NIELIT GORAKHPUR

Course Name: O Level (2nd Sem) **Subject:** Introduction to ICT Resources
Topic: Virus and Antivirus (Part 2) **Date:** 14-05-2020

Virus and Antivirus

Symptoms of a Virus Attack

The following lists some of the symptoms of a virus attack, which if detected can be suspected virus.

1. You receive an e-mail with an odd attachment and open it with unexpected results, such as the appearance of odd dialog boxes or a sudden degradation in system performance.
2. An antivirus program will not install on the PC (or appears to install, but then will not run), but other programs will.
3. An antivirus program is disabled for no apparent reason (probably with an X over its icon in the notification area), and you are unable to enable it. The system may or may not report an error condition.
4. Odd dialog boxes or messages appear on the screen frequently or occasionally.
5. There is a double extension of an attachment that you recently opened, such as myfile.jpg.vbs . In order to spot double-extension files, switch on "***the display of extensions for known file types***" in Windows. To do this, click the Tools menu, click Options and deselect the "***Hide Extensions for Known File Types***" checkbox on the View tab.
6. Several files are missing, especially those bf a common type. For example, some viruses delete all graphic files of a particular type.
7. You notice the presence of new users with full security permissions that you know you did not create, or you notice inappropriate permissions assigned to existing users.
8. The mouse pointer changes to some different graphic on its own.
9. Odd icons appear on the desktop although you did not place them there or you have not installed any new applications lately.
10. Strange sounds or music plays from the speakers for no apparent reason.
11. File sizes or date/time stamps have changed on files that you know you did not alter.
12. Your friends tell you that they receive strange e-mail messages from your address containing odd attachments or virus.
13. Your PC starts performing actions on its own, like moving the mouse pointer, opening or closing windows, running programs, or opening and closing the CD tray.
14. Windows operating system will not start because certain important system files are missing.
15. Your PC suddenly starts running slow and/or takes a long time to start up,
16. When you view the system processes via Task Manager, you notice that an unknown process is consuming a high percentage of the CPU time.

There is no simple magical formula to determine whether a virus infection is there or not. Many of the above virus symptoms are similar to the symptoms of normal system problems. The list above, however, can help you make an intelligent guess. For definitive virus detection, you

must turn to antivirus software with updated definitions. If a reputable antivirus program will install, run and complete a check successfully, and if its definitions have been updated within the last 24 hours, you can be fairly confident that the problem is not a virus. Otherwise, virus infection is susceptible.

Antivirus Programs

Antivirus software is a computer program used to prevent, detect, and remove computer virus/malware. Antivirus software can identify and block many viruses before they can infect your computer. How-ever, it is important to keep it up-to-date. Antivirus software scans files and your computer's memory for certain patterns that may indicate an infection. The patterns it looks for are based on the signatures, or definitions, of known viruses. Virus authors are continually releasing new and updated viruses, so it is important that you have the latest definitions installed on your computer. Many antivirus packages include an option to automatically receive updated virus definitions. It is a good idea to take advantage of this option.

Antivirus software was originally developed to detect and remove computer viruses, hence the name. However, with the proliferation of other kinds of malware, antivirus software started to provide protection from other computer threats. In particular, modern antivirus software can protect users from: malicious browser helper objects (BHOs), browser hijackers, ransomware, keyloggers, backdoors, rootkits, trojan horses, worms, malicious LSPs, dialers, fraudtools, adware and spyware. Some products also include protection from other computer threats, such as infected and malicious URLs, spam, scam and phishing attacks, online identity (privacy), online banking attacks, social engineering techniques, advanced persistent threat (APT) and botnet DDoS attacks.

Once you have installed an anti-virus package, scan your computer periodically. You can configure your antivirus software to perform an automatic scan. In automatic scans, it automatically scans specific files or directories and prompts you at set intervals to perform complete scans.

It is also a good idea to manually scan files you receive: from an outside source before opening them. This includes the following:

(a) Saving and scanning email attachments or web downloads rather than selecting the option to open them directly from the source.

(b) Scanning media, including Pen Drive , CDs and DVDs, for viruses before opening any of their files.

Exercise:

1: What are common Symptoms of a Virus Attack?

2: What is Antivirus software?