COMPUTER VIRUSES, WORMS AND BUGS

Computer viruses are computer programs that silently replicate/reproduce themselves on a storage media without the computer user realizing it and negatively affect the functionality of your computer. Viruses are therefore malicious software programs (malware) that aim at damaging or interfering with regular performance of other programs in the computer.

A virus is a computer program/code that can copy itself and infect a computer without permission or knowledge of a user.

A computer program/code specifically designed to damage or cause irregular behavior in other programs on a computer. It is designed to infect and affect the computer's performance negatively.

A virus can only spread from one computer to another when its host is taken to the uninfected computer or if the computers are connected to the same network. For example; a virus can be spread if the author sent it over the internet or a network or if it is carried on a removable medium such as a floppy diskette, CD, flash disk etc.

Viruses are sometimes confused with computer worms and Trojan horses. A worm can spread itself to other computers without needing to be transferred as a part of a host, and a Trojan horse is a file that appears harmless until executed.

With the advent (coming) of the internet connection and usage of LANs, computer viruses have

become the most terrifying problem in the usage of ICT. This is because a virus can be spread through E-mails; information shared over the internet and locally shared documents over LANs.

EXAMPLES OF COMPUTER VIRUS SCANNING SOFTWARE

These include;

- Norton Antivirus software
- McAfee Virus Scan
- AVG Antivirus
- Avast Antivirus
- Panda Antivirus
- Dr. Solomon Antivirus Toolkit
- Web scan antivirus
- Kaspersky Antivirus
- Avira Antivirus
- Bit Defender Antivirus
- Smadav Antivirus
- Thunder byte antivirus
- F-secure antivirus
- USB disk security

DISASTERS CAUSED BY VIRUS.

- Damaging programs/software
- Deleting files/data on storage devices
- Formatting the hard disk.
- Boot failure
- Take up/ fill up computer memory
- Causes system crashes.

- Corruption of files
- Slows down the speed of the computer

TYPES OF VIRUSES

There are many software codes regarded as computer viruses that can cause damage to computer systems. They include:-

- Boot sector viruses
- File viruses
- Resident virus
- Non-Resident virus
- Macro virus
- Polymorphic virus
- Hoax viruses
- Trojan horses
- Backdoors
- Worms
- Hoax
- Key loggers
- Jokers
- Partition sector viruses
- Test viruses
- Logic/Time Bombs
- Multipartite viruses

Boot sector viruses

This destroys the booting information on the computer or storage devices. It affects the booting files and causes failure in booting.

File infector viruses

These attach themselves to computer files. They usually delete files or cause erratic behaviors in the file system.

Hoax viruses

They are usually lies; they don't exist in real sense. They only exist in the imagination of the press and public. They don't exist despite the rumor of their distribution and creation. The rumour about their creation and spread is usually spread through e-mails or the press.

Trojans/ Trojan horse

This is a small program code hidden within legitimate software. The software continues to work normally until such a time when they are activated to cause trouble. A Trojan horse does not have the capacity to replicate (copy) itself like a worm or a virus. The program does irritating actions like flickering of the screen and the cursor disappearing. Some of these are failed or incomplete computer games.

Worms

This sticks in the computer memory and re-writes (replicate) itself in the memory until it can't multiply anymore. This causes the computer to stop working because the memory is full.

Backdoors

This may be a Trojan or a worm that allows hidden access to a computer system.

Droppers

These are programs that have been written to perform useful tasks like compressing files, previewing video clips etc. but end up introducing viruses in the system in the process of performing their functions.

Failed virus

These are viruses that have failed to meet their goals. This is mainly due to poor programming by the author/designer or is intercepted by a real virus. They are common on the internet when downloading software.

Packagers

These hide the existence of a virus from virus guard by masking some codes around the actual software programs. It is only when a virus has appeared that you realize the software had a virus.

Test virus

These are simply written to test some virus guard or anti-virus software. They are not harmful, just for learning purposes only.

Time bombs

A program code that's activated in conjunction with predetermined days/events. For example,

Valentines, Fools' Day, Friday 13th etc. These use logical calculations to determine their trigger days.

A virus or a Trojan may have a virtual logic in it.

Jokes

A joke is a harmless program that does amusing things on the screen. E.g. Messages like-"Your computer is about to explode in five minutes, please run away……" These messages appear and disappear in few seconds.

The following viruses are classified according to the way they hide.

- **Boot Sector Viruses**

The boot sector is the first section on a floppy diskette. It contains vital information about a diskettes logical set up. When a virus infects a diskette, it alters this information or relocates it elsewhere on the diskette. This causes the computer to display messages like "Non systems" or "the diskette is not formatted".

- **File infector Viruses**

This appends itself or inserts itself into program files like those, which have extensions .exe, .com; such that when these files are run, the virus attacks other executable files either directly or indirectly. It affects the memory of the computer and whenever the host file is executed, it attacks other files because it uses the infected memory space.

- **Partition Sector Viruses**

This is the first sector on a hard disk which contains information about the disk specifications like the number of sectors and tracks in each partition, where DOS partition starts.

When a partition sector virus attacks a computer, it modifies the code located here, causing the computer not to boot fully.

- **Overwriting Viruses**

These infect files by overwriting the entire or part of a file thereby causing the file not to execute or work as it is supposed to do. These are normally DOS based.

- **Macro Viruses**

With the introduction of macro programming languages in some applications, macro viruses have emerged. These can cause some toolbar icons to work differently. Macro viruses are common in Microsoft word documents.

- **Companion Viruses**

A computer virus works by creating different file names with an extension .com similar to the executable file with the .exe extension, such that it can be run first and pass control to the actual program file with the .exe extension.

This is because when running programs under DOS, DOS will prefer to run a file with the .com extension first rather than with .exe extension.

- **Multipartite Viruses**

These are viruses that use a combination of techniques to infect the different executable files, boot sectors and or partition sectors.

They are normally difficult to trap.

SOURCES OF VIRUSES

Viruses spread in various ways but the most common ways are:-

- **Fake Games**

Computers games are a common source of viruses because most games are irresistible. Virus designers design fake games and attach virus onto them. Once a game is executed, a virus is run and activated. These games keep infecting systems as they are installed. Such games have “irresistible” names like HOTSEX.EXE, JACKPOT.COM, and ROMANCE.EXE etc.

- **Contaminated systems**

Contaminated computer systems can spread virus if used freely. For example, installation diskettes for a particular application program can introduce viruses on to a system whenever that application is installed. There by spreading the virus. Itis also common for pirated software.

- **Freeware and shareware**

These software programs are usually given/downloaded free of charge. These are good grounds for distributing viruses.

Freeware are software programs which are usually distributed on line free of charge while shareware refers to those software programs, which can be shared freely amongst the users.

- **Legitimate Software Updates**

Software may get a virus from software house during programming by unscrupulous virus authors or during the distribution say through a network, where they get viruses from the wild viruses across the internet.

- **Pirated software**

The use of pirated software introduces the risk that the software may be contaminated by virus code or amended to perform some other destructive function which may affect the system. Pirated software is that which was copied illegally with an aim of making profit

WAYS OF SPREADING VIRUSES

Viruses are commonly spread or activated in 3 basic ways:

- Opening an infected file
- Running an infected program
- Starting up the computer with an infected floppy diskette
- Use of infected storage devices like floppy diskettes, hard disk etc.
- Through E-mails or distributed maliciously through the internet.
- Through downloads from the internet especially free ones
- Through freeware and shareware.

SYMPTOMS OF VIRUSES

- Unfamiliar graphics or quizzical messages appearing on screens.
- Programs taking longer than usual to load.
- Disk accesses seeming excessive for simple tasks
- Unusual error messages occurring more frequently
- Less memory available than usual
- Access lights turning on for non-referred devices.
- Programs and files disappearing mysteriously.
- Computer indicating that the storage devices are full.

* Any evidence of these or similar events should be an immediate cause for concern to isolate the PC at once and investigate.

PRECAUTIONS TO GUARD AGAINST VIRUSES (control measures).

- Ensure that there are regulations and a policy on the usage of computers and their protection (e.g.no foreign diskettes unless first scanned)
- Ensure that the e-mails are from a trusted source before opening them or e-mail attachments
- Avoid opening e-mails before scanning them for viruses
- Install latest anti -virus utility and update its virus definitions frequently for detecting and removing viruses.
- Never start up a PC with a floppy diskette in the drive.
- Scan all floppy drives and files for possible virus infection before operating them.

- Write protect the recovery disk before using it.
- Back up important files regularly.
- Activating firewalls.
- Sensitizing users about dangers of a computer virus.
- Avoid downloading e-mail attachments before scanning them.
- Never install programs you are not sure of.
- Limit access by using passwords.
- Penalizing offenders who install and download unlicensed software programs.

* An anti -virus utility is a program that prevents, detects and removes viruses from a computer's memory or storage devices.

SAMPLE QUESTIONS:

1(a) Explain what's meant by a computer virus?

(b). State two precautions which should be taken to prevent viruses from affecting computers.

1(a) What is a virus?

(b) Outline four common ways in which viruses are spread.

(c). State four ways used to protect your computer Vs viruses

(d). Name any 3 virus scanning software.

(e). State 3 symptoms of viruses.

(f). Mention 2 ways in which a computer can be infected by a virus.

BUGS

A computer bug is an error in a computer system which causes undesirable results or unwanted procedures.

A bug error can be both software and hardware problems.

The millennium bug for example, was a hardware based error, which dealt/affected the computer clock.

NB: Every computer contains two types of clocks i.e.

- The hardware clock, which is in-built also called the RTC (Real Time Clock).

- Virtual clock/system clock.

The RTC runs continuously whether the computer is on or off and the system clock is a 24hour timer, which only exist when the computer is running. Therefore, it is the operating system that uses the BIOS to read the RTC and track independently.

The millennium bug existed when programmers anticipated that computers may fail to recognize the year 2000. It is the Bios provided had a prefixed '19' and it would read the year '2000' as 1900. This is a code error (bug).

COMMON COMPUTER BUGS

1. DIVIDE BY ZERO.

In programming, am integer divided by zero causes a program to terminate or as in the case of floating point (numerical representation system in which a string of digits represents a real number) numbers may result in a special not a number.

2. NULL POINTER DEFERENCE

A null pointer has a reserved value often but not necessarily the value zero, indicating that it refers to no object.

3. INFINITE LOOPS

A sequence of introductions in a computer program which loops endlessly either due to the loop having no terminating condition or having one that can never meet.

3. ARITHMETIC OVERFLOW AND UNDERFLOW

4. EXCEEDING ARRAM BOUNDS.

5. DEAD LOCK.

6. BUFFER FLOW

7. USING AN UNINITIALISED VARIABLE.

EFFECTS OF THE COMPUTER BUG (Disadvantages).

- May lead to the program crash of freeze leading to the demand of services.
- Some bugs (errors) qualify as security bugs and may enable a malicious user to bypass access controls in order to obtain unauthorized privileges.
- In computer controlled machines, bug may bring system failure and result of the computer failing execute positive commands.

PREVENTION.

Bugs are a consequence of the human factors in the programming tasks. They cause from oversights made by computer programmers during design coding and data entry.

The software industry has put much effort into finding methods for preventing bugs in programming which include:-1. PROGRAMMING STYLE.

Innovations in programming style and defensive programming have been designed to make typing errors (bugs) less likely or easier to spot.

2. PROGRAMMING TECHNIQUES.

Bugs often create inconsistencies in the internal data of a running program. Programs can be written to check the inconsistency of their own internal data while running. If an inconsistency is encountered, the program can immediately halt so that the bug can be located and fixed.

The program can simply inform the user attempt to correct the inconsistency and continue running.

3. DEVELOPING METHODOLOGIES.

Schemes for managing programmer activity have been designed so that fewer bugs are produced, for example program specifications are used to create the exact behavior of programs so that bugs can be eliminated.