LUMS

Information Systems and Technology

20
17

PROTECTION
AGAINST
COMPUTER VIRUS

IST TIPS

Computer Virus

A computer virus is a type of malicious code/program/script written to alter the way a computer operates. It is designed to replicate itself so that it can spread from one computer to another. A computer virus is meant to harm system software by corrupting data in system's hard drive. Numerous computer viruses now operate over the internet and new computer viruses are discovered every day. The increased use of internet has accelerated the spread of computer viruses more easily than ever.

Major Types of Computer Viruses

Some major types of computer viruses are:

Boot Sector Virus:
A boot sector virus replaces the boot program used to start a computer with a modified, infected version of the boot program. When the computer runs the infected boot program, the computer loads the virus into its memory. Once the virus is in memory, it spreads to any disk inserted into the computer.

File Virus:
A file virus attaches itself to or replaces program files; the virus then spreads to any file that accesses the infected program.

Trojan Horse Virus:
A Trojan horse virus is a virus that hides within or is designed to look like a legitimate program.

Macro Virus:
A macro virus uses the macro language of an application, such as word processing or spreadsheet, to hide virus code. When you open a document that contains an infected macro, the macro virus loads into memory.

Flash Drive Virus:
Flash drives are a very common source of virus distribution. One should be very careful when using flash drives. Some common symptoms of infected flash drives are:

- Most flash drives auto-run automatically after inserting it into a PC, so if you see two folders for same name then there is definitely something wrong with it.
- It may open in new window
- Removable disk icon is replaced by a folder icon or no icon
- Some random error might appear when you try to open it
- It might create shortcut for every file and folder on flash disk and is commonly known as shortcut virus

Symptoms of Infected Systems:

- Decrease in system performance
- Unexplained freezing/crashing
- Unable to open programs
- Unable to install new programs
- Computer has trouble booting windows
- Computer crashes and restarts every few minutes
- Desktop appearance and other visual settings are changed unexpectedly

- Files or folders are deleted unexpectedly
- Worsening condition over a period of a few days to a few weeks as viruses download more malicious software as time goes on
- Unexpected decrease of hard disk space
- Unusual error messages
- Unable to open files or folders
- Internet access is blocked

Measures to Prevent Virus Attacks:

- Installation of antivirus software
- Keep your antivirus software up to date
- Run regular computer scans
- Keep your operating system up to date
- Keep your firewall enable
- Avoid websites that provide pirated material

- Do not open an email from someone you don't know
- Do not click on any link provided in the email unless it is from a legitimate source
- Download files only from trusted websites
- Never open any USB/external drive/memory card unless you scan it

Top Rated Antivirus Programs:

Removing a Shortcut Virus from Flash Drive/Memory Card:

Shortcut virus mimics your data with shortcut icons of your files and folders. In this situation user is unable to access the data stored on flash drive. This virus can be removed by small utility called shortcut remover that is available for LUMS staff/faculty/students on LUMS software bank. To access this, you must be connected to LUMS network through LAN/Wireless.

1. Press Windows+R to open Run
2. Type **sus.lums.net** and press **Enter**
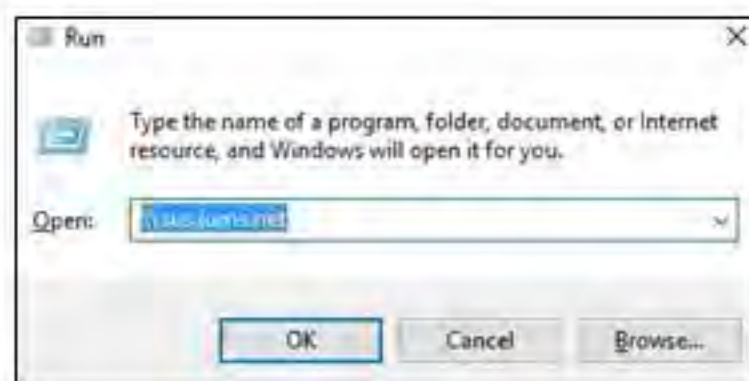
3. A network folder will be opened. Go to Software/Freeware and search for **'Shortcut Remover'**
4. Copy this utility on your desktop and open it
5. Select Pen Drive

6. Select appropriate device from the list and hit Scan

7. If the scan is successful a folder will be created in your drive containing all your recovered folders and files.
8. Delete the shortcuts