UNIT 2

Software is a set of instructions, data or programs used to operate computers and execute specific tasks. It is logical aspect of computer.

What is computer software?

Computer software is a series of programs, data and instructions used in a computer's hardware to help the device operate and you complete tasks. Hardware is the physical components that comprise a computer, such as the graphics card, data storage and motherboard. Software is important because it allows your computer to perform important tasks while also allowing you to work efficiently on your device.

Types of computer software examples

1. Application software

The most common type of software is application software, or apps, which is performed by the end-user and lets you complete your tasks. An end-user is the individual using the device. Individuals may also refer to these applications as non-essential software. You can install these applications on your devices yourself. Additionally, several types of application software can help you complete many tasks. Here are some types of application software you can use:

- Word processing apps: This type of application allows you to complete writing tasks, such as writing, editing and formatting. With this tool, you can also create and edit tables and print documents as needed.
- Spreadsheet apps: A spreadsheet application can help you complete tasks to compute and organize data. With this tool, you can store business data, create budgets and generate reports and charts.
- Databases: This type of application allows you to store and sort business information in fields, records and files. With a database app, you can enter and edit data, maintain business files and create new records.
- Applications suites: Companies create application suites, which are composed of a few different but related applications. An application suite can have similar interfaces, making it easier for you to navigate between the applications when you're completing tasks.
- Multimedia apps: This type of application can contain a combination of text, animation, audio, video and image content. You can use these tools to create content, assemble and watch videos and record and mix audio tracks.
- Communication apps: Communication applications allow you to connect with other individuals who also have these applications to share text, video and audio. These tools can help you host meetings remotely and work with other professionals who may live across the country.
- Internet browsers: These types of applications allow you to access the internet through different host providers. With this tool, you can access and view websites to help you complete your tasks.
- Email apps: You can these types of applications to write, send, receive and read emails from other individuals. These programs are helpful when you're working or trying to contact other individuals.

2. System software
System software helps you, the hardware of your device and the application software work together to help you complete your tasks. A computer system relies on software systems to allow it to function properly and efficiently. For example, the memory of your device is part of your system software. Unlike the application software, the system software it's not end-user oriented, which means these programs run in the background of your devices instead of you using them. This means you can use the application software while the system software runs in the background to assist the apps' operations.

3. Middleware
Middleware software is the function that helps system software transition to or from application software programs. This can help your device manage communication and data between the two software programs. Types of middleware can include data management, authentication and communication through messages.

4. Driver software
The driver software is part of the system software, and this can help your computer manage the external devices you connect to it. This tool can help the device plugged in to operate as intended. Driver software helps translate the commands of the hardware or device's operating system to complete the task. For each device you have plugged into your computer, it requires one driver software. Often, the external devices come with installed drivers, which means you won't need a third-party installation. If the device doesn't have a built-in driver, you can install your own with a third party.

Here are a few examples of external devices that driver software can help support:

- Printers
- Wireless mice
- Network cards

5. Programming software
Programming software is for coding and not primarily user-end unless you're a professional who uses and writes codes. As a programmer, you can use this type of software to write, produce, inspect and debug application and system software. These programs can help make completing your tasks more productive and efficient. Additionally, coders can use this software as a translator program. A translator program means it interprets program coding language into machine language code. This helps programmers run code by each line and ensure it's correct so the computer can complete basic instructions.

6. Freeware
Freeware software is a type of application that is free for you to download. You can download these programs online and they are in the application software and end-user category. These types of software value and respect an individual's need for community and freedom. Here are a few examples of freeware you can download:

- Instagram

- Facebook
- Adobe Reader
- Skype

7. Open source software

Open-source software is a type of program that allows users to change the coding and share it with other users. You can share these programs with any user and they can use them for a variety of reasons. Here are some examples of open-source software:

- Internet browsers, such as Firefox
- LibreOffice
- GIMP

8. Proprietary software or closed software

Proprietary software, or closed software, is a type of program with coding for users who pay a fee to access it. This means only the author who created the coding and the program has the authority to change the codes and distribute the software. Here are a few examples of proprietary or closed software:

- Microsoft Office
- Java
- Adobe Flash Player

9. Shareware

Shareware software is a type of application that is paid program but offered to users for a trial period before requesting payment for continual usage. During the trial duration, you can use all the features in the application without having to pay a fee. At the end of the trial, the application may ask for payment if you desire to continue to use the program if you like it. When you're given a trial duration, you can assess if you would like to invest financially in it later. Here are a few examples of shareware:

- Netflix
- Adobe Photoshop
- YouTube TV

10. Utility software

Utility software is a type of system software that can help you maintain the health of your device and manage the performance of the programs. You may purchase some of these software programs in-store or online to download on your computer. These programs can scan and analyze your device to find any challenges or make improvements when necessary. Here are a few examples of utility software you can download:

- Antivirus and security
- Data backup
- Disk cleaner and defragment

Programs v/s Software

Software is a broad term that covers the programs and components that it required to run. Software consists the files, whereas a program can itself be a file. Along with these differences, there are various other comparisons between both terms.

Now let's see the comparison chart between the program and software. Here, we are showing the comparison in the tabular format on the basis of some characteristics.

On the basis of	Program	Software
Definition	A computer program is a set of instructions that is used as a process of creating a software program by using programming language.	Software is a set of programs that enables the hardware to perform a specific task.
Types	Programs do not have further categorization.	The software can be of three types: system software, application software, and programming software.
User Interface	A program does not have a user interface.	Every software has a user interface that may be in graphical format or in the form of a command prompt.
Size	Programs are smaller in size, and their size exists between Kilobyte (Kb) to a megabyte (Mb).	Software's are larger in size, and their size exists between megabytes (Mb) to gigabytes (Gb).
Time taken	A program takes less time to be developed.	Whereas software requires more time to be developed.
Features and functionality	A program includes fewer features and limited functionalities.	It has more features and functionalities.
Development approach	The development approach of a program is unorganized, unplanned, and unprocedural.	The development approach of software is well planned, organized, and systematic.

Documentation	There is a lack of documentation in the program.	Softwares are properly documented.
Examples	Examples of the program are - video games functions, malware, and many more.	Examples of software are - Adobe Photoshop, Adobe Reader, Google Chrome, and many more.

Definition of Computer Viruses
A computer virus is a type of malicious software, or malware, that spreads between computers and causes damage to data and software.

Computer viruses aim to disrupt systems, cause major operational issues, and result in data loss and leakage. A key thing to know about computer viruses is that they are designed to spread across programs and systems. Computer viruses typically attach to an executable host file, which results in their viral codes executing when a file is opened. The code then spreads from the document or software it is attached to via networks, drives, file-sharing programs, or infected email attachments.

Common Signs of Computer Viruses

A computer virus will more than likely have an adverse effect on the device it resides on and may be discoverable through common signs of performance loss, including:
Speed of System

A computer system running slower than usual is one of the most common signs that the device has a virus. This includes the system itself running slowly, as well as applications and internet speed suffering. If a computer does not have powerful applications or programs installed and is running slowly, then it may be a sign it is infected with a virus.
Pop-up Windows

Unwanted pop-up windows appearing on a computer or in a web browser are a telltale sign of a computer virus. Unwanted pop-ups are a sign of malware, viruses, or spyware affecting a device.
Programs Self-executing

If computer programs unexpectedly close by themselves, then it is highly likely that the software has been infected with some form of virus or malware. Another indicator of a virus is when applications fail to load when selected from the Start menu or their desktop icon.
Accounts Being Logged Out

Some viruses are designed to affect specific applications, which will either cause them to crash or force the user to automatically log out of the service.

Crashing of the Device

System crashes and the computer itself unexpectedly closing down are common indicators of a virus. Computer viruses cause computers to act in a variety of strange ways, which may include opening files by themselves, displaying unusual error messages, or clicking keys at random.
Mass Emails Being Sent from Your Email Account

Computer viruses are commonly spread via email. Hackers can use other people's email accounts to spread malware and carry out wider cyberattacks. Therefore, if an email account has sent emails in the outbox that a user did not send, then this could be a sign of a computer virus

Changes to Your Homepage

Any unexpected changes to a computer—such as your system's homepage being amended or any browser settings being updated—are signs that a computer virus may be present on the device.
How Do Computer Viruses Attack and Spread?
In the early days of computers, viruses were spread between devices using floppy disks. Nowadays, viruses can still be spread via hard disks and Universal Serial Bus (USB) devices, but they are more likely to be passed between devices through the internet.

Computer viruses can be spread via email, with some even capable of hijacking email software to spread themselves. Others may attach to legitimate software, within software packs, or infect code, and other viruses can be downloaded from compromised application stores and infected code repositories. A key feature of any computer virus is it requires a victim to execute its code or payload, which means the host application should be running.

Types of Computer Viruses

There are several types of computer viruses that can infect devices. This section will cover computer virus protections and how to get rid of computer viruses.
Resident Virus

Viruses propagate themselves by infecting applications on a host computer. A resident virus achieves this by infecting applications as they are opened by a user. A non-resident virus is capable of infecting executable files when programs are not running.
Multipartite Virus

A multipartite virus uses multiple methods to infect and spread across computers. It will typically remain in the computer's memory to infect the hard disk, then spread through and infect more drives by altering the content of applications. This results in performance lag and application memory running low.

Multipartite viruses can be avoided by not opening attachments from untrusted sources and by installing trusted antivirus software. It can also be prevented by cleaning the boot sector and the computer's entire disk.

Direct Action

A direct-action virus accesses a computer's main memory and infects all programs, files, and folders located in the autoexec.bat path, before deleting itself. This virus typically alters the performance of a system but is capable of destroying all data on the computer's hard disk and any USB device attached to it. Direct action viruses can be avoided through the use of antivirus scanners. They are easy to detect, as is restoring infected files.

Browser Hijacker

A browser hijacker manually changes the settings of web browsers, such as replacing the homepage, editing the new tab page, and changing the default search engine. Technically, it is not a virus because it cannot infect files but can be hugely damaging to computer users, who often will not be able to restore their homepage or search engine. It can also contain adware that causes unwanted pop-ups and advertisements.

Browser hijackers typically attach to free software and malicious applications from unverified websites or app stores, so only use trusted software and reliable antivirus software.

Overwrite Virus

Overwrite viruses are extremely dangerous. They can delete data and replace it with their own file content or code. Once files get infected, they cannot be replaced, and the virus can affect Windows, DOS, Linux, and Apple systems. The only way this virus can be removed is by deleting all of the files it has infected, which could be devastating. The best way to protect against the overwrite virus is to use a trusted antivirus solution and keep it updated.

Web Scripting Virus

A web scripting virus attacks web browser security, enabling a hacker to inject web-pages with malicious code, or client-side scripting. This allows cyber criminals to attack major websites, such as social networking sites, email providers, and any site that enables user input or reviews. Attackers can use the virus to send spam, commit fraudulent activity, and damage server files.

Protecting against web scripting is reliant on deploying real-time web browser protection software, using cookie security, disabling scripts, and using malicious software removal tools.

File Infector

A file infector is one of the most common computer viruses. It overwrites files when they are opened and can quickly spread across systems and networks. It largely affects files with .exe or .com extensions. The best way to avoid file infector viruses is to only download official software and deploy an antivirus solution.

Network Virus

Network viruses are extremely dangerous because they can completely cripple entire computer networks. They are often difficult to discover, as the virus could be hidden within any computer

on an infected network. These viruses can easily replicate and spread by using the internet to transfer to devices connected to the network. Trusted, robust antivirus solutions and advanced firewalls are crucial to protecting against network viruses.

Boot Sector Virus

A boot sector virus targets a computer's master boot record (MBR). The virus injects its code into a hard disk's partition table, then moves into the main memory when a computer restarts. The presence of the virus is signified by boot-up problems, poor system performance, and the hard disk becoming unable to locate. Most modern computers come with boot sector safeguards that restrict the potential of this type of virus.

There are common examples of what computer and internet users believe to be viruses, but are technically incorrect.

Is Trojan a Virus?

A Trojan horse is a type of program that pretends to be something it is not to get onto a device and infect it with malware. Therefore, a Trojan horse virus is a virus disguised to look like something it is not. For example, viruses can be hidden within unofficial games, applications, file-sharing sites, and bootlegged movies.

Is a Worm a Virus?

A computer worm is not a virus. Worms do not need a host system and can spread between systems and networks without user action, whereas a virus requires users to execute its code.

Is Ransomware a Virus?

Ransomware is when attackers lock victims out of their system or files and demand a ransom to unlock access. Viruses can be used to carry out ransomware attacks.

Is Rootkit a Virus?

A rootkit is not a virus. Rootkits are software packages that give attackers access to systems. They cannot self-replicate or spread across systems.

Is a Software Bug a Virus?

"Bug" is a common word used to describe problems with computers, but a software bug is not a virus. A bug is a flaw or mistake in software code, which hackers can exploit to launch a cyberattack or spread malware.

How To Prevent Your Computer From Viruses

While the best way is antivirus software, operating systems already come with programs like Windows Defender and Windows Security. There are also other, free programs like Avast and Kaspersky.

They may seem simple, but they're highly effective at destroying Trojan horses, worms and spyware. It's also important to keep on top of updates. There are other ways to prevent viruses infecting your devices:

- Take special care on social media. Never open files without checking their source.
- Close websites when the browser tells you they're not secure.
- Do not accept files from people you don't know.
- Back up your files regularly.

1. Install antivirus or anti-malware software

It might seem obvious, but many home computers don't have this protection. It's essential to keep your PC virus free.

2. Keep your antivirus software up to date

Protective software is one thing; but keeping it up to date is another. While free antivirus software is better than nothing, it's not the best solution. Microsoft has a free security package if you operate with Windows, even though you would've already paid for the Windows licence. Many people don't know about it; but, actually, it's a good form of protection.

3. Run antivirus scans regularly

This might also go without saying, but we often forget to do it. Adjust the settings so scans run at regular intervals (like once a week). Using the device while antivirus software is running can be challenging. Try running it at night when the computer is idle. Because we usually turn our devices off at night, we tend to overlook scans. Set the antivirus software to run on a specific night and only leave the computer on at that time. Make sure it doesn't switch off automatically or go into hibernation mode.

4. Keep your operating system up to date

Whether you use Windows, Mac OS X, Linux or another operating system, always keep it up to date. Developers regularly release patches to plug security leaks. The patches will help keep your system safe. You should also keep your antivirus software up to date. New viruses and malware are emerging constantly. Their software scanning is as sophisticated as their databases, so make sure you're on top of things.

5. Protect your network

Many PCs connect to files, printers and the Internet via Wi-Fi. Make sure the network requires a secure password and never browse on open networks.

Use WPA or WPA2 encryption. PME is no longer secure enough. Expert hackers can circumvent it in minutes. It's also a good idea not to disclose the name of your Wi-Fi network (the SSID). You can connect to the network manually on your device by typing in the SSID and password. If you usually let guests use your Internet, give them an alternative SSID and password just in case.

6. Think before you click

Avoid websites you don't trust. Don't open email attachments from people or companies you don't know. Don't click on links in unwanted emails. Always hover the mouse over a link (especially a short URL) before clicking on it to see where it will take you.

If you need to download something from the Internet, an email, an FTP site, a file exchange service, etc., check it over first. Good antivirus software will do it automatically, although you have to make sure it's running.

7. Keep your personal information secure

This is probably the hardest thing to do on the Internet. Many hackers use social engineering over brute force to access your files. They can gather enough information to hack your online accounts to collect even more data.
They go from account to account until they have all they need to get hold of your bank details and steal your identity. Be careful on message boards and social media. Block all your privacy settings and avoid using your real name in chat forums.
8. Don't use unsecured Wi-Fi
Don't use the free, open Wi-Fi (no password or encryption) in cafés, libraries, airports, etc. Think about it. If you can connect easily, how far can a hacker go?
9. Back up your files
Backing up all your files is the best form of protection. Ideally, keep your files in three places: where you work on them (your computer); an external storage device; and somewhere else. Use a back-up service or get two external hard drives and keep one at work; a relative or a friend's house; or in a safe.
10. Use several secure passwords
Never use the same password twice, especially for bank accounts. We usually use the same email address or username, which are easy to see and steal. If you always use the same password and someone uncovers it, it'll take just a few seconds to hack into all your accounts. Choose a strong password with lower- and upper-case letters, numbers and symbols. Make it easy to remember but difficult to predict. Don't use dates or pets' names.

Antivirus

Antivirus software helps protect your computer against malware and cybercriminals. Antivirus software looks at data — web pages, files, software, applications — traveling over the network to your devices. It searches for known threats and monitors the behavior of all programs, flagging suspicious behavior. It seeks to block or remove malware as quickly as possible.

Antivirus protection is essential, given the array of constantly-emerging cyberthreats. If you don't have protective software installed, you could be at risk of picking up a virus or being targeted by other malicious software that can remain undetected and wreak havoc on your computer and mobile devices.

If you already have antivirus software, you may believe you're all set. But it might not be that simple. With new and savvier cyberthreats and viruses surfacing, it's important to stay current with the latest in antivirus protection.

If there's any crack in your cybersecurity defenses, cybercriminals likely will try to find a way in. Ensuring your antivirus software is up and running, and up-to-date, is a good place to start. However, hackers, scammers, and identity thieves are constantly tweaking their methods, so it's a good idea to get protection from a comprehensive security solution.

What is antivirus software designed to do?

What exactly is antivirus software designed to do? We're talking about a program or umbrella of programs whose purpose is to scan for and eradicate computer viruses and other malicious software, also known as malware. Antivirus software is a vital component of your overall online

and computer security strategy in its protection against data and security breaches along with other threats.

When looked at simply, a computer virus is similar to a cold virus. It's designed to go from one computer or device to the next, copying itself, and spreading malicious codes and programs that can damage and infiltrate your operating systems. Viruses are designed to give criminals access to their victims' devices.

These viruses, spyware, and other malicious software are known as malware, and can be surreptitiously installed on your computer or device. Malware can do everything from crashing your device to monitoring or controlling your online activity. This control may enable hackers to send spam and steal your private information, which could eventually lead to identity theft.

Antivirus software provides protection against these types of threats by performing key tasks:

- Pinpointing specific files for the detection of malicious software
- Scheduling automatic scans
- Scanning either one file or your entire computer at your discretion
- Deleting malicious codes and software
- Confirming the safety of your computer and other devices

As cybercrime evolves and becomes more sophisticated, whether it's your own PC or other devices on a larger network, you don't want to leave yourself or your network vulnerable. If you don't have security software, you could be opening the door for cybercriminals to gain access to your most sensitive information — and potentially garner control over your computer and mobile devices.

What are the different types of antivirus protection?

Several types of antivirus programs have evolved over the years. When setting up your umbrella of protection, it's important to understand the more common antivirus programs available.

Malware signature antivirus

Malware, or malicious software, installs viruses and spyware on your computer or device without your knowledge. Malware can steal your login information, use your computer to send spam, crash your computer system, and essentially give cybercriminals access to your devices and the information stored on them, and even the ability to monitor and control your online activity.

Malware signature antivirus software detects malware signatures, which are digital fingerprints of malicious software. Antivirus protection can scan for specific malicious codes, identify specific viruses, and disable these programs.

While malware signature antivirus protection is key for detecting and eradicating known viruses, one limitation is its inability to address new viruses. The antivirus product simply doesn't contain these new virus signatures.

System monitoring antivirus

This is where system monitoring antivirus software comes into play. This antivirus protection can monitor software and computer systems for behavior that is suspect or atypical of the user.

For instance, alerts are created when a user connects to unfamiliar sites or attempts to access a large number of files, or when there's a significant increase in data usage.

Machine learning antivirus

Another form of protection can be machine learning techniques, which monitor "normal" computer or network behaviors. The machine learning antivirus software is able to limit activities by programs or computers if they look suspicious.

More specifically, machine learning detection implements algorithms to facilitate malware detection that is broader in scope. This type of antivirus protection is beneficial because it works in tandem with other antivirus applications to provide multiple layers of protection.

One example of machine learning is the design of Microsoft's latest antivirus software, which can gather data from more than 400 million computers running on Windows 10 to discover new malware. (Note: To be clear, this is diagnostic data that a consumer can opt out of reporting.) This, in turn, takes us back to the importance of signatures, as this intelligence will allow for the development of new signatures for the latest malware discovered. This automation is key in its ability to stay on top of the latest viruses.