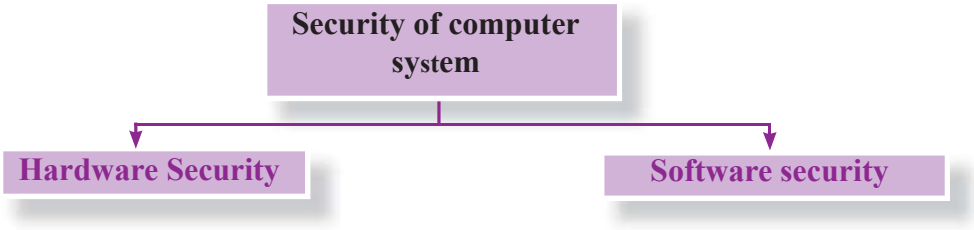
03 Security of the Computer System

3.1 Let's protect Computer System

It is essential to have adopted various prior protective measures for the safety and the durability of computers. The security of the computer system can be divided into two parts.



3.2 Let's protect Computer Hardware

Computer Hardware

Any physical component of a computer that you can touch and see is called hardware. It has a definite shape. As there are hardware devices outside of a computer, there are hardware devices inside the system unit too.

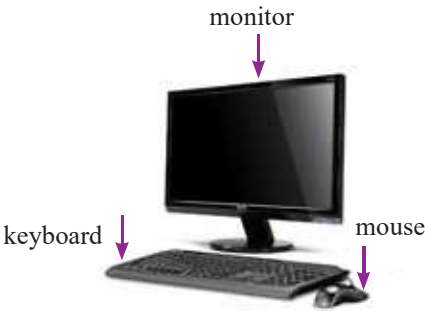


Figure 3.1 - Some hardware devices that can be seen externally

Figure 3.2 - Some hardware devices inside the system unit

Exercise 1: See Workbook 3.1

3.2.1 Possible Hardware Security Issues

Some main factors that may cause physical damage to hardware devices;

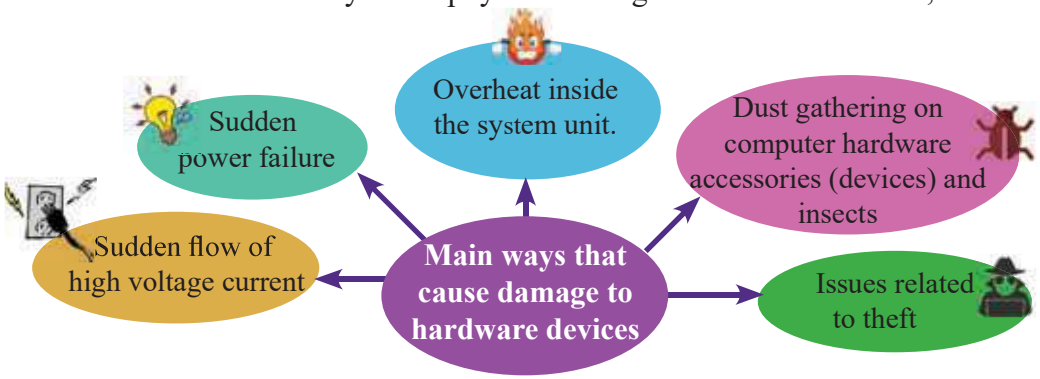
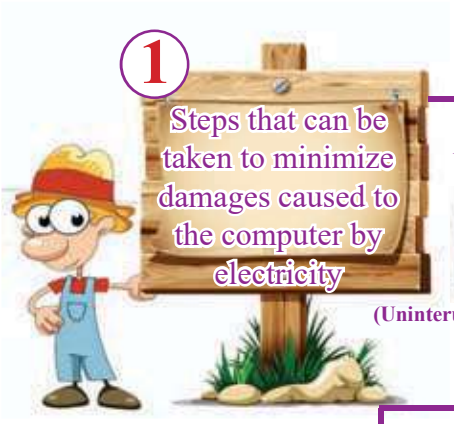


Figure 3.3 – Some ways that cause damage to hardware devices

3.2.2 Precautionary Methods to protect Physical Components of a Computer



Using UPS

(Uninterupted power supply - UPS)

- During sudden power failure, UPS continues to supply power to computer without interruption for a while.
- So, it enables to give sufficient time to save the current work and shut down the computer.

Using Fuse

fuse

- Prevents damages caused to computer due to sudden flow of high voltage current
- It is widely used in power supply units and etc.
- However, at present Mini Circuit Breakers-MCB are used in place of fuse due to easy use.

Using surge protection

surge protection

- Protects the computer from high voltage current and lightning
- Controls the flow of high voltage current to the devices and sends it to earth

Installing air conditioners in the computer laboratory to control the heat

Fixing cooling fans on devices which get heated highly inside the computer

It is essential to keep the computer laboratory clean and tidy in order to protect it from physical harm such as dust gathering,high moisture and insects' menace. For that, some steps that we can follow can be shown as follows.

Figure 3.4 – Some steps that can be taken to protect the computer from physical harm

- By entering the lab without footwear, the computer lab can be kept free of sand and dust.
- Dust gathering on computer circuits (devices) can be prevented by cleaning all the computers in the lab at least once in every three months.
- Taking food in the lab can attract insects like ants to the food particles fallen on the ground
- Moisture in the laboratory may cause short circuit.

- Making doors and windows of the laboratory in such a way as to be locked Property.

- Protecting system unit by locking it

- Using CCTV camera

Exercise 2 : see Workbook 3.2

3.3 Let's protect Computer Software Components

Computer Software

Data and information in the computer and programmes used for various tasks come under the category of software.

Example:

Operating System
Word processing software
Files containing documents
Files containing pictures / images

3.3.1 Possible Software Security Issues

Some instances that may cause possible threat to software are mentioned below.

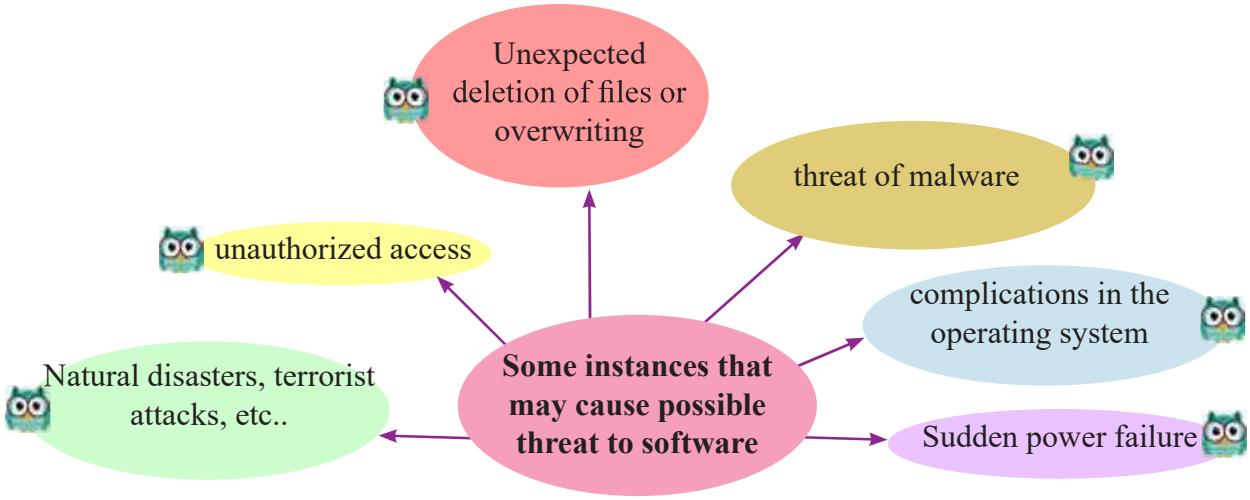


Figure 3.4 – Some instances that may cause possible threat to software

3.3.2 Precautionary methods to protect Software Components of a Computer

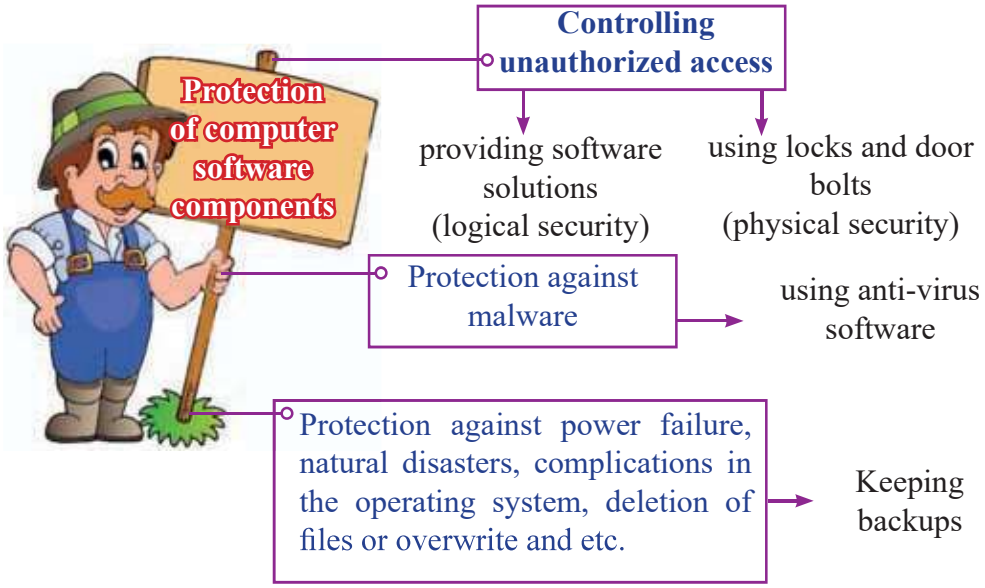


Figure 3.5 – Some steps that can be taken to protect software components

Exercise 3 : see Workbook 3.3

1 Providing Protection against Malware

Malware is a main factor that can couse a threat against the security of computer software.

What is malicious software (malware)?

Malicious software can be defined as any man-made software or part of a software that functions against the requirements of the computer user and designed to intentionally cause damage to

- software installed in the computer
- data, information stored in the computer
- computer networks
- and perhaps computer hardware devices as well.

There are several types of malware. Some of them are hybrid in nature, that is, they take different forms. From time to time they operate in different forms.
For example,
A malware that behaves as a computer virus at a time, behaves as a Trojan horse at another time.

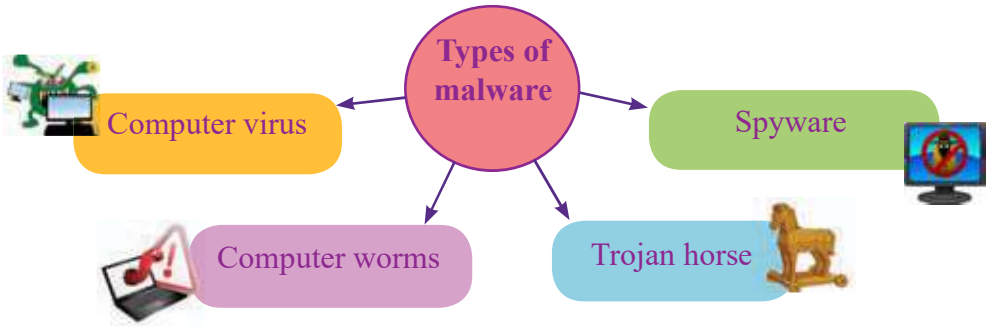


Figure 3.6 – Some types of malware

1. Computer virus

A computer virus is a main malicious software that gains entry to computer software and files and which is capable of replacating itself and designed to spread from computer to computer through portable devices. It can delete or modify data / information and it can corrupt software as well.

2. Computer worms

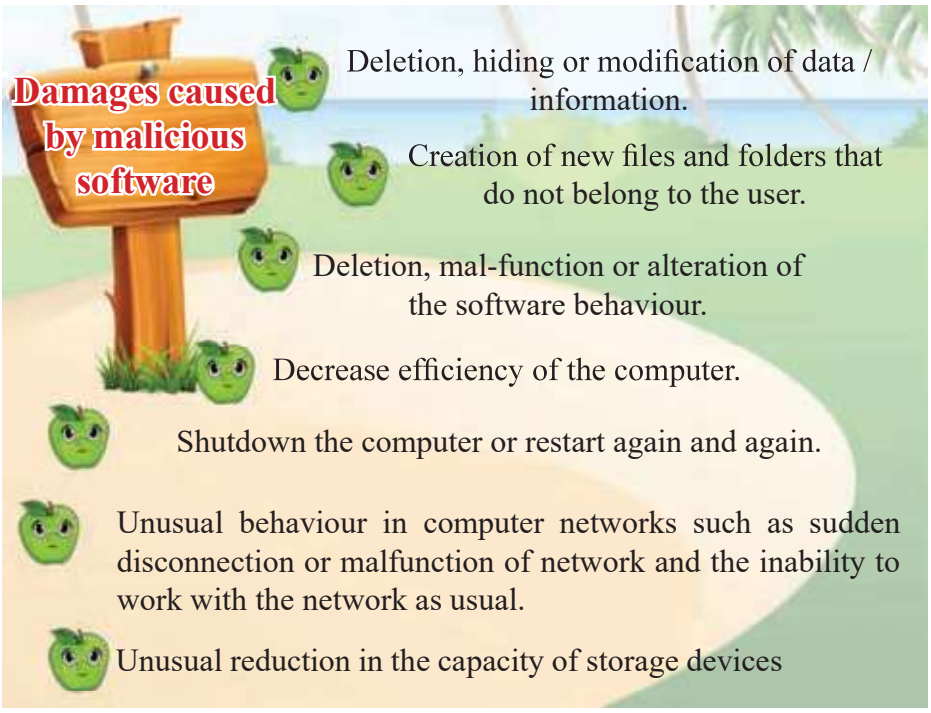
It causes damages similar to those of viruses. However, the main difference is that it spreads across computer networks or internet without the support of a host program or any human interaction.

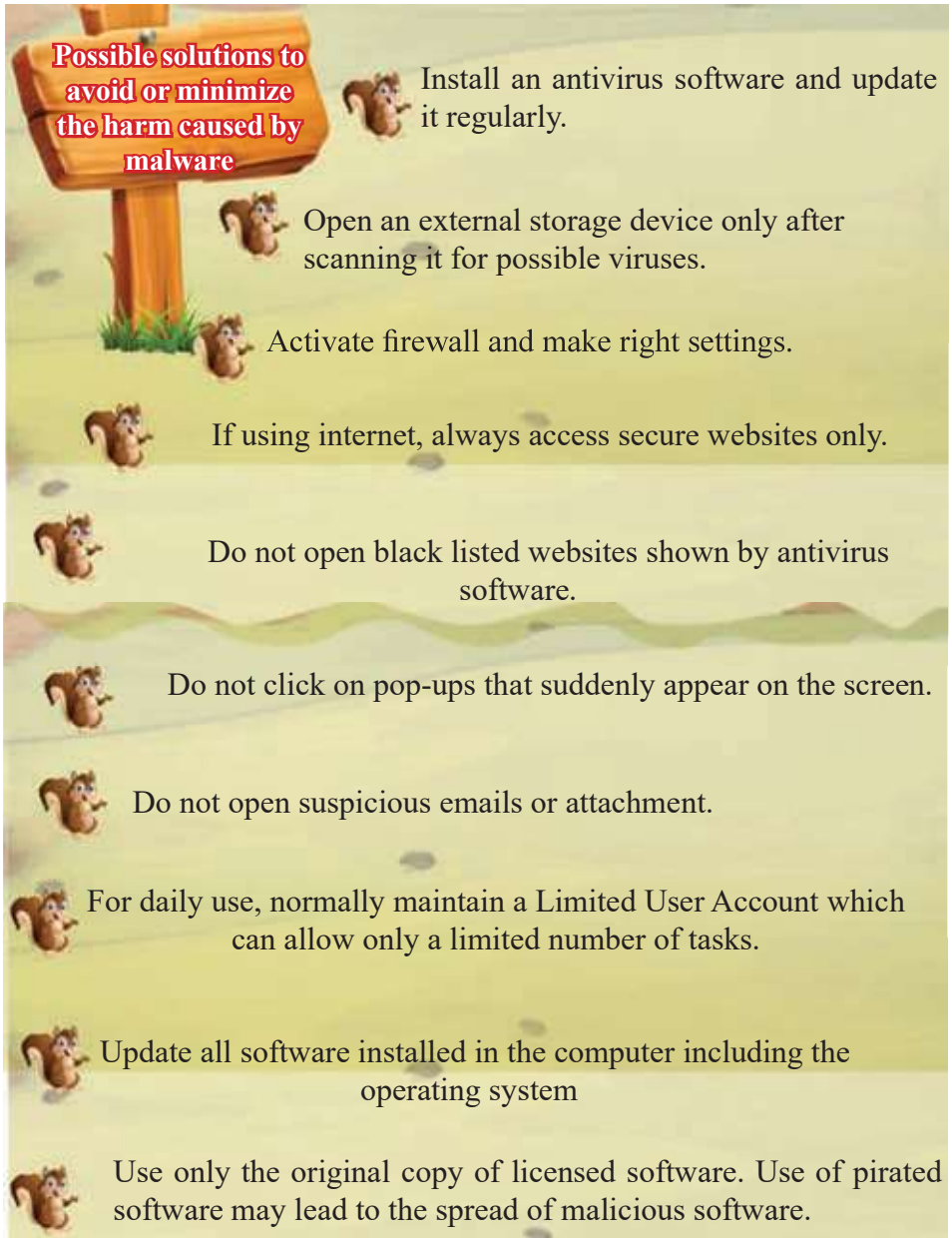
3. Trojan horse

While it seems a useful software at first sight, it will cause damage to the user secretly once he begins to use it.

4. Spyware

It is a malicious software that secretly collects data about a person's computer usage, internet usage and etc.., and sends them to the relevant party without his knowledge. Data and information too can be provided to the other party secretly through this software.





Exercise 5 : see Workbook 3.5

2 Keeping Backups

Keeping backups can be defined as a process of keeping copies of software components.

Copies kept as backups can be used in case the original copy is misplaced or damaged. Several storage techniques can be applied to keep backups.

eg:

Compact disks (CD)
Digital Video Disks (DVD)
external hard disks
Different location in the same computer (another folder or another drive)

3 Access Control

Providing software solutions for access control

It means the methods and services provided by several software to control access to computer and safeguard its resources.

- Using strong and difficult to guess password
- Creation of suitable user accounts
- Encryption

By following the above mentioned methods, not only access to computer can be controlled but also data and information can be protected from sudden loss.

Encryption is another way of protecting data. Encrypted data cannot be read and understood even if it falls into wrong hands. This method is adopted especially when sensitive data is to be communicated.

Use of physical locks for access control

The computer system, data and information stored in the computers and software are protected by using devices and methods that are in the form of hardware in this method.

For this, following methods are used.

1. Keeping the computer at a secure place.

It is advisable to keep the computer that contains sensitive and valuable data, information at a secure place, so that it will be protected from thieves and unlawful entry of people.

2. Use of CCTV cameras and alarms

Tasks such as monitoring movements when necessary, provision of automatic urgent messages are done by this system.

3. Use biometric passwords

At present, finger prints and voice recognition methods are widely used to access computer systems and to open doors of the computer laboratory.

Unlike a conventional password, using biometric passwords is somewhat a modern method. Permission to access the system is granted only after recognizing authorized person's identity through finger prints, voice, face or iris.

Figure 3.7 Use of biometric passwords in mobile phones and laptop computers

Exercise 5 : see Workbook 3.5

Summary

- ★ When providing security to the computer system, both hardware and software components should be given equal attention.
- ★ Some possible hardware security issues;
  - sudden power failure
  - flow of high voltage current
  - overheating inside the computer system
  - dust gathering on computer hardware and insects menace
  - theft menace
- ★ For the protection of hardware, precautionary methods such as,
  - minimizing harm caused to the computer by electricity
  - minimizing overheating inside the computer
  - protecting computer from physical damage
  - protecting from thieves

  can be used.
- ★ Some possible software security issues;
  - attack of malware
  - unauthorized access
  - sudden power failures
  - natural disaster, terrorism etc..,
  - complications in the Operating System
  - unexpected deletion of files, or overwrite
- ★ For the protection of software, precautionary methods such as,
  - providing protection against malware
  - keeping backups
  - access control

  can be used.