Computer Maintenance Software (CM274)

Chapter 4: Viruses & Backup

Prepared by Eisa Haider
Supervised by Meshal Al-Dhamen
(Oct., 2015)

1

What is a Computer Virus?

2

What is a Computer Virus?

- **A computer virus is a piece of malicious code that attaches to important areas within computers, such as executable file, and the boot areas of hard disks.**
- A virus can destroy data after copying itself to other host files or disks.
- The virus spreads when its host file runs and the malicious code is unleashed.

3

What is a Computer Virus?

- The virus can quickly spread into memory as the computer boots from an infected disk.
- Once in memory, the virus can infect other executable files or disk boot sectors.
- Typically, a virus remains dormant until some trigger event occurs, such as a system date.
- In addition to replication, a computer virus often performs some other function, usually intended to do damage or spread a message.

4

How do viruses spread?

- Program viruses spread through just about any network, modem, or magnetic medium. Most boot viruses can only spread by way of floppy disks.
- The explosive growth of LAN, Internet, and global email connectivity has dramatically accelerated the rate at which viruses can spread.
- The primary threat of infection comes from files that are shared, and then opened and used.

5

Types of Viruses

6

Types of Viruses

1. **Boot viruses.**
2. **Program viruses.**
3. **Macro viruses.**

7

Boot Viruses

What they infect?	How they infect?	Damage
Boot viruses insert instructions into the boot sectors of floppy disks, or the boot sector or master boot record (partition sector) of a hard disk.	When the computer boots from an infected floppy disk, the virus infects the hard disk and loads its code into memory. The floppy disk does not have to be bootable for the virus to spread. The virus remains memory resident and infects any floppy disks that are accessed.	A floppy disk or hard disk with an infected boot sector won't infect any files unless the virus is also multipartite. A true boot virus can't spread to a server or over the network.

8

Program Viruses

What they infect?	How they infect?	Damage
Program file viruses attach to executable files such as .COM, .EXE, and .DLL files by inserting instructions into the execution sequence.	There are three sub classifications of program file viruses: Memory resident: Stay in memory as terminate-stay-resident (TSR) programs. Direct action: Execute, infect other files, and unload. Companion: Associates itself with an executable file without modifying it.	The damage caused by program file viruses varies from irritating, such as displaying screen messages, to data destroying.

9

Macro Viruses

What they infect?	How they infect?	Damage
Unlike other viruses, macro viruses do not infect program files; they infect documents. Common targets for many macro viruses are word processors such as Microsoft Word, and spreadsheets like Microsoft Excel.	Word uses macros to perform actions such as formatting text and opening or closing a document. Macro viruses can modify macros defined by the Word application to perform malicious actions such as overwriting or redefining default definitions in Word.	The damage caused by macro viruses can range from inserting unwanted text into documents to significantly reducing the functionality of a computer. For example, Format.C will format your hard disk.

10

How Does Symantec Antivirus Prevent Infection?

11

How does Symantec Antivirus prevent infection?

- Virus infections can be easily avoided. Viruses that are quickly detected and removed from your computer cannot spread to other files and cause damage.
- Symantec Antivirus uses a variety of methods to detect file, boot, and macro viruses early:
  - **Real-Time Protection.**
  - **Signature-Based Scanning.**

12

Real-Time Protection

Real-Time Protection:

Constantly monitors activity on your computer by looking for viruses when a file is executed or opened, and when modifications have been made to a file, such as renaming, saving, moving, or copying a file to and from directories.

13

Signature-Based Scanning

Signature-based scanning:

Symantec Antivirus relies on signature or pattern-based scanning to detect viruses. Symantec Antivirus searches for residual virus signatures in infected files. This search is called a **scan**.

14

What is a Scan?

- **A scan is a search through your computer's memory, boot sector, partition tables, and directories for viruses or virus-like behavior.**
- There are serval types of scan:
  - **Full scan.**
  - **Custom scan.**
  - **Startup scan.**
  - **Scheduled scan.**
  - **Real-time protection.**

15

What does Symantec Antivirus do with infected files?

- Symantec Antivirus responds to infected files through actions and backup actions.
- **Actions** are response to a virus infection.
- By default, Symantec Antivirus usually attempts to clean the virus from the infected file.
- If cleaning doesn't work, Symantec Antivirus attempts to a **backup actions** as moving the virus to the Quarantine.

16

What does do with infected files?

- **Actions & Backup Actions :**
  - Cleaning the virus from the file.
  - Deleting the infected file.
  - Leaving the infected file alone.
  - Moving the infected file to the Quarantine.
- **Quarantine :**
  - Quarantine is a holding cell for infected files. Files within the Quarantine cannot be modified or saved.

17

How To Use Backup and Restore Feature in Windows 7

18

What is a Backup?

- **A computer backup is a copy of electronic data stored separately from the original files.**
- In the event that the original data set gets corrupted, damaged, deleted or lost, the backup can be used to recover or restore the data.
- A backup therefore minimizes the risk of irretrievably losing data.

19

Types of Backups

1. **Full Backup.**
2. **Differential Backup.**
3. **Incremental Backup.**

20

Types of Backups

1. Full Backup:

A full backup is a 100% copy of the original files. It is typically saved to a fresh folder that carries a timestamp. This is the traditional way to back up files. Since every single file is copied, the full backup is the slowest of all backup types.

21

Types of Backups

2. Differential Backup:

A differential backup backs up all files that have changed since the last full backup. This means it adds all new and updated files to an existing full backup.

22

Types of Backups

3. Incremental Backup:

Like a differential backup, an incremental backup backs up only changed files. The difference between the two is that the incremental backup simply backs up files that were changed since the previous backup, no matter whether this was a full, differential, or incremental backup. This is the fastest way to update an existing backup.

23

Backup and Restore Feature in Windows 7

Windows 7 features its own backup tool, also known as the Backup & Restore Feature.

24

What Does Windows 7 Backup & Restore Do?

- **It creates a backup of your personal files and you can also include a system image to back up system settings and program files.**
- By default, the backups runs on a weekly schedule, but the schedule can be customized or turned off.
- Should disaster strike, you can use the backup to restore personal files to a new installation of Windows.

25

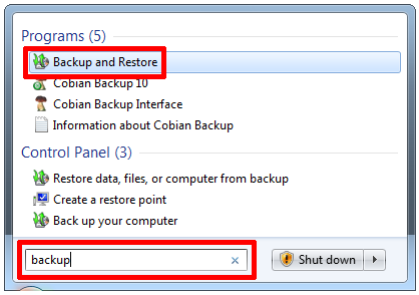
What Do I Need?

- **You need a backup medium. Ideally, this is an external hard drive or a network drive, but it can also be a second hard drive or partition within your computer.**
- Regardless of which medium you choose, it requires enough free space to hold your backup.

26

How Can I Set It Up?

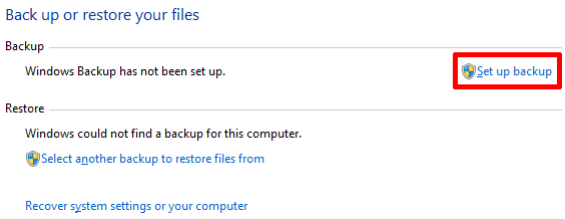
- Setting up a backup with the Windows 7 Backup and Restore feature is straightforward, taking only a few easy steps.
- To launch Windows 7 Backup and Restore:
  - Go to **Start**, and type **Backup** into the search field.
  - From the results select **Backup and Restore** and press **Enter**.



27

How Can I Set It Up?

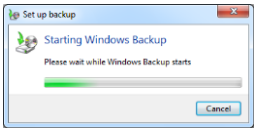
In the Backup and Restore window, click **Set up backup** in the top right.

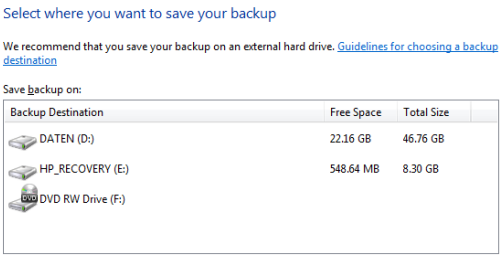


28

How Can I Set It Up?

Once the Set up backup window loads, you will see a list of backup destinations.

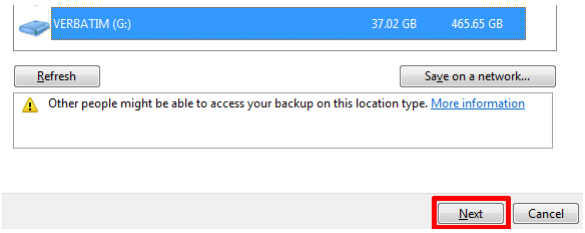




29

How Can I Set It Up?

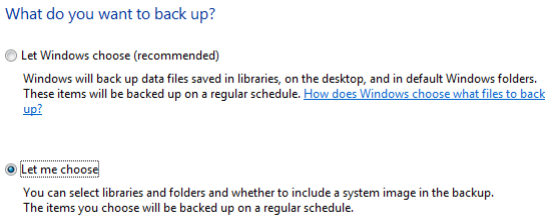
When the desired backup destination appears in the list, select it and click on **Next** in the bottom right.



30

How Can I Set It Up?

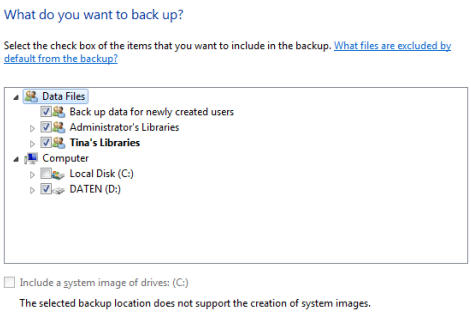
On the next screen, you can choose what to back up and you can either decide to **Let Windows choose** or **Let me choose**, i.e. choose yourself.



31

How Can I Set It Up?

After clicking Next in the previous window, you can check the drives, partitions, and folders you want to back up. Note that Backup and Restore does not back up Program Files or system files, even if you include the system drive in your backup. However, you can Include a system image in your backup, provided there is enough space available on your backup destination.

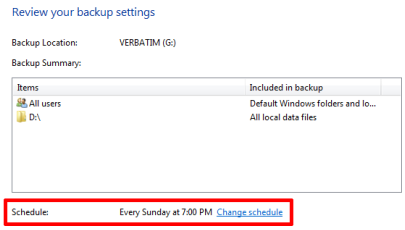


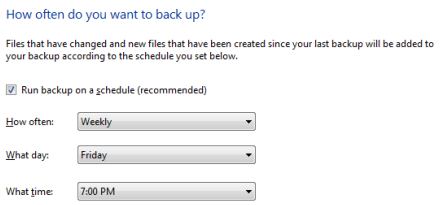
32

How Can I Set It Up?

In a final step you can review your settings and manage the schedule of your backup.

Click on **Change schedule** to create a custom time for your backup.

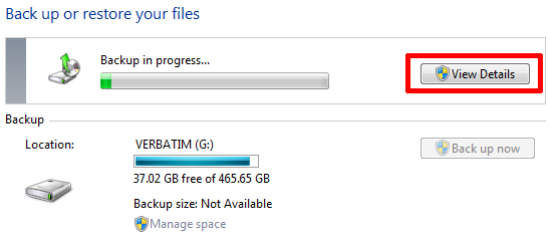




33

How Can I Set It Up?

Click **OK** to confirm the schedule, then click **Save settings** and run backup in the Review your backup settings window. This will take you back to the initial Backup and Restore Control Panel window. The backup you just confirmed will start immediately.



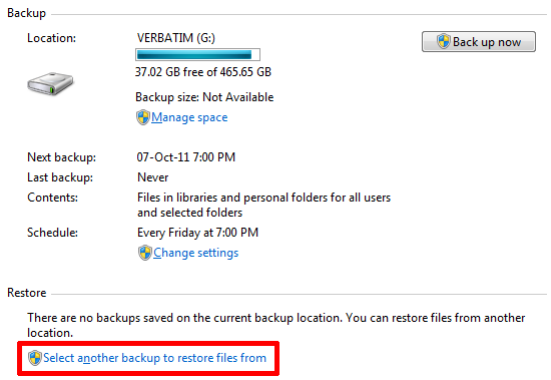
34

How Can I Set It Up?

- The Backup and Restore window will now list your backup and you can change your backup settings here, for example change what you want to back up or adjust the schedule.
- At the bottom of the window, there is a small section called **Restore**. To restore backups, click Select another backup to restore files from and browse for a previous backup you wish to restore.

35

How Can I Set It Up?



36