MODULE 7 THREATS TO THE COMPUTER

UNIT 1 COMPUTER VIRUS

CONTENTS

13.0 INTRODUCTION

One of the biggest fears of having computers is viruses. Viruses are malicious programs designed entirely for destruction and havoc. Viruses are created by people who either know a lot about programming or know a lot about computers.

14.0 OBJECTIVES

At the end of this unit, you should be able to:

- explain the concept of computer virus
- explain the ways in which computer viruses are transmitted
- detect viruses in computers
- explain how computer viruses can be prevented
- clean viruses from a computer installation.

3.0 MAIN CONTENT

3.1 Computer Virus

Computer virus is one of the greatest threats to computers and computer applications.

Once the virus is made, it is generally distributed through shareware, pirated software, e-mail or other various ways of transporting data. Once the virus infects someone's computer it will either start infecting other data, destroying data, overwriting data, or corrupting software. The reason these programs are called viruses is that they spread like human viruses. Once your PC has become infected, either by downloading something from the Internet or sharing software, any disks or writeable media that you place into the computer will then be infected. When that disk is put into another computer, the computer is also infected. And if the user puts files on the Internet, and hundreds of people download those files, they will all be infected, and the process will continue infecting thousands if not millions of computers.

3.2 Mode of Transmission of Computer Virus

The majority of viruses are contracted through floppy disk information being brought from one source and then put into your computer. Viruses can infect disks, and when such disks are put into your computer, your computer will become infected with the viruses. A recent survey done in 1997 by NCSA given to PC users showed that 80% of PCs contracted viruses by floppy diskettes. The same survey showed that the other 20% of PCs contracted viruses by e-mail attachments and over the Internet. This means that the users received e-mails with attached files and opened the files, or downloaded files over the Internet.

3.3 Virus Properties

Your computer can be infected even if files are just copied: Because some viruses are memory resident, as soon as a diskette or program is loaded into memory, the virus attaches itself into memory.

Viruses can be polymorphic: Some viruses have the capability of modifying their code, which means one virus could have various amounts of similar variants.

Viruses can be memory/Non memory resident: Depending on the type, a virus can be a memory resident virus type, which first attaches itself into memory and then infects the computer. The virus can also be Non memory resident, which means a program must be run in order to infect the computer.

A virus can be a stealth virus: Stealth viruses first attach themselves to files on the computer, and then attack the computer. This causes the virus to spread more rapidly.

Viruses can carry other viruses and infect a system, and infect with the other viruses as well: Because viruses are generally written by different individuals and do not infect the same locations of memory and or files, this could mean that multiple viruses can be stored in one file, diskette or computer.

Viruses can make the system never show outward signs: Some viruses will hide changes made, such as when infecting a file, the file will stay the same size.

Viruses can stay on the computer even if the computer is formatted: Viruses have the capability of infecting different portions of the computer such as the CMOS battery or master.

3.4 How Viruses May Infect Files

Viruses can infect any files, however they usually attack .com, .exe, .sys, .bin, .pif or any data files. Viruses have the capability of infecting any file. However they will generally infect executable files or data files such as Word or Excel documents which are opened frequently.

Viruses can increase the file's size; however this can be hidden: When infecting files, viruses will generally increase the size of the file. However with more sophisticated viruses, these changes can be hidden.

Viruses can delete files as the files are run: Because most files are loaded into memory and then run once the program is in memory, the virus can delete the file.

Viruses can corrupt files randomly: Some destructive viruses are not designed to destroy random data but instead randomly delete or corrupt files.

Viruses can cause write protect errors when executing .exe files from a write protected disk: Viruses may need to write themselves to files which are executed. Because of this, if a diskette is write protected, you may receive a write protection error.

Viruses can convert .exe files to .com files: Viruses may use a separate file to run the program and rename the original file to another extension, so the .exe is run before the .com.

Viruses can reboot the computer when a file is run: Various computers may be designed to reboot the computer when run.

3.5 What Viruses May Do

The following are possibilities you may experience when you are infected with a virus. Remember that you also may be experiencing any of the following problems and not have a virus.

Once the hard drive is infected, any disk that is non-write protected that is accessed can be infected.

A virus may:

- Deleted files.
- Insert various messages in files or on programs
- Changes volume label
- Mark clusters as bad in the FAT.
- Randomly overwrite sectors on the hard disk
- Replace the MBR with own code
- Create more than one partition
- Attempt to access the hard disk drive which can result in error messages such as invalid drive specification.
- Cause cross linked files
- Cause a “sector not found” error
- Cause the system to run slowly
- Create logical partitions created. Partitions decrease in size
- Display directory as garbage
- Modify order, so files such as Com will start at the beginning of the directory
- Cause hardware problems such as keyboard keys not working, printer problems and modem problems
- Disable ports such as LPT or COM ports
- Cause keyboard to be remapped
- Alter the system time/date
- Cause the system to hang or freeze randomly
- Cause activity on HDD or FDD randomly
- Increase file size
- Increase or decrease memory size
- Randomly change file or memory size
- Extend boot times
- Increase disk access times
- Cause the computer to make strange noises, make music, clicking noises or beeps
- Display pictures
- Cause different types of error messages

3.6 Detecting Viruses

The most commonly used method of protecting against and detecting viruses is to purchase a third party application designed to scan for all types of viruses. Alternatively, a user can look at various aspects of the computer and detect possible signs indicating a virus is on the computer. While this method can be used to determine some viruses, it cannot clean or determine the exact virus you may or may not have.

4.0 CONCLUSION

Computer viruses are perhaps the greatest threats to the computer. If not detected and promptly cured, a computer virus attack could lead to the total breakdown of the computer. With the aid of our discussion in this unit, you should be able to prevent, detect and clean viruses in a computer installation.

5.0 SUMMARY

This unit has taught the following:

(a) Computer viruses are programs written by programmers with the aim of causing havoc to the computer.
(b) Computer viruses could lead to malfunctioning and total breakdown of the computer.
(c) Computer viruses are transferred from one computer to another through the use of infected storage media such as diskette, flash drive, CDROM, or across a computer network.
(d) There are antivirus packages specially written to prevent, detect and clean viruses.

6.0 TUTOR-MARKED ASSIGNMENT

1. What is a computer virus?
2. What are the differences and similarities between biological viruses and computer viruses?
3. How would you prevent virus attack in the student's computer laboratory.

7.0 REFERENCES/FURTHER READING

Akinyokun, O.C. (1999). *Principles and Practice of Computing Technology*. Ibadan: International Publishers Limited.

Balogun, V.F., Daramola, O.A. Obe, O.O. Ojokoh, B.A., and Oluwadare S.A. (2006). *Introduction to Computing: A Practical Approach.* Akure: Tom- Ray Publications.