Computer Literacy

What is a computer Virus?

A computer virus is an **executable program**. Depend on the nature of a virus, it may cause damage of your hard disk contents, and/or interfere normal operation of your computer.

By definition, a virus program is able to replicate itself. This means that the virus multiplies on a computer by making copies of itself. This replication is intentional; it is part of the virus program. In most cases, if a file that contains virus is executed or copied onto another computer, then that computer will also be "infected" by the same virus.

A virus can be introduced to a computer system along with any software program. When a virus is introduced to a computer system, it can attach itself to, or sometimes even replace, an existing program. Thus, when the user runs the program in question, the virus is also executed. This usually happens without the user being aware of it.

A virus program contains instructions to initiate some sort of "event" that affects the infected computer. Each virus has an unique event associated with it. These events and their effects can range from harmless to devastating. For examples:

- An annoying message appearing on the computer screen.
- Reduced memory or disk space.
- Modification of data.
- Files overwritten or damaged.
- Hard drive erased.

Main categories of Computer Viruses:

The three main categories are:

- Viruses
- Worms
- Trojans

Viruses: A virus is not independent and spread in computer when it attach itself with a file. viruses first started showing up in the 1990s when the use of email became widespread. Email viruses are able to spread more quickly than traditional viruses, because they are sent via email. One of the most impressive viruses to hit computers was the Melissa virus, which happened in March 1999. The virus was attached to a word document that was downloadable from an Internet newsgroup. Anyone who downloaded that document executed the virus.

Symptoms

Computer viruses are among the most known problem that is affecting online users. The dangers of viruses have gotten a lot of attention over the year, and without simple attention they will continue to spread. Computer viruses cause a number of symptoms such as:

- Computer programs taking longer to load than normal.
- The computer is slower than normal.
- Computer stops responding or freezes frequently.
- Computer crashes and restarts every few minutes.

- The computer does not run as usual.
- Applications on the computer do not work correctly.
- Disks or disk drives are inaccessible.
- Printing items is difficult.
- Error messages appear rapidly.
- Distorted menus and dialog boxes.

Worms: It is independent and spread when enter in a computer. Spread via computer networks. Computer worms are malicious software applications designed to spread via computer networks. Computer worms are one form of malware along with viruses and trojans. A person typically installs worms by inadvertently opening an email attachment or message that contains executable scripts. Once installed on a computer, worms spontaneously generate additional email messages containing copies of the worm.
They may also open TCP ports to create networks security holes for other applications, and they may attempt to "flood" the LAN with spurious Denial of Service (DoS) data transmissions.
Also Known As: malware
Worm was made to have three major effects:
• Replicate itself for the first twenty days of infection
• Replace the victim's web pages with a page stating, "Hacked by Chinese."
• Orchestrated an attack on the White House web server in an attempt to overwhelm it
Different types of Computer Worms.
Email Worms, Instant Messaging Worms, Internet Worms, IRC Worms, File-sharing Networks Worms

Trojans: When enter in a computer hide itself. Steel ID and password. Trojan Horses are actually normal computer programs. A Trojan Horse pretends to be a regular downloadable program, such as a game, but actually does something different—most likely does damage to a computer, like erasing a disk. This is different from a regular virus, because it doesn't attempt to reproduce itself. Trojan Horses do not affect a great number of people because they are discovered quickly.

Sources of Computer Virus:

1.hard disk 2. flash drives 3. floppy disk 4.Website 5.E-mail 6.Removeable disk 7.internet 8. CDs

Types of Viruses:

There are many types of computer viruses:

Memory Resident Virus:
These viruses fix themselves in the computer memory and get activated whenever the OS runs and infects all the files that are then opened.

- **Hideout:** This type of virus hides in the RAM and stays there even after the malicious code is executed. It gets control over the system memory and allocate memory blocks through which it runs its own code, and executes the code when any function is executed.
- **Target:** It can corrupt files and programs that are opened, closed, copied, renamed, etc.
- **Examples:** Randex, CMJ, Meve, and MrKlunky
- **Protection:** Install an antivirus program.

Overwrite Viruses

A virus of this kind is characterized by the fact that it deletes the information contained in the files that it infects, rendering them partially or totally useless once they have been infected.

- **Hideout:** The virus replaces the file content. However, it does not change the file size.
- **Examples:** Way, Trj.Reboot, Trivial.88.D
- **Protection:** The only way to clean a file infected by an overwrite virus is to delete the file completely, thus losing the original content.

  However, it is very easy to detect this type of virus, as the original program becomes useless.

Boot Sector Virus

This type of virus affects the boot sector of a hard disk. This is a crucial part of the disk, in which information of the disk itself is stored along with a program that makes it possible to boot (start) the computer from the disk. This type of virus is also called Master Boot Sector Virus or Master Boot Record Virus.

- **Hideout:** It hides in the memory until DOS accesses the floppy disk, and whichever boot data is accessed, the virus infects it.
- **Examples:** Polyboot.B, AntiEXE
- **Protection:** The best way of avoiding boot sector viruses is to ensure that floppy disks are write-protected. Also, never start your computer with an unknown floppy disk in the disk drive.

Macro Virus:

Macro viruses infect files that are created using certain applications or programs that contain macros, like .doc, .xls, .pps, .mdb, etc. These mini-programs make it possible to automate series of operations so that they are performed as a single action, thereby saving the user from having to carry them out one by one. These viruses automatically infect the file that contains macros, and also infects the templates and documents that the file contains. It is referred to as a type of e-mail virus.

- **Hideout:** These hide in documents that are shared via e-mail or networks.
- **Examples:** Relax, Melissa.A, Bablas, O97M/Y2K
- **Protection:** The best protection technique is to avoid opening e-mails from unknown senders. Also, disabling macros can help to protect your useful data.

Directory Virus:

Directory viruses (also called Cluster Virus/File System Virus) infect the directory of your computer by changing the path that indicates the location of a file. When you execute a program file with an extension .EXE or .COM that has been infected by a virus, you are unknowingly running the virus program, while the original file and program is previously moved by the virus. Once infected, it becomes impossible to locate the original files.

- **Hideout:** It is usually located in only one location of the disk, but infects the entire program in the directory.
- **Examples:** Dir-2 virus
- **Protection:** All you can do is, reinstall all the files from the backup that are infected after formatting the disk.

Hacking

Hackers can be people who are career criminal. They are competent and highly skilled at using computers. Once they analyze and discover a leak point in the target system, they will find ways to access and attack the system. They can use various kinds of attacks or even develop their own ways to attack the computer system. For example, they may access a system, and create bogus information or try to create an information flood. They can also break through Web servers to access or steal information.

Email Bombing and Spamming

Email bombing is characterised by abusers repeatedly sending an identical email message to a particular address. Email spamming is a variant of bombing; it refers to sending email to hundreds or thousands of users. Email spamming can be made worse if recipients reply to the email, causing all the original addressees to receive the reply. It may also occur innocently, as a result of sending a message to mailing lists and not realizing that the list explodes to thousands of users, or as a result of an incorrectly set-up auto-responder message [6]. Email bombing/spamming may be combined with email spoofing making it more difficult to determine who the email is actually coming from. If your email system looks slow or email doesn't appear to be sent or received, the reason may be that your mailer is trying to process a large number of messages. When large amounts of email are directed to or through a single site, the site may suffer a denial of service through loss of network connectivity, system crashes, or failure of a service because of overloading network connections, using all available system resources and filling the disk as a result of multiple postings and resulting syslog entries.

What is spam?

Spam is flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it. Most spam is commercial advertising, often for dubious products, get-rich-quick schemes, or quasi-legal services. Spam costs the sender very little to send -- most of the costs are paid for by the recipient or the carriers rather than by the sender.

There are two main types of spam, and they have different effects on Internet users. Cancellable Usenet spam is a single message sent to 20 or more Usenet newsgroups. (Through long experience, Usenet users have found that any message posted to so many newsgroups is often not relevant to most or all of them.) Usenet spam is aimed at "lurkers", people who read newsgroups but rarely or never post and give their address away. Usenet spam robs users of the utility of the newsgroups by overwhelming them with a barrage of advertising or other irrelevant posts. Furthermore, Usenet spam subverts the ability of system administrators and owners to manage the topics they accept on their systems.

Email spam targets individual users with direct mail messages. Email spam lists are often created by scanning Usenet postings, stealing Internet mailing lists, or searching the Web for addresses. Email spams typically cost users money out-of-pocket to receive. Many people - anyone with measured phone service - read or receive their mail while the meter is running, so to speak. Spam costs them additional money. On top of that, it costs money for ISPs and online services to transmit spam, and these costs are transmitted directly to subscribers.
One particularly nasty variant of email spam is sending spam to mailing lists (public or private email discussion forums.) Because many mailing lists limit activity to their subscribers, spammers will use automated tools to subscribe to as many mailing lists as possible, so that they can grab the lists of addresses, or use the mailing list as a direct target for their attacks.

Antivirus:

Definition: "antivirus" is protective software designed to defend your computer against malicious software. Malicious software, or "malware" includes: viruses, Trojans, keyloggers, hijackers, dialers, and other code that vandalizes or steals your computer contents. In order to be an effective defense, your antivirus software needs to run in the background at all times, and should be kept updated so it recognizes new versions of malicious software.
Also Known As: anti-virus, anti virus

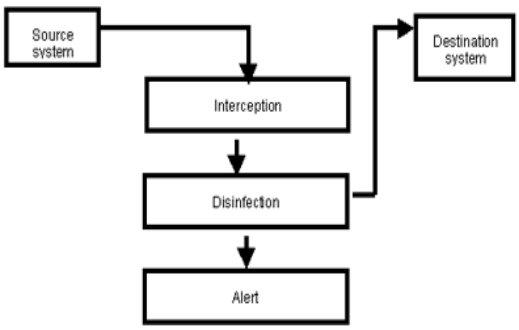
Top Anti Virus Software

- The Shield Deluxe 2009 Antivirus & Antispyware
- Webroot Antivirus with Antispyware 6.0
- BitDefender Antivirus 2009
- CA Anti-Virus Plus 2009
- McAfee VirusScan Plus 2009
- Norton Antivirus 2009
- ESET NOD 32 3.0

- Avast Antivirus
- Panda Antivirus
-

How anti-virus work:

An antivirus program is no more than a system for analyzing information and then, if it finds that something is infected, it disinfects it. The information is analyzed (or scanned) in different ways depending on where it comes from. An antivirus will operate differently when monitoring floppy disk operations than when monitoring e-mail traffic or movements over a LAN. The principal is the same but there are subtle differences.



The information is in the 'Source system' and must reach the 'Destination system'. The source system could be a floppy disk and the destination system could be the hard disk of a computer, or the origin an ISP in which a message is stored and the destination, the Windows communication system in the client machine, Winsock.
The information interpretation system varies depending on whether it is implemented in operating systems, in applications or whether special mechanisms are needed.
The interpretation mechanism must be specific to each operating system or component in which the antivirus is going to be implemented,

Site License

Definition - What does Site License mean?
A site license is used when purchasing software for single site usages but with multiple users. It denotes the usage of purchased, rights-protected work used by multiple users at a single location. These users are granted permission to access copy protected work, but only at that particular location.

Agreements of site licenses sometimes include a set of limitations on the number of software copies made by end users. Simultaneous computer usage of copyrighted digital information is made possible by site licensure.

This term is also known as software licensing.
Techopedia explains Site License
Site licensing is less costly than purchasing multiple copies of protected works. However, users cannot take copies of the digital media outside of the location specified in the site license. Site license agreements must be observed for license holders to protect themselves against liability.

Privacy:

Privacy International's mission is to defend the right to privacy across the world, and to fight surveillance and other intrusions into private life by governments and corporations. Our vision is a world in which privacy is protected by governments, respected by corporations and cherished by individuals. PI was founded in 1990 and is the oldest international privacy organisation in the world.

Privacy is the right to control who knows what about you, and under what conditions. The right to share different things with your family, your friends and your colleagues. The right to know that your personal emails, medical records and bank details are safe and secure. Privacy is essential to human dignity and autonomy in all societies.

The right to privacy is a qualified fundamental human right - meaning that if someone wants to take it away from you, they need to have a damn good reason for doing so.

The world is changing. Technology is transforming our lives and relationships. The threat of terrorism is giving governments carte blanche to ramp up state surveillance and curtail civil liberties. We believe that technological developments should strengthen, rather than undermine, the right to a private life, and that everyone's personal information and communications must be carefully safeguarded, regardless of nationality, religion, personal or economic status. That's why we do what we do.

Internet security

Internet security is a branch of computer security specifically related to the Internet, often involving browser security but also network security on a more general level as it applies to other applications or operating systems on a whole. Its objective is to establish rules and measures to use against attacks over the Internet. The Internet represents an insecure channel for exchanging information leading to a high risk of intrusion or fraud, such as phishing. Different methods have been used to protect the transfer of data, including encryption.
Internet security relies on specific resources and standards for protecting data that gets sent through the Internet. This includes various kinds of encryption such as Pretty Good Privacy (PGP). Other aspects of a secure Web setup includes firewalls, which block unwanted traffic, and anti-malware, anti-spyware and anti-virus programs that work from specific networks or devices to monitor Internet traffic for dangerous attachments.

Internet security is generally becoming a top priority for both businesses and governments. Good Internet security protects financial details and much more of what is handled by a business or agency's servers and network hardware. Insufficient Internet security can threaten to collapse an e-commerce business or any other operation where data gets routed over the Web.

Types of security:

- Network layer security
- Electronic mail security (E-mail)
- Firewalls
- Antivirus

Computer Network

What is Computer Network?

Networks are collections of computers, software, and hardware that are all connected to help their users work together. A network connects computers by means of cabling systems, specialized software, and devices that manage data traffic. A network enables users to share files and resources, such as printers, as well as send messages electronically (e-mail) to each other.

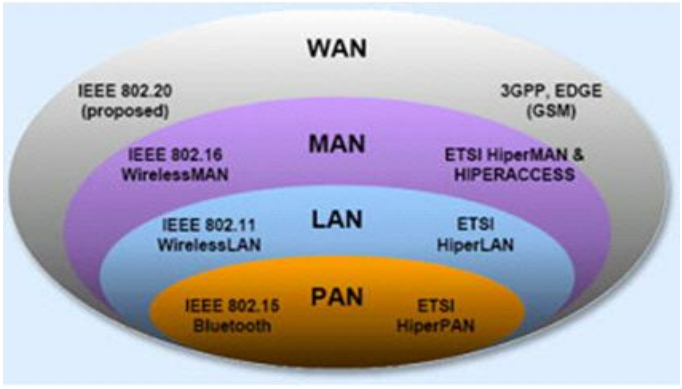
Computer Network Types:
Computer networks fall into two main types:

- client/server networks
- peer-to-peer networks.

A client/server network uses one or more dedicated machines (the server) to share the files, printers, and applications. A peer-to-peer network allows any user to share files with any other user and doesn't require a central, dedicated server.

Most common networks:

- Local Area Networks or LANs
- Wide Area Networks or WANs
- Metropolitan Area Network or MAN
- Wireless Local Area Network or WLAN
- SAN - Storage Area Network, System Area Network, Server Area Network, or sometimes Small Area Network
    - CAN - Campus Area Network, Controller Area Network, or sometimes Cluster Area Network
    - PAN - Personal Area Network
    - DAN - Desk Area Network



Some of these are described below:

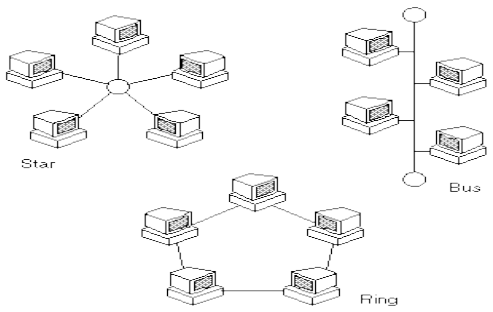
Local Area Network:

A LAN connects network devices over a relatively short distance. A networked office building, school, or home usually contains a single LAN, though sometimes one building will contain a few small LANs (perhaps one per room).

Types of Local-Area Networks (LANs)

Following characteristics differentiate one LAN from another:

- **Topology :** The geometric arrangement of devices on the network. For example, devices can be arranged in a ring or in a straight line etc.
    1. Ring topology
    2. Star topology
    3. Bus topology

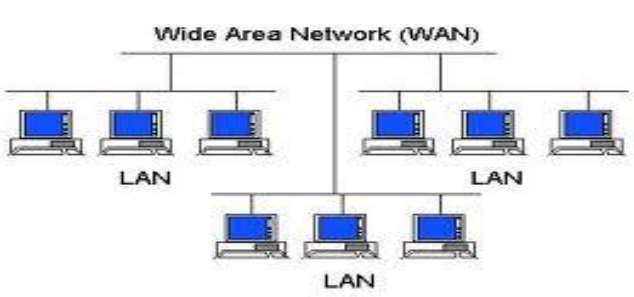


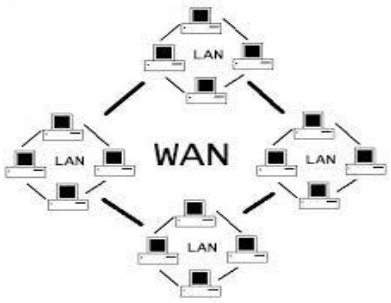
- **Protocols :** The rules and encoding specifications for sending data. The protocols also determine whether the network uses a peer-to-peer or client/server architecture.
- **Media :** Devices can be connected by twisted-pair wire, coaxial cables, or fiber optic cables. Some networks do without connecting media altogether, communicating instead via radio waves.

Wide Area Network

As the term implies, a WAN spans a large physical distance. The Internet is the largest WAN, spanning the Earth.

A WAN is a geographically-dispersed collection of LANs. A network device called a router connects LANs to a WAN. In IP networking, the router maintains both a LAN address and a WAN address.





Metropolitan Area Network

A network spanning a physical area larger than a LAN but smaller than a WAN, such as a city. A MAN is typically owned an operated by a single entity such as a government body or large corporation.

NETWORK TOPOLOGY