SYSTEM SECURITY AND COMPUTER CRIMES

MULTIPLE CHOICE QUESTIONS
DATA INTEGRITY AND SECURITY

1. What have caused the rise in computer crimes and new methods of committing old computer crimes?
    a. Increased use of computer and expansion of the internet and its services.
    b. New security methods of detecting computer crimes.
    c. Creation of new software.
    d. World Wide Web.

2. What has become more important because of the increased use of computers, the internet and WWW.
    a. Natural Disasters
    b. Hardware Malfunctions
    c. Data integrity and data security
    d. Malicious deletions.

3. Accurate and complete data enters the system for processing and remains accurate thereafter, is said to have:
    a. Integrity
    b. Security
    c. Viruses
    d. Accidental deletion.

4. Inaccurate data entry, worms and viruses, fraud and Hardware malfunction are ways in which what are comprised:
    a. Data Security
    b. Users
    c. Software
    d. Data Integrity

5. What is the difference between Data Integrity and Data Security?
    a. Limiting physical access to computer systems; assigning passwords to users.
    b. Consistent, accurate and reliable data; protection of data from unauthorized access.
    c. Encryption; Audit trails
    d. Distributing work to preserve integrity; installing system passwords

6. Two ways data can be secured are:
    a. Physical and Software safeguards.
    b. Use of Passwords and Electronic Doors
    c. Use of Monitoring systems and Storage of data in another building.
    d. Encryption of data and protection of hardware.

7. What is the difference between Physical Data security and Software-based data security?
    a. Physical data security deals with the protection of data while Software-based data security deals with ensuring only authorized personnel are allowed access to the buildings.

    b. Software-based Data security deals with the prevention of unauthorized used of computer files while physical data security deals with the protection of hardware and software from accidental or malicious damage, destruction or theft.

    c. Physical data security deals with the installation of burglar alarms while software-based data security deals with issuing of passwords to users.

    d. Software-based data security deals with issuing passwords for computer systems while physical data security deals with outer building security.

SYSTEM SECURITY AND COMPUTER CRIMES

8. Listed below are methods used to protect data using physical data security. Answer each method in the space provided:
    a. Only allow authorized personnel access to computer facilities. Its goals is:

       ……..

    b. It eliminate or reduces:

       …….

    c. Name three methods used to enforce this:

        i. …….
        ii. …….
        iii. …….

    d. Outer Structural Security entails: …….

       ……..

    e. Storing data in another building or location. This physical backup is used in case of …….

    f. Distributing Work to a number of employees instead of just one, so no one employee has access to …….

    g. Long term storage of data is known as…… this type of data is stored on devices such as……..,

       …… or …….

9. Some of the most common software safeguards are:
    a. Passwords for ……..

    b. Passwords for …….. providing entry to different levels of ……in a database or computer storage system.

    c. Audit trails or access logs this involves the computer tracking users who access data …….. or how …… to easily track breach of security.

    d. Encryption- this is the encoding of data during ……or ……. So it is not understood by unauthorized persons without the ……..

    e. Firewall – a ……. , ……. Or a combination of both that …… information coming through your computer systems. Firewalls can perform …… and …… functions that record all access attempts to and from a network. Two popular firewall software are …… and …… Firewalls protect system from:

        i. …….. someone is able to connect to your computer and control it in some form.
        ii. …….
        iii. ……..
        iv. ……..

10. Anti-virus software is a special type of software used to remove or inactivate know viruses from a computer's hard disk, floppy disk or memory stick.
    a. True
    b. False

11. Worms and Viruses are programs that can cause destruction to data and software, but they differ on how they spread and function.
    a. True
    b. False

12. What is a Worm?
    a. A weakness in security system that never copies itself into a computer's memory until no more space is left.
    b. A program that uses computer networks and security holes to copy itself in the computer memory until no more memory is left.
    c. Attaches itself to e-mails.
    d. Corrupts or replaces boot sector instructions.

13. Draw a line to match the most common types of viruses to their definitions:

a. File Virus	corrupts or replaces instructions in the boot sector preventing the OS from loading properly thus stopping the Computer from powering up.
b. Trojan Horses	infects program files
c. E-mail Virus	a computer program that places destructive code in programs such as games to erase either hard disk or programs on disk.
d. Boot-Sector Virus	comes as an attachment to an e-mail or as the e-mail itself.

14. How are viruses spread?
    a. Through Firewalls
    b. Downloading infected programs and files from internet.
    c. Garbled information.
    d. Install anti-virus.

15. How do users prevent and protect themselves against viruses?
    a. Do not open e-mail attachments, use an OS that has virus security features, scan other users' media storage devices before using them on your computer.
    b. Missing Files or folders should be deleted.
    c. Files with weird and obscene messages should be stored.
    d. Delete unwanted SPAM from your computer.