a locally administered MAC address generated from a 46-bit random number. The individual/group bit of the address is set to 0, and the universal/local bit of the address is set to 1.
Answer: C is incorrect. BSS (Basic Service Set) is the basic building block of an IEEE 802.11 wireless LAN. BSS is the collection of stations that can communicate together within an 802.11 WLAN (Wireless Local Area Network). The BSS may or may not include an AP (Access Point) which provides a connection onto a fixed distribution system such as an Ethernet network. There are two types of BSS: Independent Basic Service Set and Infrastructure Basic Service Set.
Answer: D is incorrect. IBSS (Independent Basic Service Set) is an ad-hoc network of client devices that does not require a central control access point. In IBSS, the SSID is chosen by the client device that starts the communication. The broadcasting of the SSID is performed in a pseudo-random order by all devices that are members of the network.

QUESTION 21
You are selecting RAM for a new laptop. Which of the following types of chips should you choose?

A. SIMM
B. RIMM
C. DIMM
D. SO-DIMM

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
SO-DIMM (Small Outline Dual Inline Memory Module) is a common RAM chip used in laptops. Some laptops also use MicroDIMM.
Small Outline Dual Inline Memory Module (SO-DIMM) is a type of memory module that comes in 72 pins and 144 pins. The 72-pin SO-DIMM supports 32-bit transfers, and the 144-pin SO-DIMM supports 64-bit transfers. It was introduced for laptops. SO-DIMMs come in smaller packages, consume lesser power, but are more expensive than DIMMs.
Answer: C is incorrect. Dual Inline Memory Modules are full sized chips used in servers and PC's.

QUESTION 22
Which of the following tools is used to monitor the status of computer security settings and services and to specify the problem using a pop- up notification balloon?

A. Windows Sync Center
B. Windows Aero
C. Windows Defender
D. Windows Security Center

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Windows Security Center is one of the security-related features in Windows Vista. It monitors anti-malware software detection, User-Account Control, several Internet Explorer security settings, and Windows Defender. By default, it displays the following types of security features:
Firewall
Automatic Updating
Malware protection
Other security settings
Windows Security Center is used to monitor the status of computer security settings and services and to specify the problem using a pop-up notification balloon.
Answer: C is incorrect. Windows Defender detects spyware or malware and reports to the user when it is detected.
Answer: B is incorrect. Windows Aero is a high-performance graphical user interface for Windows Vista. It is used to offer premium user

experience that makes it easier to visualize and work with. It is used to provide smoother and more stable desktop experience.
Answer: A is incorrect. Windows Sync Center is used to enable users to keep information synchronized between the following:
Computers and mobile devices, such as digital cameras, music players, mobile computers, etc.
Computers and files stored in network folders (offline files).
Computers and programs that support Sync Center.

QUESTION 23
Which of the following protocols is widely used for setting up and tearing down multimedia communication sessions such as voice and video calls over the Internet (VoIP)?

A. ICMP
B. UDP
C. SIP
D. LDAP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Session Initiation Protocol (SIP), designed by Henning Schulzrinne and Mark Handley in 1996, is a signaling protocol, widely used for setting up and tearing down multimedia communication sessions such as voice and video calls over the Internet (VoIP). Other feasible application examples include video conferencing, streaming multimedia distribution, instant messaging, presence information and online games. The protocol can be used for creating, modifying, and terminating two-party (unicast) or multiparty (multicast) sessions consisting of one or several media streams. The modification can involve changing addresses or ports, inviting more participants, adding or deleting media streams, etc.
The SIP protocol is a TCP/IP-based Application Layer protocol. Within the OSI model, it is sometimes placed in the session layer. SIP is designed to be independent of the underlying transport layer; it can run on TCP, UDP, or SCTP. It is a text-based protocol, sharing many elements of the Hypertext Transfer Protocol (HTTP), upon which it is based, allowing for easy inspection by administrators. SIP clients typically use TCP or UDP (typically on port 5060 and/or 5061) to connect to SIP servers and other SIP endpoints.
Answer: D is incorrect. Lightweight Directory Access Protocol (LDAP) is a protocol used to query and modify information stored within directory services.
Answer: A is incorrect. Internet Control Message Protocol (ICMP) is an integral part of IP. It is used to report an error in datagram processing. The Internet Protocol (IP) is used for host-to-host datagram service in a network. The network is configured with connecting devices called gateways. When an error occurs in datagram processing, gateways or destination hosts report the error to the source hosts through the ICMP protocol. The ICMP messages are sent in various situations, such as when a datagram cannot reach its destination, when the gateway cannot direct the host to send traffic on a shorter route, when the gateway does not have the buffering capacity, etc.
Answer: B is incorrect. User Datagram Protocol (UDP) is often used for one-to-many communications, using broadcast or multicast IP datagrams. Microsoft networking uses UDP for logon, browsing, and name resolution. UDP is a connectionless and unreliable communication protocol. It does not guarantee delivery, or verify sequencing for any datagram. UDP provides faster transportation of data between TCP/IP hosts than TCP.

QUESTION 24

Which of the following is a software program that collects email addresses of users and creates a mailing list to send unwanted emails to the users?

A. Adware

B. Port scanner

C. Malware

D. Spambot

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Spambot is a software program that collects email addresses of users and creates a mailing list to sent unwanted emails to the users.

Answer: C is incorrect. The term malware refers to malicious software, which is a broad class of malicious viruses, including spyware. Malware is designed to infiltrate or damage a computer without the consent of the owner.

Answer: B is incorrect. A port scanner is a software tool that is designed to search a network host for open ports. This tool is often used by administrators to check the security of their networks. It is also used by hackers to compromise the network and systems.

Answer: A is incorrect. Adware is software that automatically downloads and display advertisements in the Web browser without user permission. When a user visits a site or downloads software, sometimes a hidden adware software is also downloaded to display advertisement automatically. This can be quite irritating to user. Some adware can also be spyware.

QUESTION 25

Which of the following Windows Security Center features is implemented to give a logical layer protection between computers in a networked environment?

A. Malware Protection

B. Automatic Updating

C. Other Security Settings

D. Firewall

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Firewall is a security-related feature used to protect the network of an organization from external attacks by intruders.

Answer: B is incorrect. Automatic updating is used to maintain the security and to update the system regularly at a certain time of

interval.
Answer: A is incorrect. The Malware protection feature is used to monitor antivirus software on the user's computer. It performs many unwanted operations on a computer.
Answer: C is incorrect. Other Security Settings is a feature related to User Account Control.

QUESTION 26
Which of the following are touch screen technologies? Each correct answer represents a complete solution. Choose all that apply.

A. Surface Wave
B. Resistive
C. Capacitive
D. Transitive

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Touch screen is a computer display screen that is sensitive to human touch. It allows a user to interact with a computer by touching the icons or graphical buttons on the monitor screen. It is a system that is designed to help users who have difficulty in using mouse or keyboard and is used with information kiosks, computer-based training devices etc. A touch screen panel is attached externally to the monitor that is connected to a serial or Universal Serial Bus (USB) port on a computer. Nowadays, monitors are also available with built-in touch screen technology. There are three types of touch screen technologies:
1.Resistive
2.Capacitive
3.Surface Wave
Answer: D is incorrect. There is no such touch screen technology as Transitive.

QUESTION 27
You are working on a home computer. You have installed Windows Vista on your computer. A friend named Andrew visits your home and he needs to launch a Web browser to check his e-mail. Which of the following user accounts will you allow him to use?

A. Limited account
B. Standard account
C. Administrator account
D. Guest account

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Explanation:
A guest account is a built-in user account that allows a user to operate a computer in the same way as a user with a limited account operates a computer. With this account, a user can log on to a computer, browse the Internet, check e-mails, and use installed applications on the computer. A user with a guest account cannot install or remove programs as well as change the computer's settings in anyway. This account can be enabled on stand-alone computers as well as on those running in workgroups or domains.
Answer: B is incorrect. A Standard user account has a minimal set of permissions. Each account in standard user mode is designed to store a separate set of settings for users. The users are allowed to launch applications, create new documents, and modify basic system configurations.
Answer: C is incorrect. An administrator user account is the least restrictive among all the user accounts that are created on computers running the Windows Vista operating system. This account provides the user complete and unlimited authority to modify settings of a computer. The users with this account can create, change, delete user accounts, make permanent changes to the system settings, and install or remove software and hardware. This account can be configured for stand-alone computers as well as on the computers that are running in workgroups or domains.
Answer: A is incorrect. A limited account is a built-in user account that allows a user to change his account's password and picture, but it does not allow him to change computer settings, install or remove software and hardware, delete files, change system settings, etc. This account is configured on stand-alone computers and on the computers that are running in workgroups or domains.

QUESTION 28
Which of the following are the most likely causes of a virus attack? Each correct answer represents a complete solution. Choose all that apply.

A. Installing an application from an unreliable source

B. Using a floppy, a compact disk, or a pen drive from an unreliable source

C. Downloading a file from an unknown Website

D. Installing a .DLL file from an unreliable source

Correct Answer: ABCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The following are the most likely causes of a virus attack:
Using a floppy, a compact disk, or a pen drive from an unreliable source
Downloading file(s) from an unknown Website
Installing an application or a .DLL file from an unreliable source
A virus is a program code that is written for the destruction of data. This program requires writable media. A virus can infect boot sectors, data files, and system files. A computer virus passes from one computer to another on the network in the same way as a biological virus passes from one person to another.

QUESTION 29
Which of the following types of attacks is often performed by looking surreptitiously at the keyboard or monitor of an employee's computer?

A. Man-in-the-middle attack
B. Buffer-overflow attack
C. Denial-of-Service (DoS) attack
D. Shoulder surfing attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Shoulder surfing attack is often performed by looking surreptitiously at the keyboard or monitor of an employee's computer.
Shoulder surfing is a type of in person attack in which an attacker gathers information about the premises of an organization. This attack is often performed by looking surreptitiously at the keyboard or monitor screen of an employee's computer while he is typing in his password at any access point such as a terminal/Web site. An attacker can also gather information by looking at open documents on the employee's desk, posted notices on the notice boards, etc.
Answer: A is incorrect. Man-in-the-middle attacks occur when an attacker successfully inserts an intermediary software or program between two communicating hosts. The intermediary software or program allows attackers to listen to and modify the communication packets passing between the two hosts. The software intercepts the communication packets and then sends the information to the receiving host. The receiving host responds to the software, presuming it to be the legitimate client.
Answer: B is incorrect. A buffer-overflow attack is performed when a hacker fills a field, typically an address bar, with more characters than it can accommodate. The excess characters can be run as executable code, effectively giving the hacker control of the computer and overriding any security measures set.
Answer: C is incorrect. A Denial-of-Service (DoS) attack is mounted with the objective of causing a negative impact on the performance of a computer or network. It is also known as network saturation attack or bandwidth consumption attack. Attackers make Denial-of-Service attacks by sending a large number of protocol packets to a network. A DoS attack can cause the following to occur:
Saturate network resources.
Disrupt connections between two computers, thereby preventing communications between services.
Disrupt services to a specific computer.
A SYN attack is a common DoS technique in which an attacker sends multiple SYN packets to a target computer. For each SYN packet received, the target computer allocates resources and sends an acknowledgement (SYN-ACK) to the source IP address. Since the target computer does not receive a response from the attacking computer, it attempts to resend the SYN-ACK. This leaves TCP ports in the half-open state. When an attacker sends TCP SYNs repeatedly before the half-open connections are timed out, the target computer eventually runs out of resources and is unable to handle any more connections, thereby denying service to legitimate users.

QUESTION 30
Which of the following buses has a maximum data transfer rate of 2400 Mbps?

A. USB 1.1
B. FireWire 800
C. USB 2.0
D. eSATA

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
External Serial Advanced Technology Attachment (eSATA) is an external Interface and provides hot swappable hard disk drive solution. It is an external interface for Serial Advanced Technology Attachment (SATA) technology. It is designed to support hot-plugging. Hence, it allows users to connect a hard disk drive while the computer is running. eSATA has data transfer rates three times more than USB 2.0 and FireWire 400. Unlike USB and FireWire interfaces, eSATA requires its own power connector. eSATA supports a maximum data cable length of two meters. It has a maximum data transfer rate of 2400 Mbps.
Answer: B is incorrect. FireWire 800 bus has a maximum data transfer rate of 786.432 Mbps.
Answer: C and A are incorrect. Universal Serial Bus (USB) is a high speed bus standard developed by Compaq, IBM, DEC, Intel, Microsoft, NEC, and Northern Telecom. It provides the Plug and Play capability of Windows to external hardware devices. USB supports hot plugging, which means that a USB device can be installed or removed while the computer is running. A single USB port can be used to connect up to 127 peripheral devices, such as CD-ROM drives, tape drives, keyboards, scanners etc. USB 1.1 has a maximum data transfer rate of 12 Mbps and USB 2.0 has a maximum data transfer rate of 480 Mbps.

QUESTION 31
Which of the following data busses is used by a 168-pin Dual Inline Memory Module (DIMM)?

A. 64-bit
B. 128-bit
C. 32-bit
D. 8-bit

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The 168-pin Dual Inline Memory Module (DIMM) uses 64-bit wide data bus.
Answer: D is incorrect. The 30-pin Single Inline Memory Module (SIMM) uses 8-bit wide data bus.
Answer: C is incorrect. The 72-pin Single Inline Memory Module (SIMM) uses 32-bit wide data bus.
Answer: B is incorrect. The 184-pin Rambus Inline Memory Module (RIMM) uses 128-bit wide data bus.

QUESTION 32
Mark purchases a new computer and installs the Windows 2000 Professional operating system on it. He wants to connect the computer to the Internet. Which of the following actions can he take to protect his computer from unauthorized access, adware, and malware?
Each correct answer represents a complete solution. Choose two.

A. Set hidden attributes on his important files.
B. Install all the service packs available for the operating system.
C. Configure a firewall on the computer.
D. Configure auditing on the computer.

Correct Answer: BC
Section: (none)
Explanation

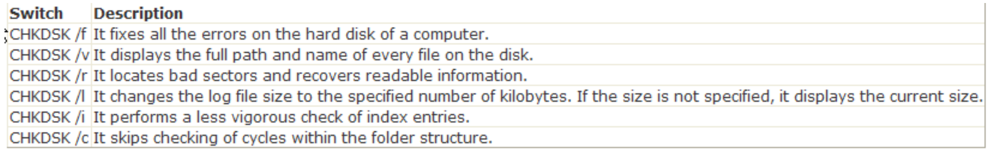
Explanation/Reference:
Explanation:
In order to protect his computer from unauthorized access, adware, and malware, Mark can take the following actions:
Install all the service packs available for the operating system.
Configure a firewall on the computer.

QUESTION 33
You work as a Network Administrator for Tech Perfect Inc. The company has a Windows-based network. You do maintenance work on a Windows 2000 Professional computer. You require to perform the following jobs:
Exhaustive disk checking.
Locate bad sectors (if any).
Recover readable information.
Which of the following commands will you use to accomplish the task?

A. CHKDSK /f
B. CHKDSK /i
C. CHKDSK /r
D. CHKDSK /v

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In order to accomplish the task, you will have to run the following command:
CHKDSK /r
The CHKDSK command verifies the integrity of the hard disk installed on a computer. Using the command with different parameters can resolve a number of issues, which are described as follows:



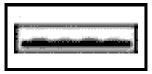
Switch	Description
CHKDSK /f	It fixes all the errors on the hard disk of a computer.
CHKDSK /v	It displays the full path and name of every file on the disk.
CHKDSK /r	It locates bad sectors and recovers readable information.
CHKDSK /l	It changes the log file size to the specified number of kilobytes. If the size is not specified, it displays the current size.
CHKDSK /i	It performs a less vigorous check of index entries.
CHKDSK /c	It skips checking of cycles within the folder structure.

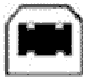
QUESTION 34
Which of the following ports is also known as PS/2?

A. 5-pin DIN connector
B. 4-pin Mini-DIN connector
C. 6-pin Mini-DIN connector
D. USB connector

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The 6-pin Mini-DIN connector is also known as PS/2 port. It uses four of the six pins on a keyboard connector. Pin 1 is used for keyboard data signal, pin 3 is used for grounding, pin 4 has +5 Volt DC, and pin 5 is used for keyboard clock. Pin 2 and pin 6 are not used. The PS/2 6-pin Mini-DIN connector is used to connect a keyboard and mouse.
Answer: A is incorrect. The 5-pin DIN connector is used on a computer that has a Baby-AT form factor motherboard.
Answer: D is incorrect. A Universal Serial Bus (USB) connector is used with the USB cable for connecting various electronic devices to a computer. USB supports a data speed of up to 12 megabits per second. Two types of connectors are used with USB, namely USB-A Type and USB-B Type.


USB-A Type


USB-B Type

Answer: B is incorrect. The 4-pin Mini-DIN connector is used for the S-Video port.

QUESTION 35
Which of the following wireless standards use the frequency of 2.4 GHz? Each correct answer represents a complete solution. Choose three.

A. 802.11b
B. 802.11a
C. 802.11g
D. Bluetooth

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The 802.11 standard refers to a family of standards developed by the IEEE for the wireless LAN technology. This standard specifies a wireless interface between a wireless client and a base station or between two wireless clients. The following 802.11 wireless standards use the frequency of 2.4 GHz:
802.11b
802.11g
Bluetooth
The 802.11b wireless standard applies to wireless LANs and provides transmission speeds of up to 11 Mbps in the 2.4 GHz frequency.
The 802.11g wireless standard applies to wireless LANs and provides transmission speeds of up to 54 Mbps in the 2.4 GHz frequency.
Bluetooth is a standard for short-range radio links between laptops, mobile phones, digital cameras, and other portable devices. Bluetooth devices contain a transceiver chip. The transceiver transmits and receives data in the frequency of 2.45 GHz.
Answer: B is incorrect. The 802.11a wireless standard applies to wireless LANs and provides transmission speeds of up to 54 Mbps in the 5 GHz frequency.

QUESTION 36
What is the maximum resolution that SXGA video technology supports?

A. 1280 x 720
B. 1024 x 768
C. 2560 x 1600
D. 1280 x 1024

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
SXGA stands for Super eXtended Graphics Array. It is a display standard that refers to video adapters. This standard is an enhancement of the standard XGA resolution developed by IBM. It is capable of displaying the resolution of 1280 x 1024 pixels. 1280 refers to horizontal pixels, and 1024 refers to vertical pixels.
Answer: A is incorrect. The WXGA video technology supports a maximum resolution of 1280 x 720.
Answer: C is incorrect. The WQXGA video technology supports a maximum resolution of 2560 x 1600.
Answer: B is incorrect. The XGA video technology supports a maximum resolution of 1024 x 768.

QUESTION 37
Which of the following types of attacks entices a user to disclose personal information such as social security number, bank account details, or credit card number?

A. Replay attack
B. Password guessing attack
C. Phishing
D. Spoofing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Phishing is a type of scam that entice a user to disclose personal information such as social security number, bank account details, or credit card number. An example of phishing attack is a fraudulent e-mail that appears to come from a user's bank asking to change his online banking password. When the user clicks the link available on the e-mail, it directs him to a phishing site which replicates the original bank site. The phishing site lures the user to provide his personal information.
Answer: D is incorrect. Spoofing is a technique that makes a transmission appear to have come from an authentic source by forging the IP address, email address, caller ID, etc. In IP spoofing, a hacker modifies packet headers by using someone else's IP address to hide his identity. However, spoofing cannot be used while surfing the Internet, chatting on-line, etc. because forging the source IP address causes the responses to be misdirected.
Answer: A is incorrect. A replay attack is a type of attack in which attackers capture packets containing passwords or digital signatures whenever packets pass between two hosts on a network. In an attempt to obtain an authenticated connection, the attackers then resend the captured packet to the system. In this type of attack, the attacker does not know the actual password, but can simply replay the captured packet.

Answer: B is incorrect. A password guessing attack occurs when an unauthorized user tries to log on repeatedly to a computer or network by guessing usernames and passwords. Many password guessing programs that attempt to break passwords are available on the Internet. Following are the types of password guessing attacks:
Brute force attack
Dictionary attack

QUESTION 38
When you are configuring a wireless access point, which of the following is broadcasted by default and should be disabled from the security point of view?

A. Wireless Access Protocol (WAP)

B. Service Set Identifier (SSID)

C. MAC address

D. Multicast address

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Service Set Identifier (SSID) is broadcasted by default and should be disabled from the security point of view.
SSID stands for Service Set Identifier. It is used to identify a wireless network. SSIDs are case sensitive text strings and have a maximum length of 32 characters. All wireless devices on a wireless network must have the same SSID in order to communicate with each other. A network administrator often uses a public SSID that is set on the access point. The access point broadcasts SSID to all wireless devices within its range. Some newer wireless access points have the ability to disable the automatic SSID broadcast feature in order to improve network security.
Answer: C is incorrect. Media Access Control (MAC) address is a numerical identifier that is unique for each network interface card (NIC). MAC addresses are 48-bit values expressed as twelve hexadecimal digits, usually divided into hyphen-separated pairs: for example, FF-00-F8-32-13-19. A MAC address consists of two parts. The first three pairs are collectively known as the Organizationally Unique Identifier (OUI). The remaining part is known as device ID. The OUI is administered by IEEE. MAC addresses are also referred to as hardware addresses, Ethernet addresses, and universally administered addresses (UAAs).
Answer: A is incorrect. The Wireless Access Protocol (WAP) is a technology used with wireless devices. The functionality of WAP is equivalent to that of TCP/IP. WAP uses a smaller version of HTML called Wireless Markup Language (WML) to display Internet sites.
Answer: D is incorrect. A multicast address is a single address that refers to multiple network devices. It represents a group of devices on a segment. Membership of a group is dynamic, i.e., devices can join or leave the group as and when required. The Mac address format used by IP for multicasts is 0100.5exx.xxxx, where x is a valid value.

QUESTION 39
Which of the following file attributes are not available on a FAT32 partition? Each correct answer represents a complete solution. Choose two.

A. Hidden

B. Compression

C. Read Only

D. Archive

E. Encryption

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
File attributes such as Compression and Encryption are not available on FAT32 partitions. The following file attributes are available on FAT32 partitions:
Hidden
Read Only
Archive
System
The FAT32 file system is an enhancement of the FAT16 file system. FAT32 can support hard disk drives larger than 2GB (maximum 2TB) without having to use multiple partitions. It is more efficient as compared to 16-bit FAT on larger disks, as FAT32 decreases the cluster size on large hard disk drives, thereby reducing the amount of unused space.
The Compression and Encryption file attributes are available on NTFS partitions.

QUESTION 40
Which of the following statements about SRAM are true? Each correct answer represents a complete solution. Choose two.

A. SRAM is used for main memory.

B. SRAM is faster than DRAM.

C. SRAM is used for cache memory.

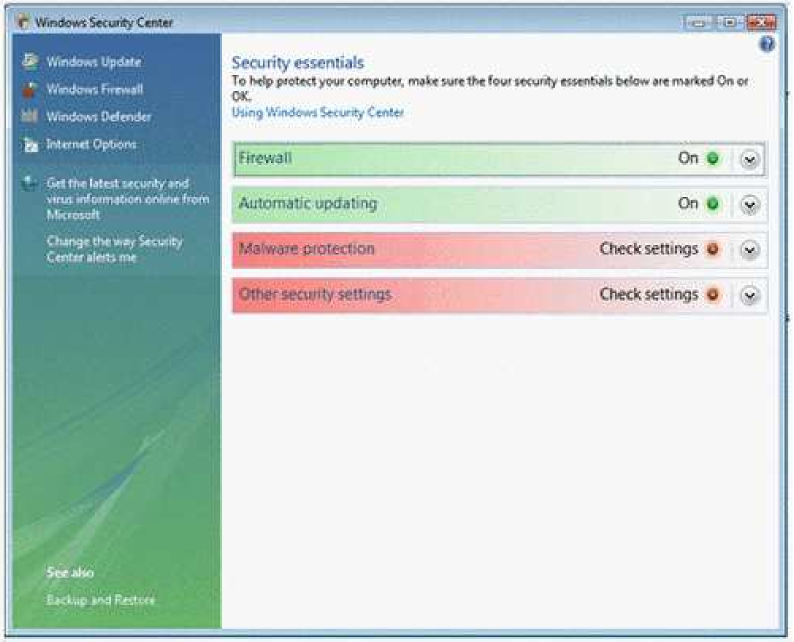
D. SRAM is used for permanent storage of information and is also known as ROM.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

Explanation:
Static Random Access Memory (SRAM) is used for a computer's cache memory and as part of the random access memory digital-to-analog converter on a video card. Unlike DRAM, SRAM does not have to be periodically refreshed. SRAM retains data bits in its memory as long as power is being supplied. SRAM is significantly faster and more expensive than DRAM.

QUESTION 41
You work as an Office Assistant in Tech Perfect Inc. All computers in the company run the Windows Vista operating system. Some users report you that their systems display a notification and put a Security Center icon in the notification area. You check the issue and experience that the Internet settings or User Account Control settings are changed to a security level which is not recommended. You open Windows Security Center. Mark the option that you will choose to check the Internet security settings and User Account Control settings.



Security essentials

To help protect your computer, make sure the four security essentials below are marked On or OK.

Using Windows Security Center

Firewall On ●

Automatic updating On ●

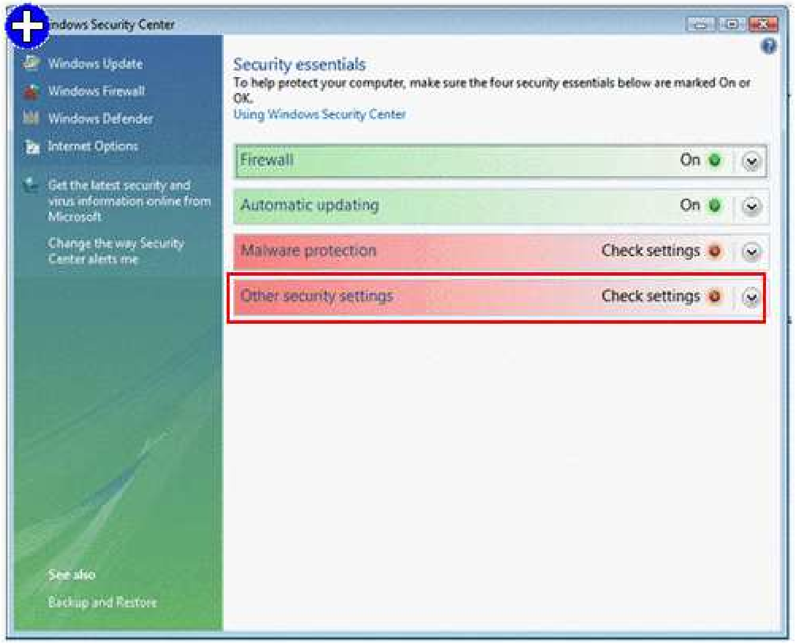
Malware protection Check settings ●

Other security settings Check settings ●

A.
B.
C.
D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:


ndows Security Center
Windows Update
Windows Firewall
Windows Defender
Internet Options
Get the latest security and virus information online from Microsoft
Change the way Security Center alerts me
See also
Backup and Restore
Using Windows Security Center

Security essentials

To help protect your computer, make sure the four security essentials below are marked On or OK.

Firewall On

Automatic updating On

Malware protection Check settings

Other security settings Check settings

Windows Security Center is included in Windows Vista as a consumer-based application. It has
Explanation: numerous security-related
features and settings. By default, there are four different types of security features in Windows Security Center as follows:
Firewall: It is implemented to provide a logical layer protection among computers in a networked environment. It ensures that only specified applications and services are able to connect to the computer.
Automatic updating: This feature is used to install new updates automatically.
Malware protection: Anti-malware is installed to protect the operating system from the installation of malware.
Other security settings: Internet Security Settings and User Account Control are included in other security settings.
Windows Security Center is used to monitor and manage security settings.

QUESTION 42

Which of the following AT Attachment (ATA) standards supports transfer mode UltraDMA/133?

A. ATA-7

B. ATA-5

C. ATA-6

D. ATA-4

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The AT Attachment-7 (ATA-7) standard supports transfer mode UltraDMA/133. With the market introduction of Serial ATA, the ATA is sometimes referred to as Parallel ATA (PATA).

QUESTION 43
Which of the following are Internet standard protocols for email retrieval? Each correct answer represents a complete solution. Choose two.

A. IMAP4

B. POP3

C. SMTP

D. SNMP

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:
IMAP4 and POP3 protocols are Internet standard protocols for email retrieval.
Internet Message Access Protocol 4 (IMAP4) is an e-mail message retrieval protocol that allows e-mail clients to retrieve e-mail messages from e-mail servers.
Post Office Protocol version 3 (POP3) is a protocol used to retrieve e-mails from a mail server. It is designed to work with other applications that provide the ability to send e-mails. POP3 is mostly supported by the commercially available mail servers. It does not support retrieval of encrypted e-mails. POP3 uses port 110.
Answer: D is incorrect. Simple Network Management Protocol (SNMP) is a part of the TCP/IP protocol suite, which allows users to manage the network. SNMP is used to keep track of what is being used on the network and how the object is behaving.
Answer: C is incorrect. Simple Mail Transfer Protocol (SMTP) is a protocol for sending e-mail messages between servers. E-mailing systems use this protocol to send mails over the Internet. SMTP works on the application layer of the TCP/IP or OSI reference model. The SMTP client typically initiates a Transmission Control Protocol (TCP) connection to the SMTP server on the well-known port designated for SMTP, port number 25. However, e-mail clients require POP or IMAP to retrieve mails from e-mail servers.

QUESTION 44
You have a customer who wants to move files and settings from an old PC to a new one she is buying. What tool do you recommend?

A. Windows Explorer

B. User State Migration Tool

C. Disk Management

D. File and Settings Transfer Wizard

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The files and settings wizard is made specifically for home users to transfer files and settings from an old PC to a new one.
Answer: B is incorrect. The User State Migration Tool is for IT administrators to handle large scale deployments.

QUESTION 45
How many devices can be connected to an IEEE 1394 port?

A. 1

B. 63

C. 256

D. 127

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
An IEEE 1394 port can connect upto 63 devices. This port is also known as FireWire.

QUESTION 46
An ISP hosting a Web site should be protected against a copyright infringement regarding the contents that are posted on the Web site. Which of the following protects an ISP from liability for copyright infringement?

A. Digital Millennium Copyright Act

B. InetLoad

C. Copyright law

D. Trademark

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Digital Millennium Copyright Act protects an ISP against a copyright infringement regarding the contents of a Web site that is being hosted by the ISP.
Answer: B is incorrect. InetLoad is a Microsoft utility that is used to measure the performance of a Web application when it is being bombarded with hits from all sides. It is a free utility that helps site administrators to stress test their applications by simulating simultaneous access by thousands of Internet users.
Answer: C is incorrect. A copyright is a form of intellectual property, which secures to its holder the exclusive right to produce copies of his or her works of original expression, such as a literary work, movie, musical work or sound recording, painting, photograph, computer program, or industrial design, for a defined, yet extendable, period of time. It does not cover ideas or facts. Copyright laws protect intellectual property from misuse by other individuals.
Answer: D is incorrect. A trademark is a mark that is used by a company to distinguish its products from those of other companies. There are various ways a company uses its trademark to distinguish its products from others. It can use words, letters, numbers, drawings, pictures, and so on, in its trademark.

QUESTION 47
Which of the following protocols transmits error messages and network statistics?

A. ICMP
B. NNTP
C. DHCP
D. TCP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
ICMP transmits error messages and network statistics.
Internet Control Message Protocol (ICMP) is an integral part of IP. It is used to report an error in datagram processing. The Internet Protocol (IP) is used for host-to-host datagram service in a network. The network is configured with connecting devices called gateways. When an error occurs in datagram processing, gateways or destination hosts report the error to the source hosts through the ICMP protocol. The ICMP messages are sent in various situations, such as when a datagram cannot reach its destination, when the gateway cannot direct the host to send traffic on a shorter route, when the gateway does not have the buffering capacity, etc.
Answer: D is incorrect. Transmission Control Protocol (TCP) is a reliable, connection-oriented protocol operating at the transport layer of the OSI model. It provides a reliable packet delivery service encapsulated within the Internet Protocol (IP). TCP guarantees the delivery of packets, ensures proper sequencing of data, and provides a checksum feature that validates both the packet header and its data for

accuracy. If the network corrupts or loses a TCP packet during transmission, TCP is responsible for retransmitting the faulty packet. It can transmit large amounts of data. Application-layer protocols, such as HTTP and FTP, utilize the services of TCP to transfer files between clients and servers.
Answer: B is incorrect. NNTP stands for Network News Transfer Protocol (NNTP). It is a simple ASCII text-based protocol used to post, distribute, and retrieve network news messages from NNTP servers and NNTP clients on the Internet.
Answer: C is incorrect. Dynamic Host Configuration Protocol (DHCP) is a TCP/IP standard used to dynamically assign IP addresses to computers, so that they can communicate with other network services. It reduces the complexity of managing network client IP address configuration. A DHCP server configures DHCP-enabled client computers on the network. It runs on servers only. It also provides integration with the Active Directory directory service.

QUESTION 48
You are responsible for security at a hospital. Since many computers are accessed by multiple employees 24 hours a day, 7 days a week, controlling physical access to computers is very difficult. This is compounded by a high number of non employees moving through the building. You are concerned about unauthorized access to patient records. What would best solve this problem?

A. The use of CHAP.
B. Time of day restrictions.
C. The use of smart cards.
D. Video surveillance of all computers.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Smart cards are a physical device that is needed to logon to a computer. This would mean that each person would have to have a smart card and a username/password to access any hospital computers.
Answer: D is incorrect. If there is a security breach, video surveillance might help catch the perpetrator, but it won't prevent the breach.
Answer: A is incorrect. Challenge Handshake Authentication Protocol, will not help prevent unauthorized access to computers.
Answer: B is incorrect. A hospital requires 24 hour a day access to patient data. Time of day restrictions would not work.

QUESTION 49
Which of the following interfaces is the current standard for digital LCD monitors?

A. DVE
B. SVGA
C. VGA
D. DVI

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
DVI interface is the current standard for digital LCD monitors.
DVI stands for Digital Visual Interface. It is a standard for high speed, high resolution digital display invented by Digital Display Working Group (DDWG). DVI accommodates analog and digital interfaces with a single connector. New video cards have DVI as well as VGA ports built into them. Most of LCD monitors come with a 15-pin VGA connection cable, even if they are capable of handling digital signals coming from DVI connections. However, some monitors come with both types of cables. DVI has three main categories of connectors. They are: DVI-A, DVI-D, and DVI-I. DVI-A is an analog-only connector, DVI-D is a digital-only connector, and DVI-I is an analog/digital connector. DVI-D and DVI-I connectors are of two types: single link and dual link. DVI supports UXGA and HDTV with a single set of links. Higher resolutions such as 1920 x 1080, 2048 x 1536, or more can be supported with dual links.
Answer: C and B are incorrect. VGA and SVGA are old standards for monitors. A VGA or SVGA interface is a 15-pin, three rows, female connector, on the back of a PC used for connecting monitors.
Answer: A is incorrect. There is no such interface standard for digital LCD monitors as DVE.

QUESTION 50
Which of the following are the Disk Management tools? Each correct answer represents a complete solution. Choose all that apply.

A. CHKDSK
B. DEFRAG
C. Device Manager
D. FORMAT

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The following are the disk management tools:
FORMAT
CHKDSK
DEFRAG

QUESTION 51
Which of the following is a technology that allows you to hear and watch video clips as soon as they start downloading from the Web site, instead of waiting for the download to complete?

A. Session Initiation Protocol
B. HTTP streaming
C. Streaming media
D. Slipstreaming

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Streaming media is a technology that allows you to hear and watch video clips as soon as they start downloading from the Web site, instead of waiting for the download to complete.
Answer: B is incorrect. HTTP streaming is a simple mechanism for sending data from a Web server to a Web browser in response to an event. Every time a seek operation is performed, the media player makes a request to the server side script with a couple of GET variables. One is the file to play and one is the start position. The server side script then starts the video from the offset given. For example, after starting the video, a user can jump directly to any part in the video without having to wait until it is loaded.
Answer: A is incorrect. Session Initiation Protocol (SIP), designed by Henning Schulzrinne and Mark Handley in 1996, is a signaling protocol, widely used for setting up and tearing down multimedia communication sessions such as voice and video calls over the Internet (VoIP).
Answer: D is incorrect. Slipstreaming is a process of integrating service pack updates into the Windows XP Professional setup files. The slipstreaming process eliminates the need of deploying service pack update on each computer separately.

QUESTION 52
Which of the following methods is based on the user's roles and responsibilities?

A. System access control
B. Role-based access control
C. Discretionary access control
D. Mandatory access control

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Role-based access control method is based on the user's roles and responsibilities.
Role-based access control (RBAC) is an access control model. In this model, a user can access resources according to his role in the organization. For example, a backup administrator is responsible for taking backups of important data. Therefore, he is only authorized to access this data for backing it up. However, sometimes users with different roles need to access the same resources. This situation can also be handled using the RBAC model.
Answer: C is incorrect. Discretionary access control (DAC) is an access policy determined by the owner of an object. The owner decides who should be allowed to access the object and what privileges they should have.
Answer: D is incorrect. Mandatory access control uses security lablel system.
Answer: A is incorrect. There is no access control method such as System access control.

QUESTION 53
Which of the following Acts of the Parliament of United Kingdom consists of the following features: Define Agency records subject to disclosure Summarize mandatory disclosure procedures Permit nine exemptions to the statute

A. Data Protection Act 1998
B. Digital Millennium Copyright Act
C. Freedom of Information Act 2000
D. Computer Misuse Act

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Freedom of Information Act 2000 is an Act of the Parliament of the United Kingdom. It is the implementation of freedom of information legislation in the United Kingdom on a national level. It is an Act of Parliament that introduces a public "right to know" in relation to public bodies. The Act implements a manifesto commitment of the Labor Party in the 1997 general election. The final version of the Act is believed to have been diluted from that proposed while Labor was in opposition. The full provisions of the act came into force on 1 January 2005.
The Act is the responsibility of the Lord Chancellor's Department. The Act led to the renaming of the Data Protection Commissioner, who is now known as the Information Commissioner. The Office of the Information Commissioner oversees the operation of the Act. The Freedom of Information Act 2000 includes the following features:
It specifies Agency records subject to disclosure.
It summarizes mandatory disclosure procedures.
It permits nine exemptions to the statute.
Answer: A is incorrect. The Data Protection Act 1998 (DPA) is a United Kingdom Act of Parliament, which defines UK law on the processing of data on identifiable living people. It is the main piece of legislation that governs the protection of personal data in the UK. Although the Act does not mention privacy, in practice it provides a way in which individuals can control information about themselves. Most of the Act does not apply to domestic use. Anyone holding personal data for other purposes is legally obliged to comply with this Act, subject to

some exemptions. The Act defines eight data protection principles, which are as follows:
1.Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
at least one of the conditions in Schedule 2 is met, and
in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2.Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3.Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4.Personal data shall be accurate and, where necessary, kept up to date.
5.Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6.Personal data shall be processed in accordance with the rights of data subjects under this Act.
7.Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8.Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.
Answer: D is incorrect. The Computer Misuse Act 1990 is an act of the UK Parliament which states the following statement:
Unauthorized access to the computer material is punishable by 6 months imprisonment or a fine "not exceeding level 5 on the standard scale" (currently 5000).
Unauthorized access with the intent to commit or facilitate commission of further offences is punishable by 6 months/maximum fine on summary conviction or 5 years/fine on indictment.
Unauthorized modification of computer material is subject to the same sentences as section 2 offences.
Answer: B is incorrect. The Digital Millennium Copyright Act (DMCA) is a United States copyright law that implements two 1996 treaties of the World Intellectual Property Organization (WIPO). It criminalizes production and dissemination of technology, devices, or services intended to circumvent measures (commonly known as digital rights management or DRM) that control access to copyrighted works.
It also criminalizes the act of circumventing an access control, whether or not there is actual infringement of copyright itself. In addition, the DMCA heightens the penalties for copyright infringement on the Internet.

QUESTION 54
Which of the following connectors are used to connect a keyboard to the computer? Each correct answer represents a complete solution. Choose three.

A. USB connector
B. Six-pin mini-DIN connector
C. Five-pin DIN connector
D. Nine-pin D type male connector

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The following connectors are used for keyboards:
Five-pin DIN connector
Six-pin mini-DIN connector
USB connector
Five-pin DIN connectors are used on the computers with a Baby-AT form factor motherboard.
Six-pin mini-DIN connectors are used on PS/2 systems and most computers with LPX, ATX, and NLX motherboards.

QUESTION 55
Which of the following resolutions is supported by the SVGA video technology?

A. 640 x 480
B. 640 x 200
C. 800 x 600
D. 1024 x 768

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The SVGA video technology supports the resolution of 800 x 600, where 800 refers to the number of pixels from side to side across the screen, and 600 refers to the number of pixels vertically from top to bottom.
Answer: A is incorrect. The VGA video technology supports the resolution of 640 x 480 with 16 colors.
Answer: B is incorrect. The CGA video technology supports the resolution of 640 x 200 with 2 colors.
Answer: D is incorrect. The XGA video technology supports the resolution of 1024 x 768.