* User Management:

User management is like being the boss of who can use a computer system. It's about making, changing, and deleting accounts and deciding what those accounts are allowed to do.

* Why User Management is Needed:

User management is needed to keep computer stuff safe. It helps control who can see and use information. It also makes sure people only get access to what they really need, keeps things organized, and helps with rules about passwords and other security things.

* Accessing User Management:

You can find user management in settings or control panels of computer systems, websites, or apps.

* User Management Features:

It helps make new users, change their details, and remove them. You can control what users can do, set strong password rules, track activities, and manage user groups.

* Do a practical to create a user from user management

1. Creating a User:
2. Step 1: Open the User Management Tool
3. Go to the system settings or control panel.
4. Look for "User Accounts" or a similar option.
5. Step 2: Add a New User
6. Find the "Add User" or "Create New User" button.
7. Fill in the user details: username, password, and any required information.
8. Follow on-screen instructions to complete the process.
9. Step 3: Set User Permissions (if available)
10. Assign specific roles or permissions to the new user.
11. Save changes.

* Do a practical to change the password of the administrator from the user management

Changing Administrator Password:

Step 1: Access User Management

Open the user management tool as you did before.

Step 2: Locate Administrator Account

Look for the administrator account in the user list.

Step 3: Change Password

Find an option like "Change Password" or "Reset Password."

Follow the prompts to enter a new password.

Save the changes.

Step 4: Confirm Changes

Than login with that password.

* What is File Folder Permission:

File and folder permissions are like rules that decide who can do what with files and folders on a computer. They control whether someone can read, edit, or delete a file, and if they can, who else can do the same.

* What is the use of file and folder permission?

Use of File and Folder Permission:

File and folder permissions keep your computer stuff safe. They make sure only the right people can access or change files. It's like having a lock on a door – you decide who gets the key and what they're allowed to do inside.

* Give a Folder Read-Only Permission STEPS:

1. Right-click on the folder you want to set permissions for.
2. Choose "Properties" from the menu.
3. Go to the "Security" tab.
4. Click on "Edit" to change permissions.
5. Select the user or group and check "Read" under "Allow."
6. Click "Apply" and then "OK" to save the changes.

* Give a File Only Admin Permission:

1. Right-click on the file you want to set permissions for.
2. Choose "Properties."
3. Go to the "Security" tab.
4. Click on "Edit" to modify permissions.
5. Select the user or group, uncheck unnecessary permissions, and leave only "Full Control" or "Modify" for Admin.
6. Click "Apply" and then "OK" to save the changes.

* Give Folder Read-Only Permission in Network:

1. Right-click on the folder in the network.
2. Choose "Properties."
3. Go to the "Sharing" tab.
4. Click "Advanced Sharing."
5. Check "Share this folder."
6. Click "Permissions."
7. Select "Everyone" or specific users.
8. Set permission to "Read."
9. Click "OK" to apply changes.

* Change Ownership of Folder and Subfolders:

1. Right-click on the folder.
2. Choose "Properties."
3. Go to the "Security" tab.
4. Click "Advanced."
5. Go to the "Owner" tab.
6. Click "Change" next to the current owner.
7. Enter the new owner (e.g., your user account or Administrators group).
8. Check "Replace owner on subcontainers and objects."

Click "OK" to apply changes.

* OS (Operating System):

An Operating System (OS) is the main software that manages computer hardware and provides services for computer programs. It acts as an intermediary between the user and the computer hardware.

* Types of OS:

There are two main types of operating systems:

Desktop/Personal OS: For individual computers, examples include Windows, macOS, and Linux.

Server OS: Designed for servers, managing network resources, and providing services, examples include Windows Server, Linux Server distributions

* Create Bootable Pendrive for Kali Linux:

1. Download Kali Linux ISO from the official website.
2. Download a tool like Rufus or BalenaEtcher.
3. Insert your USB drive.
4. Open the tool, select the Kali Linux ISO, and choose the USB drive.
5. Click "Start" or "Flash" to create the bootable USB.
6. Wait for the process to finish.
7. Create Bootable Pendrive for Windows 7:
8. Download Windows 7 ISO from a reliable source.
9. Download a tool like Rufus or Microsoft's official USB/DVD Download Tool.
10. Insert your USB drive.
11. Open the tool, select the Windows 7 ISO, and choose the USB drive.
12. Click "Start" or "Create" to make the USB bootable.
13. Wait for the process to complete.

* Installing mac os steps:

1. Create Pendrive for Mac OS Mojave with UniBeast:.
2. Download macOS Mojave from the Mac App Store.
3. Download UniBeast from the official tonymacx86 website.
4. Insert your USB drive.
5. Open UniBeast, follow the on-screen instructions, and select the Mojave installation.
6. Choose your USB drive as the destination.
7. Customize settings if needed, then click "Continue" or "Install."
8. Wait for the process to finish.

* Install Kali Linux:

1. Download Kali Linux:
2. Get the Kali Linux ISO from the official website.
3. Create Bootable USB:
4. Use a tool like Rufus or BalenaEtcher to create a bootable USB drive with the Kali Linux ISO.
5. Boot from USB:
6. Insert the USB into your computer.
7. Restart your computer and boot from the USB drive.
8. Follow on-screen instructions to start the installation.
9. Install Kali Linux:
10. Follow the installation wizard.
11. Choose your language, location, and keyboard layout.
12. Create a user account and set a password.
13. Select the installation type (usually choose the entire disk).
14. Confirm the changes and let the installation complete.

* Install Windows 10:

1. Download Windows 10:
2. Get the Windows 10 ISO from the official Microsoft website.
3. Create Bootable USB:
4. Use a tool like Rufus or the Windows Media Creation Tool to make a bootable USB drive with the Windows 10 ISO.
5. Boot from USB:
6. Insert the USB into your computer.
7. Restart your computer and boot from the USB drive.
8. Follow on-screen instructions to start the installation.
9. Install Windows 10:
10. Choose language, time, and keyboard input.
11. Click "Install Now" and enter your product key.
12. Select the installation type (usually choose "Custom" for a new installation).
13. Choose a partition to install Windows, and follow the prompts to complete the installation.

* Install macOS (macOS X):
  1. Get macOS from the Mac App Store.
  2. Create Bootable USB with UniBeast:
  3. Download UniBeast from the tonymacx86 website.
  4. Follow UniBeast's instructions to create a bootable USB with the macOS installer.
  5. Boot from USB:
  6. Insert the USB into your computer.
  7. Restart your computer and boot from the USB drive.
  8. Follow on-screen instructions to start the installation.
  9. Install macOS:
  10. Use UniBeast to install macOS on your chosen drive.
  11. Follow UniBeast's prompts and customize settings as needed.
  12. Complete the installation, and follow post-installation steps provided by UniBeast.
* Clean Install:

A clean install is starting fresh by erasing the existing operating system and data on a computer, then installing the OS again. It's like setting up a new system without keeping any old files or settings

* Process for Clean Install:

Backup important data.

Insert the installation media (USB/DVD).

Restart the computer and boot from the media.

Choose "Custom Install."

Delete existing partitions.

Select the unallocated space to install.

Follow prompts to complete the installation.

Set up user account and preferences.

* Benefits of Clean Install:

Performance: Removes clutter, potentially improving system speed.

Stability: Reduces conflicts from old settings or software.

Security: Eliminates potential malware or unwanted programs.

Fresh Start: Provides a clean slate for a new and optimized system.

* Clean Installation of Windows (Steps):

1. For Windows XP (not recommended due to security risks):
2. Insert Installation CD:
3. Insert the Windows XP installation CD into your computer.
4. Boot from CD:
5. Restart your computer and set it to boot from the CD/DVD drive in the BIOS settings.
6. Windows Setup:
7. Follow the on-screen instructions to enter the Windows XP setup.
8. Partition and Format:
9. Delete existing partitions on the hard drive.
10. Create a new partition and format it using the NTFS file system.
11. Installation:
12. Choose the newly created partition for installation.
13. Follow the prompts to complete the installation, including entering the product key.
14. Setup and User Account:
15. Set up regional settings, time zone, and keyboard layout.
16. Create a user account and set a password.
17. Finish Installation:
18. Allow the installation to complete.
19. Install drivers and necessary software.

* For Windows 8:

1. Insert Installation Media:
2. Insert the Windows 8 installation USB or DVD into your computer.
3. Boot from Installation Media:
4. Restart your computer and set it to boot from the USB or DVD drive in the BIOS settings.
5. Windows Setup:
6. Follow the on-screen instructions to enter the Windows 8 setup.
7. Product Key and License Agreement:
8. Enter the product key when prompted.
9. Accept the license terms.
10. Custom Installation:
11. Choose the "Custom" option for a clean installation.
12. Partition and Format:
13. Delete existing partitions if needed.
14. Create a new partition and format it using the NTFS file system.
15. Installation:
16. Choose the newly created partition for installation.
17. Follow the prompts to complete the installation.
18. Setup and User Account:
19. Set up regional settings, time zone, and keyboard layout.
20. Create a user account and set a password.
21. Finish Installation:
22. Allow the installation to complete.
23. Install drivers and necessary software.

* Upgrade Installation:

Upgrade installation is when you install a newer version of an operating system on a computer that already has an older version installed. The new version replaces the old one, keeping your files and settings.

* Benefits of Upgrade Installation:

Preserves Data: Your files and programs stay intact.

Saves Settings: System settings and configurations are retained.

Faster Process: Generally quicker than a clean install.

Smooth Transition: Easier for users familiar with the existing system.

* Upgrade installation steps:

1. Backup Your Data:
2. Before starting, backup important files to avoid data loss.
3. Check System Requirements:
4. Make sure your computer meets the requirements for the new version.
5. Download the Upgrade:
6. Obtain the upgrade from the official source, usually as a download or installation media.
7. Run the Installer:
8. Double-click the installer to start the upgrade process.
9. Follow On-Screen Instructions:
10. Read and follow the on-screen prompts carefully.
11. Enter Product Key:
12. If required, enter the product key during the installation.
13. Choose Upgrade Option:
14. Select the option for an "Upgrade" or "Keep Files and Settings" when prompted.
15. Wait for Installation:
16. Allow the upgrade process to complete. It may take some time.
17. Restart Your Computer:
18. After installation, restart your computer as instructed.
19. Verify Settings:
20. Check that your files, applications, and settings are preserved.
21. Update Drivers and Software:
22. Update drivers and software for compatibility with the new version.
23. Complete Any Post-Installation Steps:
24. Follow any additional steps recommended by the upgrade process.

* Upgrade from Windows 8 to Windows 10:

1. Backup Your Data:
2. Before starting, back up important files to avoid data loss.
3. Check System Requirements:
4. Ensure your computer meets the requirements for Windows 10.
5. Download Windows 10:
6. Go to the official Microsoft website and download the Windows 10 Media Creation Tool.
7. Run the Media Creation Tool:
8. Double-click the downloaded tool to run it.
9. Accept License Terms:
10. Read and accept the license terms.
11. Choose Upgrade Option:
12. Select "Upgrade this PC now" and click "Next."
13. Wait for Download and Installation:
14. The tool will download and install Windows 10. This may take some time.
15. Follow On-Screen Instructions:
16. Read and follow the on-screen prompts carefully.
17. Keep Files and Apps:
18. During the upgrade process, choose the option to keep your files and apps.
19. Wait for Installation to Complete:
20. Allow the installation process to finish.
21. Restart Your Computer:
22. After installation, your computer will restart.
23. Verify Settings:
24. Check that your files, applications, and settings are preserved.
25. Update Drivers and Software:
26. Visit the manufacturer's website to update drivers and software for compatibility.
27. Complete Any Post-Installation Steps:
28. Follow any additional steps recommended by the Windows 10 setup.

* Partitioning:

Partitioning is like dividing a hard drive into separate sections. Each section is called a partition, and it can hold its own files and operating system. It helps organize and manage data on a storage device.

* Partition:

A partition is a section of a hard drive that acts like its own mini-drive. It has its own space for files and can be formatted with its own file system. Multiple partitions allow different types of data to be stored separately on the same physical drive.

* Format:

Format is like preparing a storage area for use. It erases any existing data and sets up the file system, making the storage device ready to store new files. Think of it as getting a clean slate before putting anything new on it.

* Creating an MBR Partition:

1. Open Disk Management:
2. Right-click on the "Start" button.
3. Choose "Disk Management."
4. Select the Disk:
5. In the lower section, find the disk where you want to create the partition.
6. Right-click on unallocated space on that disk.
7. Create a New Simple Volume:
8. Choose "New Simple Volume."
9. Click "Next" on the wizard that appears.
10. Specify Size:
11. Enter the size for the partition.
12. Click "Next."
13. Assign Drive Letter:
14. Choose a drive letter or let Windows assign one.
15. Click "Next."
16. File System and Format:
17. Select "NTFS" as the file system.
18. Optionally, give the volume a label.
19. Click "Next" and then "Finish."

* Creating a GPT Partition:

1. Open Disk Management:
2. Right-click on the "Start" button.
3. Choose "Disk Management."
4. Select the Disk:
5. In the lower section, find the disk where you want to create the partition.
6. Right-click on unallocated space on that disk.
7. Create a New Simple Volume:
8. Choose "New Simple Volume."
9. Click "Next" on the wizard that appears.
10. Specify Size:
11. Enter the size for the partition.
12. Click "Next."
13. Assign Drive Letter:
14. Choose a drive letter or let Windows assign one.
15. Click "Next."
16. File System and Format:
17. Select "NTFS" as the file system.
18. Optionally, give the volume a label.
19. Click "Next" and then "Finish."

* steps to convert a partition to GPT using Command Prompt (cmd) and to format a partition:
* Convert a Partition to GPT using CMD:

1. Open Command Prompt:
2. Press Win + X and choose "Command Prompt (Admin)" or "PowerShell (Admin)."
3. Type Diskpart:
4. In the Command Prompt window, type diskpart and press Enter.
5. List Disks:
6. Type list disk and press Enter to see a list of available disks.
7. Select Disk:
8. Type select disk X (replace X with the disk number of the target disk) and press Enter.
9. Clean the Disk:
10. Type clean and press Enter. This will erase all data on the disk.
11. Convert to GPT:
12. Type convert gpt and press Enter to convert the disk to the GPT partition style.
13. Exit Diskpart:
14. Type exit and press Enter to exit Diskpart.

* Format a Partition using CMD:

1. Open Command Prompt:
2. Press Win + X and choose "Command Prompt (Admin)" or "PowerShell (Admin)."
3. Type Format Command:
4. Type format X: /FS:NTFS (replace X with the drive letter of the partition) and press Enter.
5. Optionally, add /Q for a quick format.
6. Confirm Format:
7. Confirm by typing Y and pressing Enter.
8. Wait for Format:
9. Wait for the format process to complete.

* Transferring Files:

Transferring files means moving or copying data (like documents, photos, or videos) from one place to another. This can be between devices, folders, or over a network.

* Ways of Transferring Files:

USB Drives: Copy files onto a USB flash drive and plug it into another device.

File Sharing Apps: Use apps like Dropbox, Google Drive, or OneDrive to share files over the internet.

Email: Attach files to an email and send them to someone.

Network Sharing: Share files between computers on the same network.

Bluetooth: Transfer files wirelessly between devices that have Bluetooth.

External Hard Drives: Copy files to an external hard drive and connect it to another device.

* Transfer Files Between Systems:

USB Drive: Copy files to a USB drive, then plug the drive into the other system.

Network Sharing: Share files over the same network, allowing one system to access the files on the other.

Cloud Storage: Upload files to a cloud service (like Google Drive), then download them on the other system.

Email: Attach files to an email and send them to the other system.

* Types of File Transferring Media:

USB Drive: Portable storage device connected via USB.

Network Cable: Physical cable connecting two systems on the same network.

Wi-Fi: Wireless connection for file transfer over a network.

Bluetooth: Wireless technology for short-range file transfer between devices.

Cloud Storage: Online platforms providing space to upload and download files.

* Transfer Files Between Systems via Network:

1. Identify Shared Folders:
2. On the source system, right-click on the folder you want to share.
3. Choose "Properties" and go to the "Sharing" tab.
4. Share the Folder:
5. Click "Share" and select users or Everyone.
6. Click "Add" and give the appropriate permissions.
7. Click "Share" and "Done."
8. Access Shared Folder:
9. On the other system, open File Explorer.
10. Navigate to "Network" and find the shared computer.
11. Copy Files:
12. Open the shared folder.
13. Copy the files from the source system to this folder.

* Transfer Data Between Hard Disks:

1. Open File Explorer:
2. Press Win + E to open File Explorer.
3. Identify Source and Destination Drives:
4. Identify the source drive (where files are located) and the destination drive (where you want to copy files).
5. Copy Files:
6. Navigate to the source drive.
7. Select the files or folders you want to copy.
8. Right-click, choose "Copy" (or press Ctrl + C).
9. Paste Files to Destination:
10. Navigate to the destination drive.
11. Right-click on an empty space and choose "Paste" (or press Ctrl + V).
12. Wait for Transfer:
13. Allow the system to copy the files to the destination drive.

* Administrative Tools:

Administrative tools are special programs on a computer that help manage and control the system. They are like a toolbox for system administrators to configure settings, diagnose issues, and perform advanced tasks.

* Use of Administrative Tools:

System Configuration: Adjust startup settings and system behavior.

Disk Management: Manage hard drives, partitions, and file systems.

Event Viewer: View logs and diagnose system events.

Device Manager: Control hardware devices and drivers.

Computer Management: Access various system tools in one place.

Task Scheduler: Automate tasks to run at specific times.

Services: Control system services running in the background.

Administrative tools make it easier to maintain and troubleshoot a computer system.

* List of Administrative Tools:

System Configuration: Manages system startup and configuration.

Task Scheduler: Automates tasks to run at specific times.

Event Viewer: Views logs and system events.

Device Manager: Controls hardware devices and drivers.

Computer Management: Provides access to various system tools.

Services: Manages background system services.

Disk Management: Manages hard drives, partitions, and file systems.

* Disk Management Tools:

Disk Management is a tool that helps control and organize hard drives on a computer.

It allows you to create, delete, format, and resize partitions.

You can assign drive letters, change file systems, and manage disk properties.

Disk Management is crucial for maintaining storage and organizing data on a computer.

* Delete and Reinstall a Driver from Device Manager:

1. Open Device Manager:
2. Right-click on the Start button.
3. Choose "Device Manager."
4. Locate the Driver:
5. Find the device with the driver you want to reinstall.
6. Uninstall the Driver:
7. Right-click on the device and choose "Uninstall device."
8. Check the box that says "Delete the driver software for this device."
9. Click "Uninstall."
10. Reinstall the Driver:
11. Right-click on any device in Device Manager.
12. Choose "Scan for hardware changes."
13. Windows will detect the hardware and reinstall the driver.

* Delete and Create a Partition using Disk Management:

1. Open Disk Management:
2. Press Win + X and select "Disk Management."
3. Locate the Partition:
4. Right-click on the partition you want to delete.
5. Delete the Partition:
6. Choose "Delete Volume."
7. Confirm the deletion.
8. Create a New Partition:
9. Right-click on the unallocated space.
10. Choose "New Simple Volume."
11. Follow the wizard to create a new partition.
12. Create a User with Computer Management:
13. Open Computer Management:
14. Right-click on the Start button.
15. Choose "Computer Management."
16. Navigate to System Tools:
17. In the left pane, go to "System Tools" > "Local Users and Groups" > "Users."

* Create a New User:

1. Right-click in the right pane.
2. Choose "New User."
3. Enter user details (username, password).
4. Click "Create" and then "Close."
5. Assign User to a Group (Optional):
6. Right-click on the user you created.
7. Choose "Properties."
8. Go to the "Member Of" tab.
9. Add the user to a group if needed.

* Windows Features:

Windows Features are special programs and functionalities that are built into the Windows operating system but may not be installed by default. Users can enable or disable these features based on their needs. They include tools, services, and applications that enhance or expand the capabilities of the Windows system.

* List of Windows Features:

Some common Windows features include:

Internet Information Services (IIS)

Telnet Client

.NET Framework

Hyper-V

Windows Subsystem for Linux

Remote Server Administration Tools

Media Features (Windows Media Player)

Print and Document Services

Windows PowerShell

The list may vary depending on the Windows version.

* Use of IIS (Internet Information Services):

IIS is a web server software by Microsoft.

It allows hosting and managing websites on Windows servers.

Used for creating and managing web applications, services, and hosting web pages.

Essential for developers and organizations deploying web-based applications on Windows servers.

* Reinstall IIS with Windows Features:

1. Open Windows Features:
2. Press Win + R to open the Run dialog.
3. Type optionalfeatures and press Enter.
4. Find Internet Information Services (IIS):
5. Scroll down and find "Internet Information Services (IIS)."
6. Check the box next to it.
7. Install IIS:
8. Click "OK" and wait for the installation to complete.
9. Verify IIS Installation:
10. Open a web browser and navigate to http://localhost to see the default IIS page.

* Install .NET Framework 3.5 with Windows Features:

1. Open Windows Features:
2. Press Win + R to open the Run dialog.
3. Type optionalfeatures and press Enter.
4. Find .NET Framework 3.5:
5. Scroll down and find ".NET Framework 3.5 (includes .NET 2.0 and 3.0)."
6. Check the box next to it.
7. Install .NET Framework 3.5:
8. Click "OK" and wait for the installation to complete.
9. Verify .NET Framework Installation:
10. You may not see a separate confirmation, but the feature is now installed and can be used by applications that require it.

* Disable Internet Explorer with Windows Features:

1. Open Windows Features:
2. Press Win + R to open the Run dialog.
3. Type optionalfeatures and press Enter.
4. Find Internet Explorer:
5. Scroll down and find "Internet Explorer."
6. Uncheck the box next to it.
7. Disable Internet Explorer:
8. Click "OK" and wait for the changes to take effect.
9. Verify Internet Explorer is Disabled:
10. Attempt to open Internet Explorer, and it should no longer be available.

* Backup:

Backup is the process of creating a copy or duplicate of important data, files, or information. This copy is stored separately from the original to ensure data recovery in case of loss, corruption, or accidental deletion.

* Restore:

Restore is the process of recovering or bringing back the data from a backup to its original location. It involves using the backup copy to replace or replenish data that may have been lost or compromised.

* Need of Backup:

Data Protection: Safeguards against data loss due to hardware failure, human error, or malicious activities.

Recovery: Provides a way to recover lost or deleted files.

Security: Protects against ransomware and other cyber threats.

Business Continuity: Ensures continuity of operations by minimizing downtime in case of data loss.

Peace of Mind: Offers assurance that valuable data is not permanently lost.

* Tools for Backup:

Windows Backup and Restore: Built-in tool in Windows for creating and managing backups.

File History: Another Windows feature for backing up files over time.

Time Machine (Mac): Apple's built-in backup tool for macOS.

Backup and Sync (Google): Google's tool for backing up files to Google Drive.

Acronis True Image: Third-party software for comprehensive backup solutions.

EaseUS Todo Backup: Another third-party tool for creating backups.

* How to restore:

1. Open Control Panel.
2. Select "System and Security" > "Backup and Restore."
3. Click "Restore my files" or "Restore all users' files."
4. Follow the wizard to restore from a backup.
5. File History (Windows):
6. Open Settings.
7. Go to "Update & Security" > "Backup."
8. Click "Restore files from a current backup."
9. Time Machine (Mac):
10. Open the Time Machine application.
11. Navigate to the date of the backup you want to restore.
12. Select the items you want to restore and click "Restore."

* How to Create a Restore Point (Windows):

1. Open the Control Panel.
2. Go to "System" > "System Protection."
3. In the "System Properties" window, go to the "System Protection" tab.
4. Click "Create" to create a restore point.
5. Enter a description for the restore point and click "Create."
6. Confirm the creation of the restore point.

* Create a Restore Point (Windows):

1. Open System Protection:

• Press Win + S to open the search bar.

• Type "System Protection" and select the matching result.

• In the "System Properties" window, go to the "System Protection" tab.

2. Create a Restore Point:

• Select your system drive (usually C:).

• Click the "Create" button.

• Enter a description for the restore point (e.g., "Before Software Install").

• Click "Create" and wait for the process to complete.

• Click "OK" to close the windows.

* Restore from a Restore Point (Windows):

1. Open System Protection:

• Follow the steps above to open the "System Properties" window.

2. Restore to a Previous State:

• In the "System Properties" window, click the "System Restore" button.

• Click "Next" on the welcome screen.

3. Choose a Restore Point:

• Select "Choose a different restore point" and click "Next."

• Choose a restore point from the list and click "Next."

4. Start the Restore Process:

• Click "Finish" and then "Yes" to confirm.

• Wait for the system to restore to the selected point.

* Take Backup from Another System:

1. Use a Network Location:

• Ensure both systems are on the same network.

• On the source system, share a folder with the files you want to back up.

• On the destination system, navigate to the shared folder.

• Copy the files from the source system to the destination.

* Take Backup with Recuva Backup Tool:

1. Download and Install Recuva:

• Download Recuva from the official website and install it on your computer.

2. Run Recuva:

• Open Recuva and select the type of files you want to recover (or choose "All Files" for a general backup).

3. Choose Location:

• Select the location where you want to back up files from (e.g., a specific drive or folder).

4. Start the Scan:

• Click "Scan" and wait for Recuva to analyze the selected location.

5. Recover Files:

• Once the scan is complete, select the files you want to back up.

• Click "Recover" and choose a destination to save the recovered files.

* Disk Management:

Disk Management is a tool in Windows that helps you manage the storage devices (hard drives and partitions) connected to your computer. It allows you to create, delete, format, and resize partitions, as well as assign drive letters and manage file systems.

* Use of Disk Management:

Partitioning: Create, delete, and resize partitions on your hard drives.

Formatting: Prepare a partition for use by erasing existing data and setting up a file system.

Assigning Drive Letters: Designate a letter (like C: or D:) to each partition for easy access.

Managing Volumes: Control various aspects of your storage volumes.

* Merits of Disk Management Tool:

User-Friendly: Provides a graphical interface for managing storage, making it accessible for users.

Centralized Control: Offers a single place to perform various disk-related tasks.

Prevents Data Loss: Helps prevent accidental data loss by providing clear options and warnings.

Organizes Storage: Facilitates the organization of data by allowing the creation of multiple partitions.

Improves Performance: Allows users to optimize storage for better system performance.

* Where to Find Disk Management Tool:

1. Right-click on the "Start" button.
2. Select "Disk Management" from the menu.

* Operations in Disk Management:

1. Create Partition: Make a new section on your hard drive.
2. Delete Partition: Remove an existing partition.
3. Format: Prepare a partition for storing files.
4. Change Drive Letter: Assign or change the letter associated with a partition.
5. Shrink: Reduce the size of a partition.
6. Extend: Increase the size of a partition.
7. Mark as Active: Designate a partition to start the operating system.
8. Properties: View details about a partition or drive.
9. Initialize Disk: Prepare a new disk for use on the computer.

* Create a New Partition with Disk Management:

1. Open Disk Management:
2. Right-click on the "Start" button.
3. Select "Disk Management."
4. Select Unallocated Space:
5. Right-click on unallocated space on your hard drive.
6. Create a New Simple Volume:
7. Choose "New Simple Volume."
8. Click "Next" on the wizard that appears.
9. Specify Size:
10. Enter the size for the new partition.
11. Click "Next."
12. Assign Drive Letter:
13. Choose a drive letter or let Windows assign one.
14. Click "Next."
15. Format the Partition:
16. Select "NTFS" as the file system.
17. Optionally, give the volume a label.
18. Click "Next" and then "Finish."

* Convert from MBR to GPT with Disk Management:

1. Open Disk Management:
2. Right-click on the "Start" button.
3. Select "Disk Management."
4. Backup Important Data:
5. Before converting, ensure you've backed up important data.
6. Delete Existing Partitions
7. If your disk already has partitions, delete them
8. Right-Click on the Disk:
9. Right-click on the disk in Disk Management.
10. Choose "Convert to GPT Disk."
11. Confirm Conversion:
12. Confirm the conversion. This will erase all data on the disk.

* Create a New Partition from Existing Partition:

1. Open Disk Management:
2. Right-click on the "Start" button.
3. Select "Disk Management."
4. Right-Click on Existing Partition:
5. Right-click on the existing partition you want to split.
6. Choose "Shrink":
7. Choose "Shrink Volume."
8. Enter the amount of space you want to shrink.
9. Create New Simple Volume:
10. Right-click on the unallocated space.
11. Choose "New Simple Volume."
12. Follow the wizard to create a new partition.

* Device Management:

Device Management refers to the process of controlling and maintaining the hardware devices connected to a computer or a network. It involves tasks such as installing, updating, configuring, and troubleshooting devices like printers, scanners, and network adapters.

* Need of Device Management:

Efficiency: Ensures devices work correctly, optimizing system performance.

Compatibility: Manages drivers and configurations for diverse hardware.

Troubleshooting: Facilitates the identification and resolution of device-related issues.

Security: Controls access to devices, enhancing system security.

* Benefits of Device Management:

Smooth Operation: Ensures devices function seamlessly with the computer.

Time and Cost Savings: Reduces downtime and the need for manual device configuration.

Enhanced Productivity: Allows users to focus on tasks rather than dealing with device issues.

Scalability: Easily accommodates new devices and technology changes.

* Access Device Management:

1. Right-click on the "Start" button.
2. Select "Device Manager" from the menu.

* List of Devices in Device Manager:

1. Display Adapters: Graphics cards and display controllers.
2. Sound, Video, and Game Controllers: Audio and video devices.
3. Network Adapters: Ethernet and wireless network devices.
4. Print Queues: Printers and printing devices.
5. Disk Drives: Hard drives and storage devices.
6. Human Interface Devices: Keyboards, mice, and other input devices.
7. Universal Serial Bus controllers (USB): USB devices.
8. Imaging devices: Scanners, cameras, and imaging peripherals.

* Add a Device with Device Manager:

1. Open Device Manager:
2. Right-click on the "Start" button.
3. Select "Device Manager."
4. Add a Device:
5. Right-click on a category where you want to add a device (e.g., "Network Adapters").
6. Select "Scan for hardware changes."
7. Install the Device:
8. Wait for Device Manager to scan for new hardware.
9. If a new device is found, it will be listed.
10. Right-click on the device and choose "Update driver."
11. Follow the prompts to install the driver.
12. Delete a Driver from Device Manager:
13. Open Device Manager:
14. Right-click on the "Start" button.
15. Select "Device Manager."
16. Locate the Device:
17. Find the device whose driver you want to delete.

* Delete the Driver:

1. Right-click on the device and select "Uninstall device."
2. Check the box that says "Delete the driver software for this device."
3. Click "Uninstall."
4. Confirm Deletion:
5. Confirm the action and wait for the process to complete.

* Why Physical Security is Needed:

Physical security is needed to protect people, assets, and information from unauthorized access, theft, vandalism, or harm. It ensures the safety and integrity of physical spaces, assets, and individuals within an organization or environment.

* What is Physical Security:

Physical security that we can protect such as the way of protecting body or a protecting a rare item. This can include access control systems, surveillance cameras, locks, barriers, and other tangible measures to prevent unauthorized entry, theft, or damage to physical resources. It aims to create a secure and protected environment for the people and assets it covers.

* Ways of Physical Security:

Access Control: Restricting entry to authorized personnel through locks, keycards, or biometric systems.

Surveillance: Using cameras to monitor and record activities in and around a physical space.

Perimeter Security: Fencing, barriers, or walls to control and limit access to a specific area.

Security Lighting: Adequate lighting to deter unauthorized activities and enhance visibility.

Alarms and Sensors: Systems that trigger alerts in response to unauthorized entry or unusual activities.

Guards and Personnel: Employing security personnel for physical presence and monitoring.

Identification Badges: Issuing and requiring identification badges for authorized access.

* Protecting Systems from Electrical Fluctuations:

Voltage Regulators: Use voltage regulators to stabilize and control the voltage supplied to electronic devices.

Regular Maintenance: Ensure electrical systems and wiring are regularly inspected and maintained to prevent issues.

Backup Power Sources: Have backup power sources, such as generators, in critical areas to ensure continuous operation during power disruptions.

* Firewall:

A firewall is a security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and untrusted external networks, such as the internet.

* Why Firewall is Needed:

A firewall is needed to:

Protect Against Unauthorized Access: It prevents unauthorized users or malicious software from gaining access to a network.

Control Network Traffic: It regulates the flow of data, allowing or blocking specific types of traffic based on security rules.

Detect and Block Threats: It identifies and blocks potentially harmful data packets, such as viruses and malware.

Enhance Network Security: It adds an additional layer of defense, securing the network and its connected devices from cyber threats.

Ensure Data Privacy: It helps maintain the confidentiality of sensitive information by controlling data access.

* Features of Firewall:

Packet Filtering: Examines data packets and allows or blocks them based on predefined rules.

Stateful Inspection: Monitors the state of active connections to make informed decisions about allowing or blocking traffic.

Proxy Services: Acts as an intermediary between internal and external systems, forwarding requests and responses while masking internal network details.

Network Address Translation (NAT): Modifies network address information in packet headers to hide internal IP addresses.

Logging and Auditing: Records and tracks network activity for analysis and security monitoring.

Virtual Private Network (VPN) Support: Facilitates secure remote access by implementing VPN protocols.

Application Layer Filtering: Analyzes data at the application layer, allowing or blocking traffic based on application type.

* Types of Firewall:

Packet Filtering Firewalls: Examines individual data packets and allows or blocks them based on predefined criteria.

Stateful Inspection Firewalls: Tracks the state of active connections and makes decisions based on the context of the traffic.

Proxy Firewalls: Act as intermediaries between internal and external systems, forwarding requests and responses to enhance security.

Circuit-Level Gateways: Operate at the transport layer and monitor TCP handshakes, allowing or denying connections.

Application Layer Firewalls: Analyze data at the application layer and make decisions based on the specific application or service being used.

Next-Generation Firewalls (NGFW): Combine traditional firewall features with advanced capabilities, such as intrusion prevention and deep packet inspection

* Allow AnyDesk Through Firewall:

1. Open Windows Defender Firewall:
2. Press Win + S to open the search bar.
3. Type "Windows Defender Firewall" and select the matching result.
4. Allow an App Through Firewall:
5. In the left pane, click on "Allow an app or feature through Windows Defender Firewall."
6. Change Settings:
7. Click "Change settings."
8. If prompted, enter your administrator password.
9. Find AnyDesk:
10. Scroll down to find "AnyDesk" in the list of allowed apps.
11. Allow AnyDesk:
12. Ensure both "Private" and "Public" are checked for AnyDesk.
13. Click "OK" to save the changes.
14. Turn Off Firewall Services:
15. Open Windows Defender Firewall:
16. Press Win + S to open the search bar.
17. Type "Windows Defender Firewall" and select the matching result.

* Turn Off Firewall:

1. In the left pane, click on "Turn Windows Defender Firewall on or off."
2. Disable Firewall:
3. Select "Turn off Windows Defender Firewall" for both private and public networks.
4. Click "OK" to save the changes.
5. Block IP Messenger Access:
6. Open Windows Defender Firewall:
7. Press Win + S to open the search bar.
8. Type "Windows Defender Firewall" and select the matching result.
9. Block Program:
10. In the left pane, click on "Advanced settings."
11. Create Outbound Rule:
12. In the left pane, right-click on "Outbound Rules" and choose "New Rule."

* Choose Rule Type:

1. Select "Custom" and click "Next."
2. Choose Program:
3. Choose "This program path" and browse to the location of the IP Messenger executable.
4. Click "Next."
5. Choose Action:
6. Select "Block the connection."
7. Click "Next."
8. Rule Name:
9. Enter a name for the rule (e.g., Block IP Messenger).
10. Click "Finish" to create the rule.