Computer malware risks

Malware is software designed to infiltrate or damage a computer system without the owner's informed consent.

- Malware includes computer viruses, worms, most rootkits, spyware, dishonest adware, and other malicious and unwanted software.
- A computer virus is a malicious code, if executed, replicates itself by modifying other computer programs and inserting its own code.
- it is designed to spread from host to host

How computer viruses spread

- In order to infect a computer, a virus has to have the chance to execute its code. This occurs in any of the following ways ;

(i) Booting a PC from an infected medium such as a floppy.

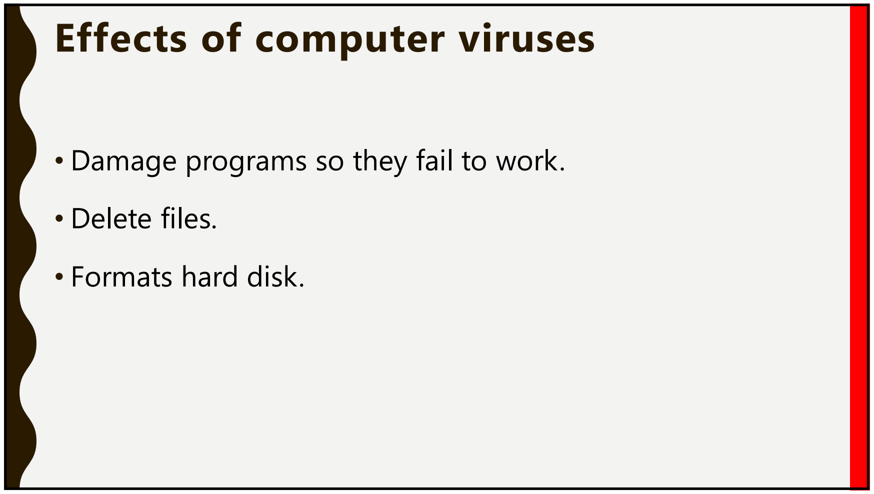
(ii) Executing an infected program.

(iii) Opening an infected file.

iv) via e-mail attachments.

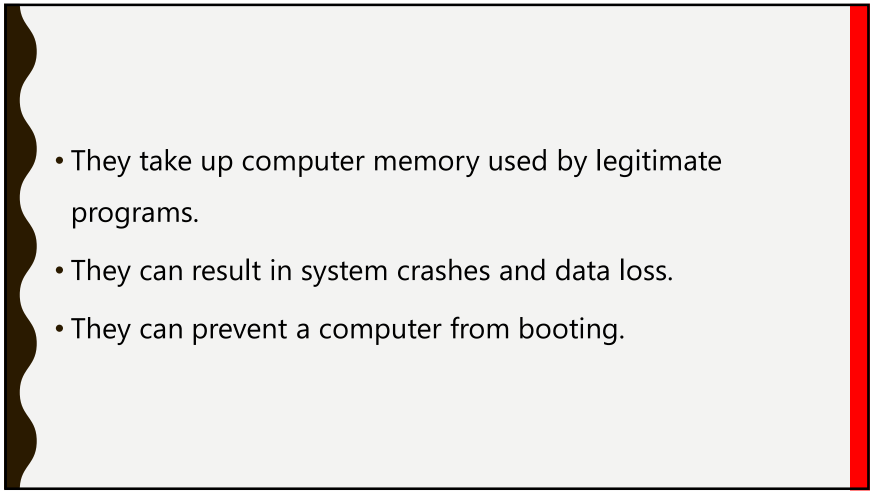
v) sending it over a network or the Internet.

vi) using an infected removable medium such as a floppy disk, CD, or USB drive in a computer.

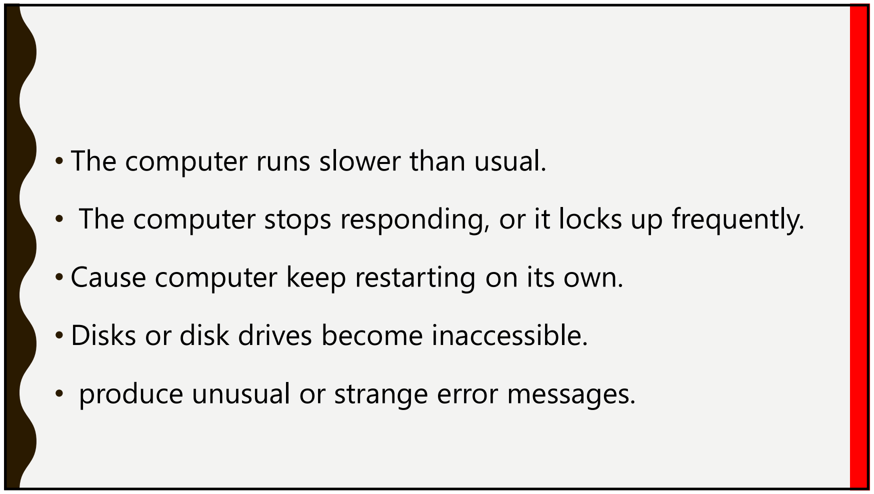


Effects of computer viruses

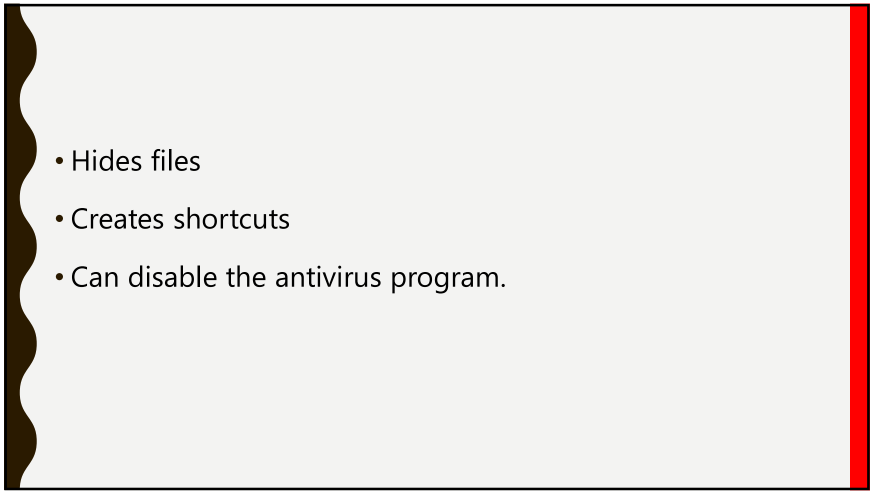
- Damage programs so they fail to work.
- Delete files.
- Formats hard disk.



- They take up computer memory used by legitimate programs.
- They can result in system crashes and data loss.
- They can prevent a computer from booting.



- The computer runs slower than usual.
- The computer stops responding, or it locks up frequently.
- Cause computer keep restarting on its own.
- Disks or disk drives become inaccessible.
- produce unusual or strange error messages.



- Hides files
- Creates shortcuts
- Can disable the antivirus program.

- It shuts down unexpectedly or crashes frequently.
- It experiences memory problems or runs out of disc space.
- Unusual files or directories appear on your system.

Virus types

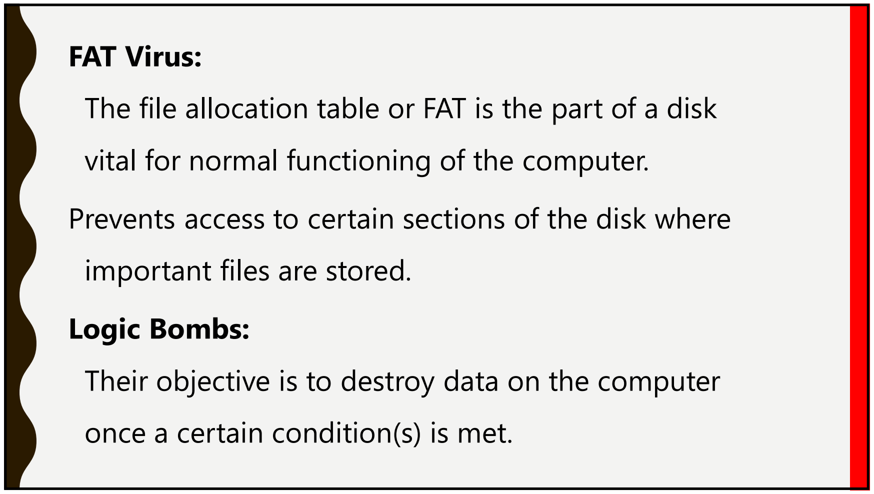
- the Nonresident viruses which immediately search for other hosts that can be infected, infect these targets,

  They are activated when an infected application runs.
- The Resident viruses loads into memory each time the computer is started, they do not search for hosts.

- The Resident virus stays active in the background and infects new hosts when those files are accessed by other programs or the operating system itself.

- **Boot Virus**

  This type of virus affects the boot sector of a hard disk. Making it impossible the computer to boot.
- **Macro Virus.** These infect files that are created using certain applications or programs that contain macros (recorded commands that automate given) set of operations.



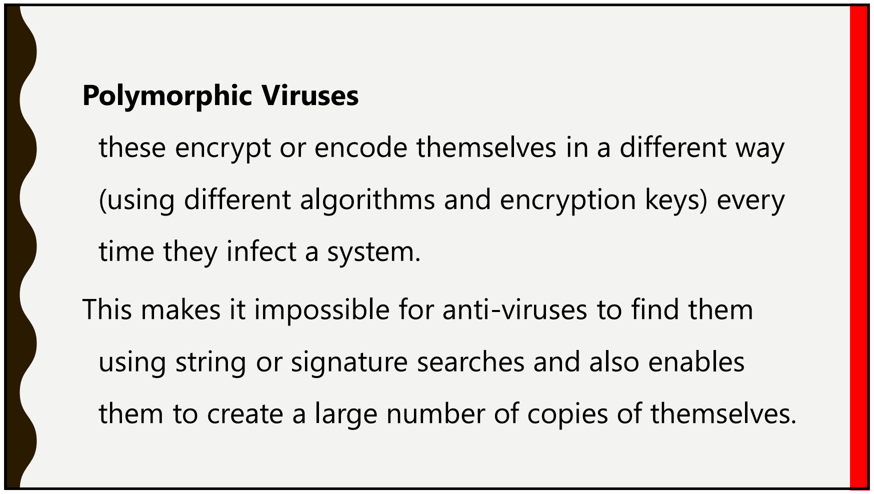
FAT Virus:

The file allocation table or FAT is the part of a disk vital for normal functioning of the computer.

Prevents access to certain sections of the disk where important files are stored.

Logic Bombs:

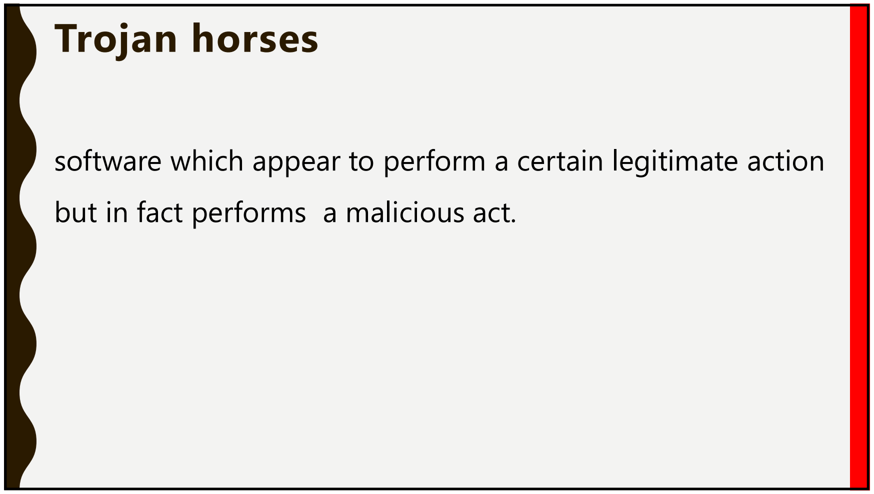
Their objective is to destroy data on the computer once a certain condition(s) is met.



Polymorphic Viruses

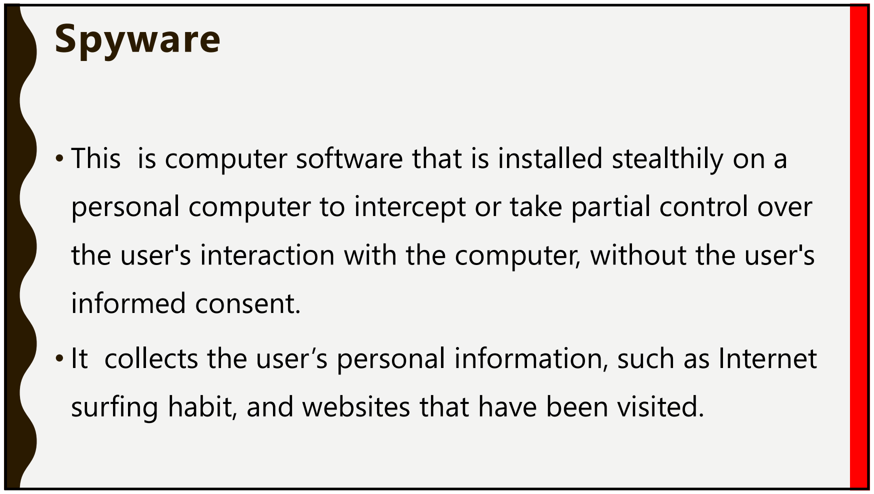
these encrypt or encode themselves in a different way (using different algorithms and encryption keys) every time they infect a system.

This makes it impossible for anti-viruses to find them using string or signature searches and also enables them to create a large number of copies of themselves.



Trojan horses

software which appear to perform a certain legitimate action but in fact performs a malicious act.



Spyware

- This is computer software that is installed stealthily on a personal computer to intercept or take partial control over the user's interaction with the computer, without the user's informed consent.
- It collects the user’s personal information, such as Internet surfing habit, and websites that have been visited.

Adware

- This is a software which automatically plays, displays, or downloads advertising material to a computer after it is installed or while the application is being used. Some types of adware are also spyware and can be classified as privacy-invasive software.

How to prevent or fight computer viruses

- install an updated anti-virus program to block possible virus attack
- Do regular disk and file scans for viruses.
- Avoid using foreign movable disks on you're your computer.
- Avoid opening strange e-mail attachments.
- Activate an antivirus shield and firewall to block virus attacks

- **<u>Virus protection utility</u>:** Antivirus software programs scan for computer viruses and removes them.
- Examples of common anti virus packages include:

- Norton Avast
- F-Secure McAfee
- Panda eScan
- Avira Kaspersky etc

Uses of the antivirus

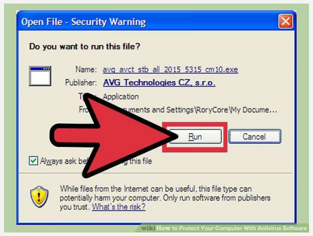
- Detects computer viruses by scanning for viruses.
- Removes the detected viruses
- Blocks/prevents computer virus attack/ real time protection from incoming threats by scanning files being downloaded or disks being inserted into the system before opening them

- Provides automatic updates, because an out of date antivirus program will not be able to detect the newest viruses.
- Can work as a firewall by alerting the user when a program is trying to access the computer.
- Blocks popups

- Protects the computer from other kinds of malware like adware, keyloggers (keystroke or keyboard capturing), backdoors and worms.

How to use an anti virus

- The anti virus can be acquired as a free package or buy one
- Install the anti-virus by running its installer



Open File - Security Warning

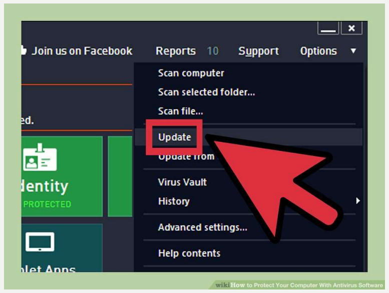
Do you want to run this file?

Name: avg_avct_stb_all_2015_5315_cm10.exe
Publisher: AVG Technologies CZ, s.r.o.
T... Application
Fro... ...uments and Settings\RoryCore\My Docume...

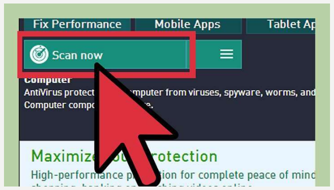
☑ Always ask be... ...g this file

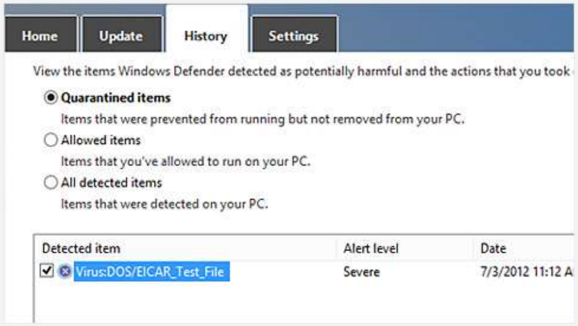
While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

- Once installed, there is need to update regularly



- Regularly scan the computer for viruses
- The antivirus can clean the disk by removing the viruses or quarantining them in case it fails to remove them.


Fix Performance
Mobile Apps
Tablet Ap
Scan now
Computer
AntiVirus protect mputer from viruses, spyware, worms, and
Computer compo e.
Maximize rotection
High-performance p ion for complete peace of mind



View the items Windows Defender detected as potentially harmful and the actions that you took

● Quarantined items

Items that were prevented from running but not removed from your PC.

○ Allowed items

Items that you've allowed to run on your PC.

○ All detected items

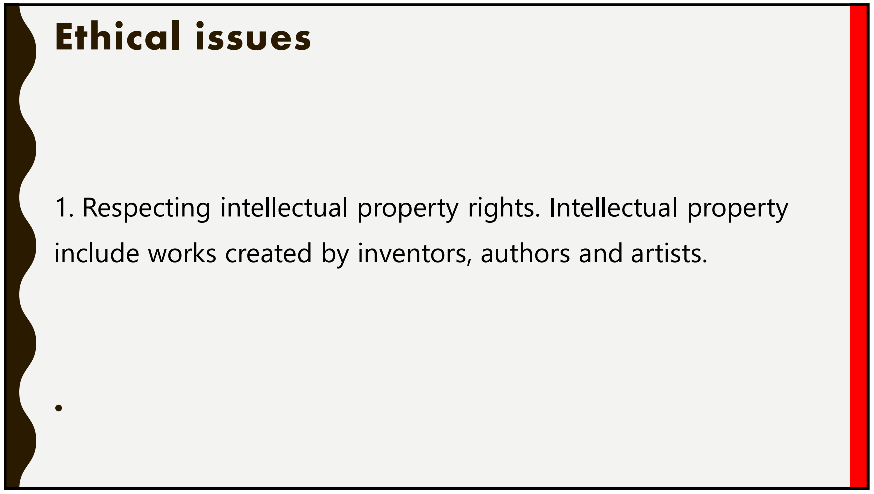
Items that were detected on your PC.

Detected item	Alert level	Date
☑ Virus:DOS/EICAR_Test_File	Severe	7/3/2012 11:12 A

- The anti-virus can be configured to work as a shield against any possible virus attack by blocking them from installing

Ethics and integrity when using computers

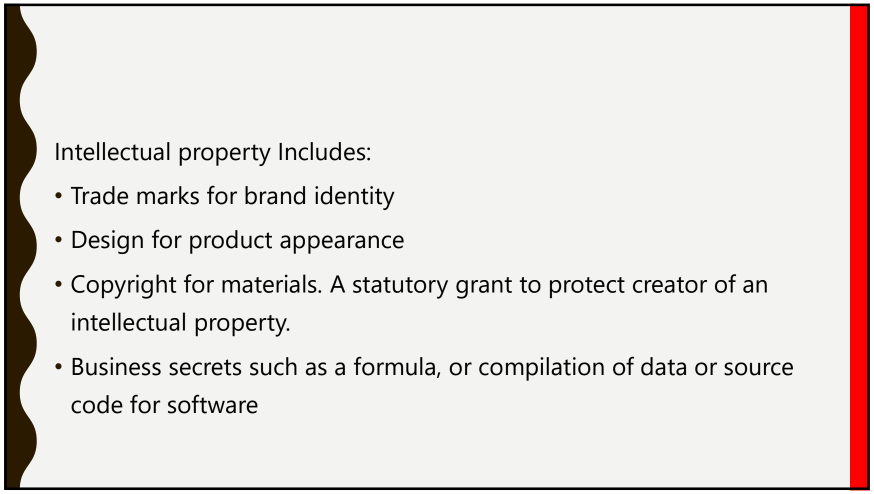
- Computer ethics is the set of moral principles that guide computer usage.
- Ethics deals with the procedures, values and practices that should be followed when using computers without damaging or violating the moral values and beliefs of society.



Ethical issues

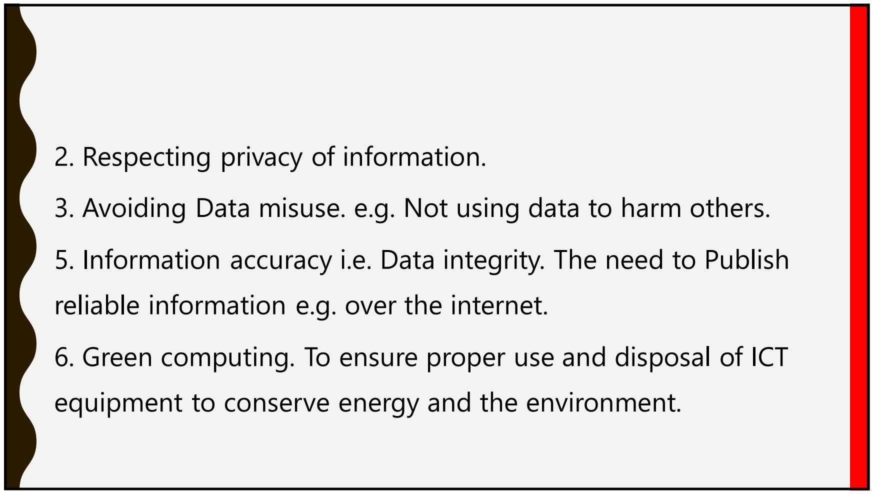
1. Respecting intellectual property rights. Intellectual property include works created by inventors, authors and artists.

•



Intellectual property Includes:

- Trade marks for brand identity
- Design for product appearance
- Copyright for materials. A statutory grant to protect creator of an intellectual property.
- Business secrets such as a formula, or compilation of data or source code for software

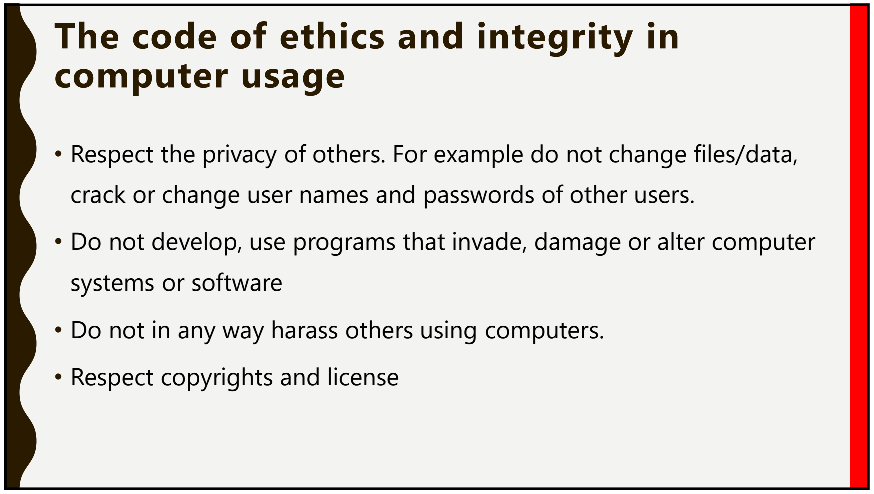


2. Respecting privacy of information.

3. Avoiding Data misuse. e.g. Not using data to harm others.

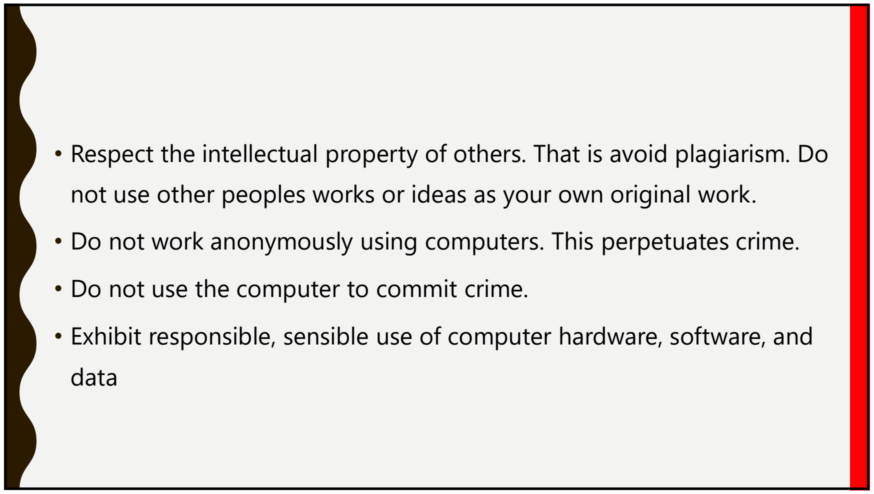
5. Information accuracy i.e. Data integrity. The need to Publish reliable information e.g. over the internet.

6. Green computing. To ensure proper use and disposal of ICT equipment to conserve energy and the environment.

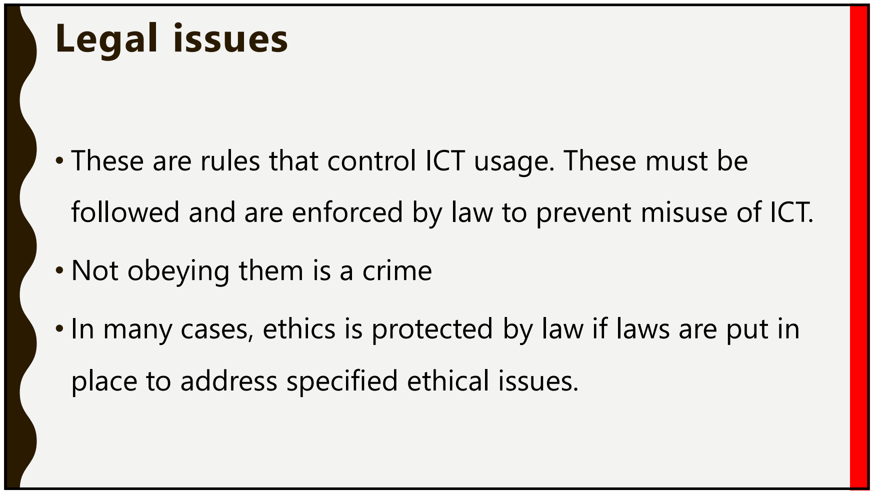


The code of ethics and integrity in computer usage

- Respect the privacy of others. For example do not change files/data, crack or change user names and passwords of other users.
- Do not develop, use programs that invade, damage or alter computer systems or software
- Do not in any way harass others using computers.
- Respect copyrights and license

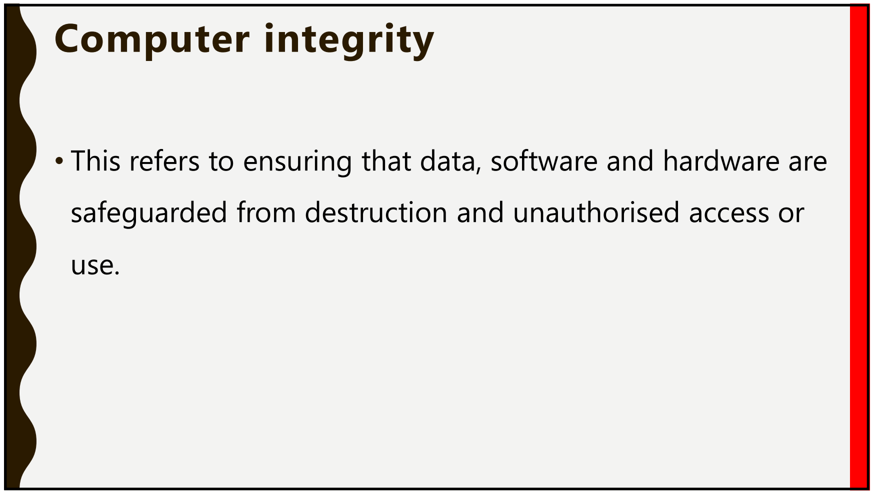


- Respect the intellectual property of others. That is avoid plagiarism. Do not use other peoples works or ideas as your own original work.
- Do not work anonymously using computers. This perpetuates crime.
- Do not use the computer to commit crime.
- Exhibit responsible, sensible use of computer hardware, software, and data



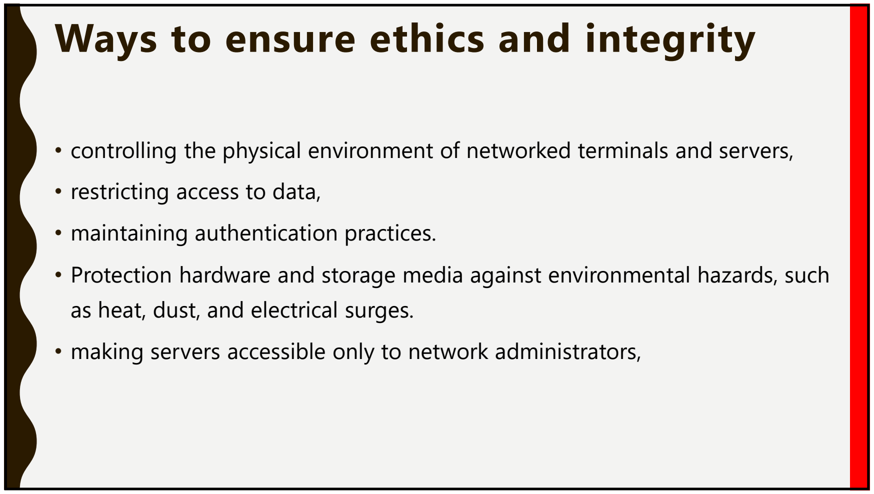
Legal issues

- These are rules that control ICT usage. These must be followed and are enforced by law to prevent misuse of ICT.
- Not obeying them is a crime
- In many cases, ethics is protected by law if laws are put in place to address specified ethical issues.



Computer integrity

- This refers to ensuring that data, software and hardware are safeguarded from destruction and unauthorised access or use.



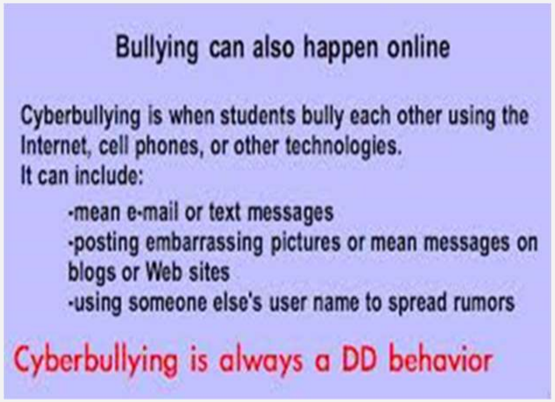
Ways to ensure ethics and integrity

- controlling the physical environment of networked terminals and servers,
- restricting access to data,
- maintaining authentication practices.
- Protection hardware and storage media against environmental hazards, such as heat, dust, and electrical surges.
- making servers accessible only to network administrators,

Common crimes commited using computers

- Writing malicious codes to infect computers i.e. viruses
- Accessing of computer resources illegally (hacking)
- Using software without license (piracy)
- Physically stealing hardware
- Phishing- obtaining others' particulars like passwords and usernames without their informed consent.
- Spamming (sending unsolicited messages)

- Cyber bullying. The use of Information Technology to harm or harass other people in a deliberate, repeated, and hostile manner.



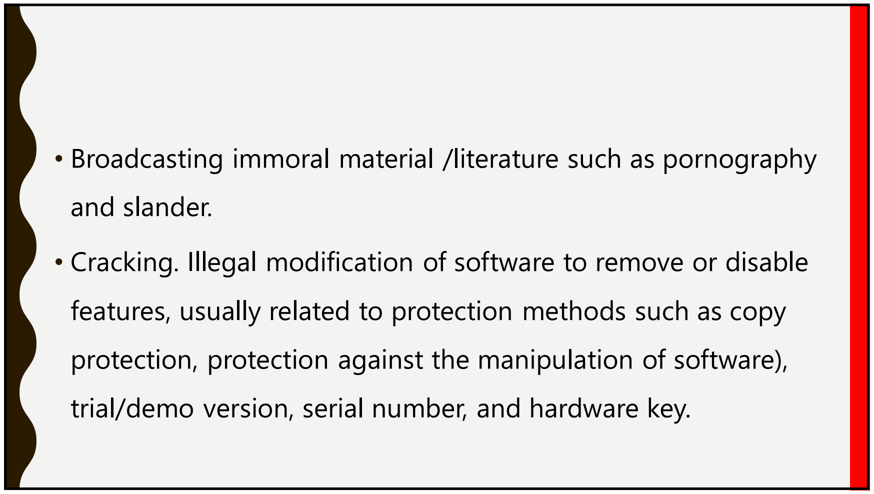
Bullying can also happen online

Cyberbullying is when students bully each other using the Internet, cell phones, or other technologies.
It can include:

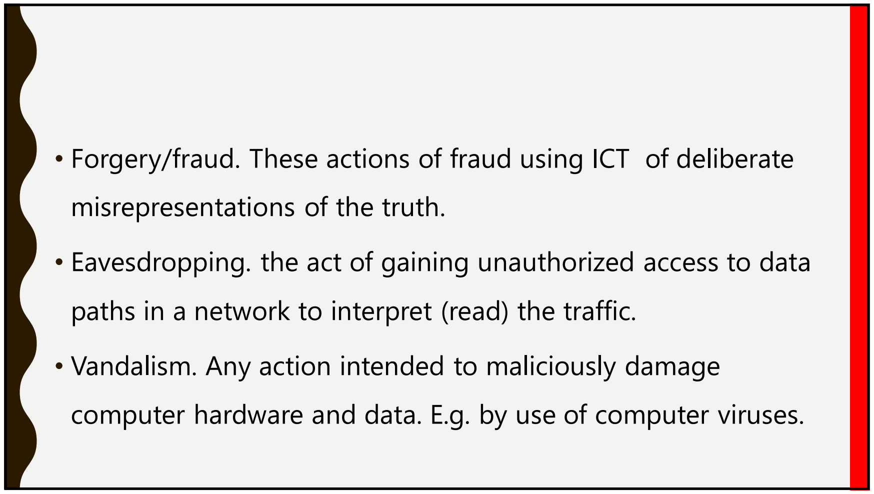
-mean e-mail or text messages
-posting embarrassing pictures or mean messages on blogs or Web sites
-using someone else's user name to spread rumors

Cyberbullying is always a DD behavior

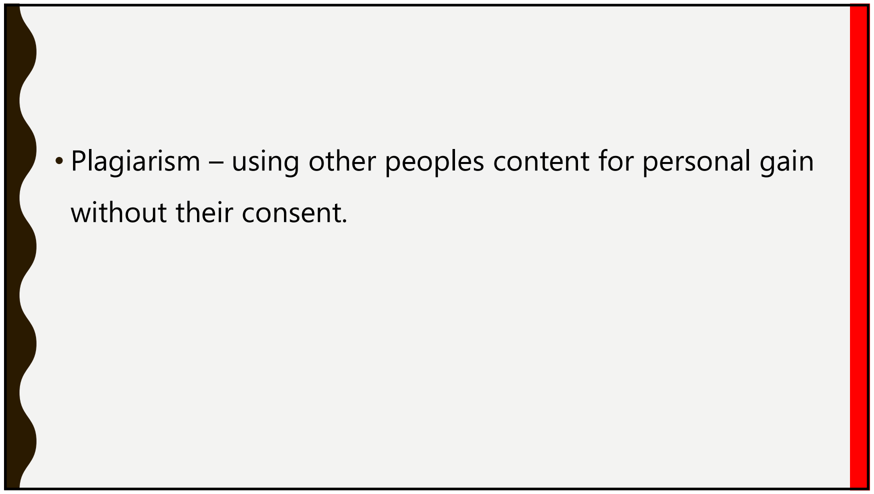
- Cyber terrorism. the politically motivated use of computers and information technology to cause severe disruption or widespread fear in society e.g. large-scale disruption of computer networks on the internet by the means of tools such as computer viruses.



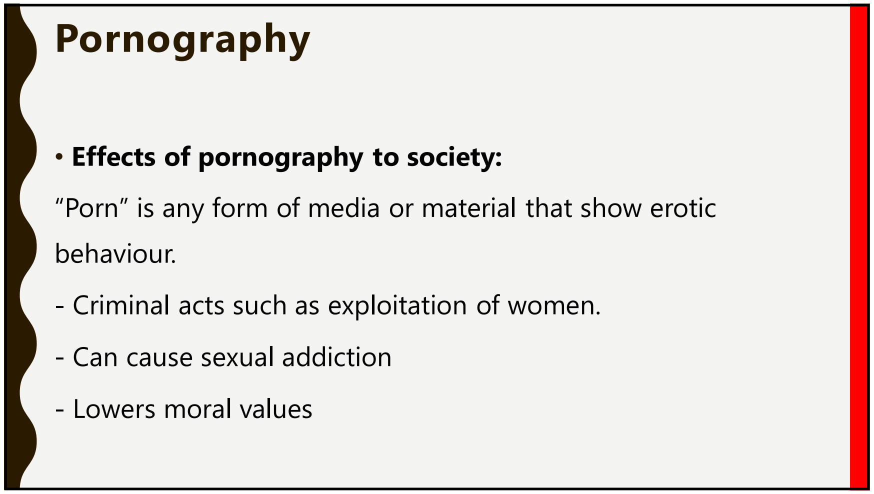
- Broadcasting immoral material /literature such as pornography and slander.
- Cracking. Illegal modification of software to remove or disable features, usually related to protection methods such as copy protection, protection against the manipulation of software), trial/demo version, serial number, and hardware key.



- Forgery/fraud. These actions of fraud using ICT of deliberate misrepresentations of the truth.
- Eavesdropping. the act of gaining unauthorized access to data paths in a network to interpret (read) the traffic.
- Vandalism. Any action intended to maliciously damage computer hardware and data. E.g. by use of computer viruses.



- Plagiarism – using other peoples content for personal gain without their consent.



Pornography

- **Effects of pornography to society:**

"Porn" is any form of media or material that show erotic behaviour.

- Criminal acts such as exploitation of women.

- Can cause sexual addiction

- Lowers moral values

Slander

- False spoken statements about someone, intended to damage his/her reputation
- Effects:

- Disregard of honesty and truth

- Causes negative attitudes towards others

Misuse of Data

Data stored could be misused in the following ways:

- Data could be deleted accidentally or maliciously
- Data could be forwarded to a third party without the knowledge of the owner of data.
- Data could be altered unknowingly or knowingly to falsify information.
- Data could be used to blackmail others.
- Data could be used to propagate cybercrime.

Ways to reduce misuse of personal data on a computer

- Use of user accounts with strong passwords
- Saving documents which are password enabled
- Limit connections to other computer networks.

❑Encrypt data. Data encryption is the act of changing electronic information into an unreadable state

❑Use filtering software(firewall)

- Enact and enforce data protection laws .i.e. If you handle personal information about individuals, you have a number of legal obligations to protect that information under the Data Protection or information Privacy Act.
- Limit physical access to your computer.
- Use of biometric facilities to limit access

- Keeping transmission media (such as cables and connectors) covered and protected to ensure that they cannot be tapped,
- Creating disaster recovery plans for occurrences such as power outages, server failure, and virus attacks.
- Putting in place a strong copyright law

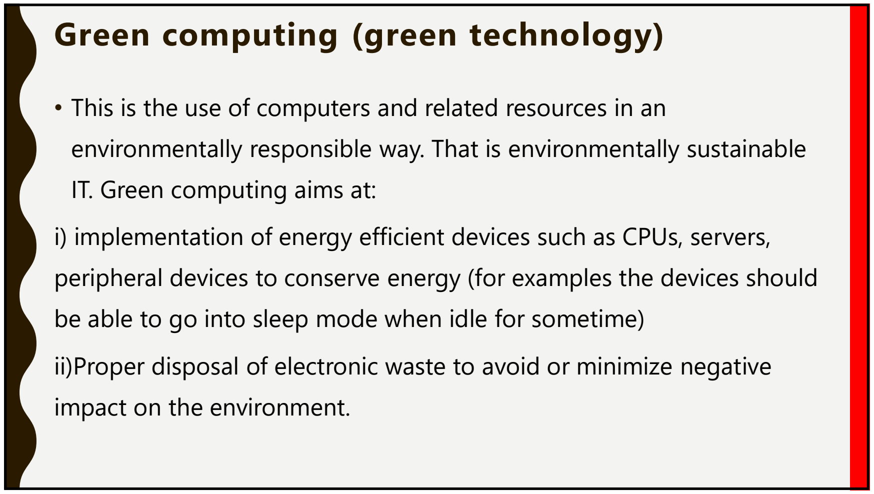
How to prevent/safeguard against computer crime

- Use of passwords
- Burglar proofing
- Enforcing copy right laws.
- Log off or log out from your account after use.
- Sensitization of the public about dangers of computer crimes.
- Using biometric devices e.g. face, finger prints, Voice, iris detection devices etc.

- Encryption of data
- Blocking some websites.

How to prevent software piracy

- Use of product key/serial key
- Sensitizing users on the dangers of acquiring and using software illegally.
- Use of holograms, a component which comes with the original and cannot be duplicated.
- Require software authentication/determine whether software is genuine or counterfeit and activation.
- Incorporate flexible licensing.
- Prosecute the software pirates
- Institute and enforce a copyright law

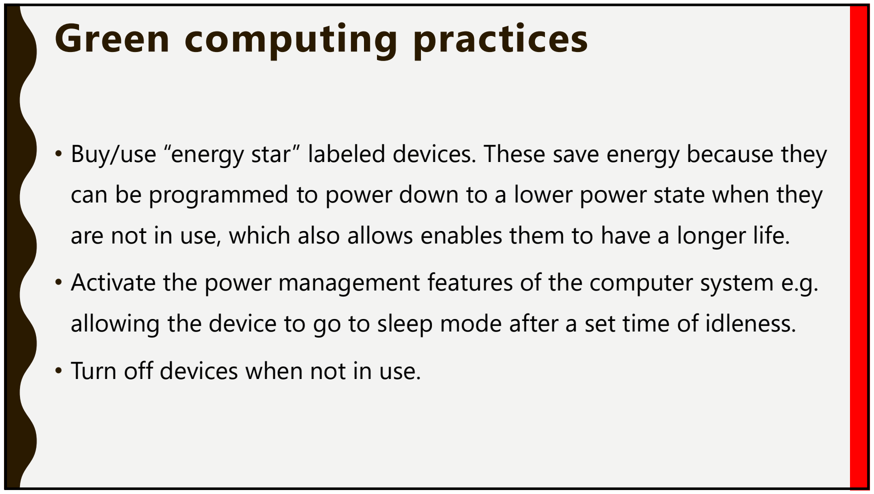


Green computing (green technology)

- This is the use of computers and related resources in an environmentally responsible way. That is environmentally sustainable IT. Green computing aims at:

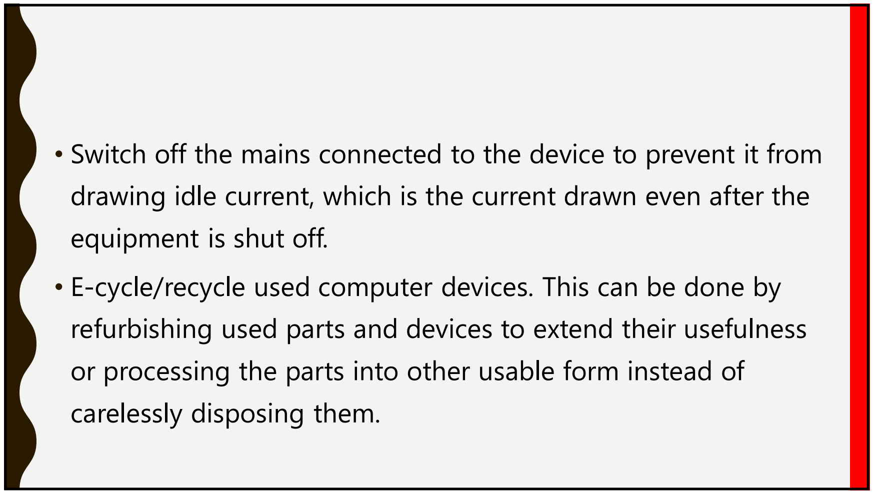
i) implementation of energy efficient devices such as CPUs, servers, peripheral devices to conserve energy (for examples the devices should be able to go into sleep mode when idle for sometime)

ii)Proper disposal of electronic waste to avoid or minimize negative impact on the environment.

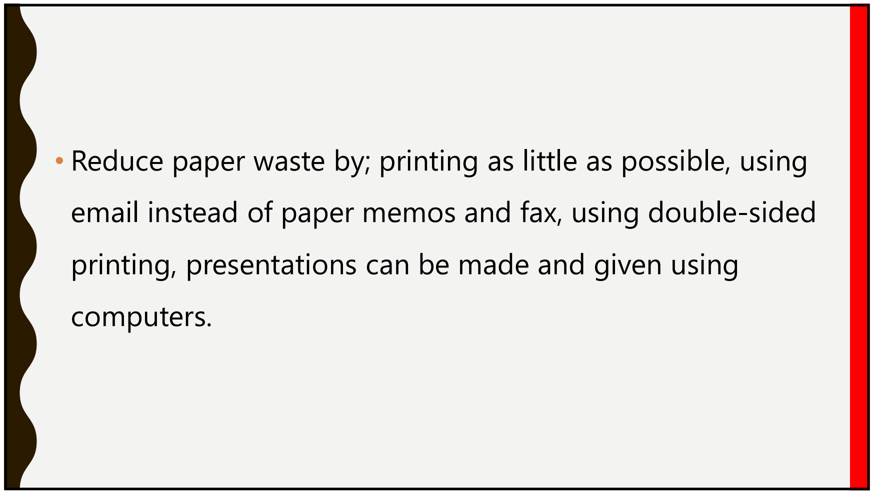


Green computing practices

- Buy/use "energy star" labeled devices. These save energy because they can be programmed to power down to a lower power state when they are not in use, which also allows enables them to have a longer life.
- Activate the power management features of the computer system e.g. allowing the device to go to sleep mode after a set time of idleness.
- Turn off devices when not in use.



- Switch off the mains connected to the device to prevent it from drawing idle current, which is the current drawn even after the equipment is shut off.
- E-cycle/recycle used computer devices. This can be done by refurbishing used parts and devices to extend their usefulness or processing the parts into other usable form instead of carelessly disposing them.



- Reduce paper waste by; printing as little as possible, using email instead of paper memos and fax, using double-sided printing, presentations can be made and given using computers.