Lesson 10 Data and Hardware Protection

Lesson Objectives

- Understand types of backups.
- Select a backup method.
- Determine a schedule for backing up data.
- Backup and restore files and folders.
- Protect a computer from theft and physical damage.

Backing Up and Restoring Files

- You make a backup or duplicate copy of a file so that you can access data if you lose the file as a result of a virus, inadvertently overwriting the file, or a hard drive crash.

Understanding Types of Backups

- The following are the four most common types of backups for individual computer users:
  - A full system backup is an exact duplication of the hard drive.
  - A differential backup contains copies of the files that have changed since the last full system backup.
  - An incremental backup contains copies of the files that have changed since the last full system backup or the last incremental backup.
  - A selective backup contains copies only of designated folders and files.

Selecting a Backup Method

- Backup methods include using software installed on your computer or an online backup service provider.
- Backup software is a set of system utilities for creating and updating backups, and restoring files from a backup.
- Backup software compresses files selected for a backup into a single large file.
- Windows 8 provides the following backup and restore software:
  - File History
  - System Image Backup
  - Recovery
- A location is selected for backups:
  - External hard drive
  - USB flash drive
  - Optical disc
  - Network folder
- You can use software and online services to synchronize files so that the files stored in the cloud are the same as those stored on your computer's hard drive.
- Dropbox is an example of a cloud storage service that synchronizes more than one computer with the files stored in a cloud folder.

Following a Backup Plan

- You establish a backup plan to follow a regular schedule for creating different types of backups.
- The Backup 3-2-1 rule is as follows:
  - 3 backups: Maintain two full system backups (Backup A and Backup B).
  - 2 types of media: Use an external hard drive and DVDs or a cloud folder.
  - 1 off-site backup: Create one full system backup off-site and one in your home or office.

- Quick Tip: To back up a smartphone or tablet running iOS, you can use iCloud or iTunes. Backing up to iCloud happens automatically when your device is connected to the Internet. To back up using iTunes, you connect your Apple smartphone or tablet to a computer on which iTunes is installed. You can also automatically back up an Android device to Google Drive.
- Quick Tip: To be safe, you should create more than one backup and keep each one up to date. Store at least one copy in a safe place near your computer for convenience in restoring files. Store at least one other copy in an off-site location, such as a safe deposit box, a locked file cabinet at home or work, or a network folder. If you store all your backups near your computer, and the computer is damaged from a calamity such as a fire, flood, or intruder, the backups could also be damaged or destroyed at the same time.
- Quick Tip: You can also access File History settings on the PC settings screen. Display the PC settings screen, click Update and recovery in the left pane, and then click File History.

Protecting Hardware

- In addition to protecting data using software tools such as antivirus software, you need to protect the computer hardware and peripherals from theft and physical harm.

Protecting Against Environmental Damage

- Environmental hazards include temperature extremes, humidity, electrical fields, and power fluctuations.
- Guidelines for protecting your computer against environmental hazards include:
  - Controlling the temperature: 68 to 75 degrees (F)
  - Controlling the humidity: 30 to 50 percent
  - Preventing spillage
  - Preventing physical damage from dropping
  - Protecting against power fluctuations

Protecting Against Theft

- Use a cable lock to secure a mobile computer to a desk or table.
- Install tracking software. Features of tracking software include:
  - Alarm
  - Data removal
  - Unauthorized user notification
  - Battery control

Key Terms

- **Backup:** A duplicate copy of a file that you use if the original file is lost, damaged, or destroyed. (Mod1-272)
- **Backup plan:** A plan that follows a regular schedule for creating different types of backups. (Mod1-284)
- **Backup software:** A set of system utilities for creating and updating backups, and for restoring files from a backup. (Mod1-274)
- **Differential backup:** A backup that contains copies of the files that have changed since the last full system backup. (Mod1-273)
- **Encryption:** A security method that encodes data so that only authorized people can access it. (Mod1-276)
- **Full system backup:** An exact duplication of the hard drive, including data files, system files and settings, application files, and the operating system. (Mod1-272)
- **Incremental backup:** Contains copies of the files that have changed since the last full system backup or the last incremental backup. (Mod1-273)

- **Local backup:** When the backup medium is stored close to the computer. (Mod1-276)
- **Online backup:** An online service that automatically creates backups on a secure server. (Mod1-280)
- **Redundancy:** Creating more than one copy of a backup so that at least one backup survives a destructive event. (Mod1-284)
- **Remote backup:** An online service that automatically creates backups on a secure server. (Mod1-280)
- **Restore:** To copy the file to its original location on your computer. (Mod1-272)
- **Selective backup:** Selecting the folders and files you want to back up. (Mod1-273)
- **Synchronize:** Comparing files on two drives and then updating files as necessary so the drives contain the same versions of the files. (Mod1-283)
- **Uninterruptible power supply (UPS):** A battery that provides power if the normal current is interrupted. (Mod1-286)