

UNIT 3

INFORMATION AND COMPUTER SECURITY

UNIT OUTCOME

Students will be able to:

- understand the responsible behaviour in the computer laboratory;
- recognize the nature of computer virus and measure to protect.

3.1 INFORMATION AND COMPUTER SECURITY

Security of information and related computer systems is a big concern for the computer users. So, the effective methods of protection are required. In this unit, you will learn about information and computer security.

● Responsible Behaviour in the Computer Lab

A computer laboratory is a special place which contains delicate and expensive equipment (see Fig. 3.1).



Fig. 3.1: Students working in a computer lab

In order for the computer lab to maintain the equipment and an excellent learning environment you must behave in a calm manner and not damage any machines or furniture; you must not touch any electrical connection for any reason.

You need to follow some guidelines for responsible behaviour in the Computer Lab. These are:

- 1 Students are not allowed in the computer lab unless directly supervised by a computer teacher or any other staff member.
- 2 Never share your password, even with your best friend.

- 3 No gum, eat or drinks in the computer lab, electronic equipment does not like to get wet or sticky.
- 4 Listen to directions given by your computer teacher.
- 5 Review your notes, on-line materials and of course the HELP option in all programs.
- 6 Only use the Internet as instructed. Do not click on links that seem suspicious or are offers of “free” anything.
- 7 Do not use the mouse or keyboard as a toy, that is, do not randomly click on the mouse or hit the keys on the keyboard without a purpose.
- 8 Do not change computer preference settings or endeavour to “hack” into unauthorized areas.
9. Always use print preview before you print.
- 10 Take permission from your computer teacher before printing.
- 1 Before leaving from the computer lab you should follow these procedures:
 - (i) Exit any programs you are using. The login screen should be showing on the desktop. Return supplies (if any).
 - (ii) Straighten your work area and retrieve your books from the book shelf.
 - (iii) Log Off/Turn Off your computer and push in your chair.



Do not give own or another’s data to anyone. E-mail address should not be given to anyone. Always stick to safe on-line behaviour.

Sanctions

It is always expected that students will follow these rules and codes of behaviour; there may be occasions when sanctions will need to be invoked (called upon), including:

- 1 Temporary removal from the lesson (time out).
- 2 A temporary or permanent ban on **Internet** use or even using the computers in general. (Parents would usually be informed at this stage.)
- 3 **When** necessary, police or local authorities may have to be involved.
- 4 Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.

● School ICT Policy

Information and Communication Technology (ICT) prepares pupils to participate in a rapidly changing world in which work and other activities are increasingly transformed by access to varied and developing technology. Pupils use ICT tools to find, explore, analyse, exchange and present information responsibly, creatively and with discrimination. They learn how to employ ICT to enable rapid access to ideas and experiences from a wide range of people, communities and cultures. Increased capability in the use of ICT promotes initiative and independent learning; with pupils being able to make informed judgements about when and where to use ICT to best effect, and consider its implications for home and work both now and in the future.”

Table 3.1 gives some responsibilities of the schools relating to ICT, which need to be allocated.

Table 3.1: Some Responsibilities Relating to ICT

Managing the implementation of ICT policy	Ensuring safe on-line behaviour
Ensuring staff access to ICT	Assessment of students
Ensuring attitude towards ICT	Overseeing equipment maintenance
Ensuring ICT progression	Health and safety policy and practice
Purchasing/organizing ICT resources	Reviewing the ICT policy

The following points must be included for implementing the ICT policy:

- 1 How does the school ensure that all students have opportunities to use ICT according to their needs?
- 2 How does ICT help to give students with special educational needs access to the whole curriculum?
- 3 How does ICT support gifted students?
- 4 How is the gender issue handled?
- 5 What account is taken of pupils' use of ICT at home?



All pupils should be given equal access to ICT within the school with appropriate arrangements being made to support individual needs, when and where necessary.

Developing a school ICT policy

The school ICT policy means the rules prepared by the school to use ICT. The ideas given here should be adapted to ensure that the policy is appropriate and relevant for your school. When deciding on the school's aims for ICT, internal, local and national factors should be considered.

The school's overall aim for ICT is to enrich learning for all students. The school management must ensure that ICT Co-ordinator and computer teachers develop confidence and competence to use ICT as a tool aiding effective teaching across the curriculum (see Fig. 3.2).

The school ICT policy must identify the important issues and guide the students to live with it. Some of these include:

- 1 A statement defining ICT capability.
- 2 The aims for ICT in the school.
- 3 Guidance on record-keeping, assessment.
- 4 Guidance on health and safety.
- 5 Specific rules for the use of Internet and E-mail.
- 6 Statement of the school's position on copyright, data protection.
- 7 Information regarding maintenance/repair/viruses.
- 8 Date for review.



Fig. 3.2: ICT Co-ordinator addressing the students about ICT policy



The day-to-day organization procedures, guidance, rules and other operational matters should be placed in a school handbook.



STUDENT'S ACCEPTANCE OF THE SCHOOL'S ICT POLICY

Please complete and return this form to the ICT Co-ordinator or Computer Teacher.

Student's agreement:

I have read and understood the school rules for ICT policy. I will use the computer systems and Internet in a responsible way and obey these rules at all times.

I understand that if I break these rules then I may not be allowed to use the Computer Lab.

Student's signature _

Date / / _

Parent's/Guardian's Acknowledgement:

I have read and understood the school rules for ICT policy and give permission for my son/daughter to live with it. I understand that the school will take all reasonable precautions to ensure that students cannot access inappropriate materials, although I understand that the school cannot accept liability for the material accessed, or any consequences of Internet access.

Parent's/Guardian's signature _

Date / / _

Name of Student _ _ _

Grade _

● Nature of Computer Viruses

Computer viruses are software programs like other applications. But they get attached with the general applications and use their setup or .exe file to get installed on the computer system. Computer viruses are proving to be main cause of crashing computer system. To solve or remove viruses from computer, install any updated Anti-Virus software on your PC and perform a system scan.

Let us focus on the nature, recovery and prevention of computer viruses.

Computer Viruses

A computer virus is a malicious program that is designed to corrupt or delete the information stored in the computer. You will know if you have a computer virus very quickly, because nothing will function as it should. If other computers are connected to this computer by network or e-mail, the virus can be spread very quickly because the virus replicates itself to enter and infect these computers (see Fig. 3.3).



Fig. 3.3: Computer virus can create problems on computer

These viruses do basically three types of damage to the computer it affects:

- 1 First is Trojans or worms which are designed to steal important personal information such as your ID's, passwords, account numbers, and other personal information found on your computer.
- 2 Second type is designed to gain access to your machine and then hijack it. Once it has control of the affected computer a hacker can use it for malicious purposes or as a spam machine to send thousands of unwanted e-mails.
- 3 Third type is sometimes referred to as macro viruses. This type of virus is designed so they can delete or overwrite the system or data files on the affected computer. This causes the computer to crash and become unbootable or non-operable. Many of the computers that get this type of virus have a crashed hard drive which is not repairable and all your data is lost permanently.



Computer Viruses are spread through transportable secondary storage devices and networks.

Measures to Protect

The best way to protect computer viruses is installing antivirus software. **Antivirus** software consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software (malware).

Good antivirus software comes with features like a built-in firewall and usually offers an access to online data backup. This antivirus software has the option to deactivate the malicious viruses.

Firewalls are systems which help protect computers and computer networks from attack and subsequent intrusion (see Fig. 3.4).

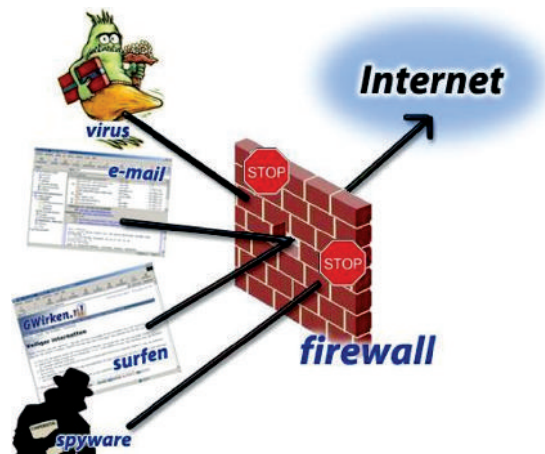


Fig. 3.4: Firewall

The antivirus software protects your computer from virus attacks in three main ways:

- 1 The first way is prevention which involves detecting and eliminating new viruses from your computer. They get the latest virus definitions from their server so they know what to look for and protect against.
- 2 The second way is cleaning infected computers. This involves detection and extermination of the virus, along with repairing the damaged files.
- 3 The third way is protecting your computer by monitoring e-mails, downloads and protection while Internet surfing *i.e.*, on-line. The antivirus regularly scans the computer or a preset scheduler to keep your computer virus free.



Figure 3 illustrates Norton and Quick Heal antivirus:

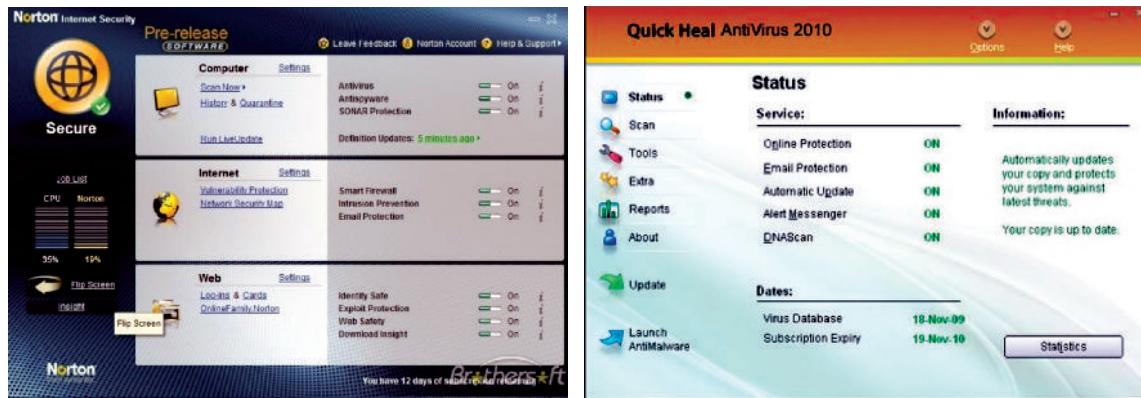


Fig. 3.5: Norton and Quick Heal Antivirus

As mentioned earlier antivirus software is very effective in finding and deleting harmful computer viruses. The computer users should follow these safety rules to protect against viruses:

- 1 Do not open unsolicited e-mails.
- 2 Never download an attachment to an e-mail without scanning it for viruses first.
- 3 Make sure you also use a firewall.
- 4 Do not download free software or music.
- 5 Do not use free antivirus software.
- 6 Search on Internet for antivirus reviews and research yourself for best antivirus software.

Microsoft Malicious Software Removal Tool protects your system from Computer Viruses. You can download and install this software from official website of Microsoft. This software is compatible with Windows 7 Vista, XP and Windows server 2003. At the end of the process, you will get a thorough report about any malicious software that have been detected and removed.

Turn on Automatic updates on your system and then perform the following:

Click **Start** → **Control Panel** → **System** → **Automatic Updates**



ACTIVITY 3.1

RESPONSIBLE BEHAVIOUR IN THE COMPUTER LABORATORY

In small groups students will discuss “Responsible Behaviour in the Computer Laboratory”. The group leader from each group will give a brief presentation to the class based on the discussions.

Computer Laboratory

A computer laboratory is a special place which contains delicate and expensive equipment.



Fig. 3.6: Computer laboratory

To keep your computer laboratory and computers in proper working condition, it is necessary to behave in a calm manner and not damage any machines or furniture. You must not touch any electrical connections for any reason.

Points to be borne in mind while working in the computer laboratory:

✓ **Do's**

1. Sit properly and behave in a calm manner.



Fig. 3.7: Responsible behave in computer lab

2. Only use the Internet as instructed.
3. Ensure that the power switch on the system unit, monitor and printer are in the OFF position before switching off the mains.

✗ **Do nots**

1. Do not shout.



Fig. 3.8: Shouting is not allowed

2. Do not damage any machines or furniture.

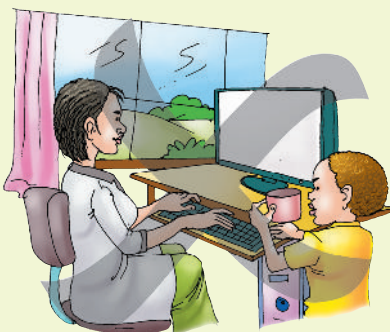


Fig. 3.9: Damaging is not allowed

3. Do not allow eating or drinking near the computer.
4. Do not touch any electrical connections.

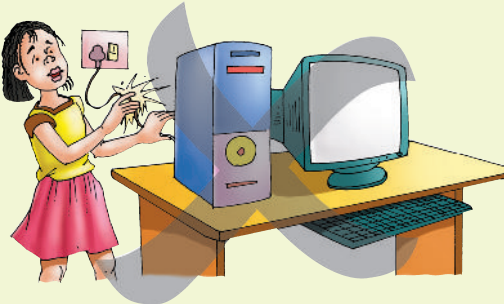


Fig. 3.10: Touching an electrical connection can be very dangerous

5. Never share your password, even with your best friend.

Always remember that responsible behaviour in the computer laboratory will help you in the ICT field forever.



KEY CONCEPTS

- Security of information and related computer systems is a big concern for the computer users.
- Computer laboratory contains delicate and expensive equipment.
- In computer lab; students must behave in a calm manner and not damage any machines or furniture; they must not touch any electrical connections for any reason.
- School ICT policy means rules prepared by the school and students must live with it.
- Computer viruses are software programs which are proving to be main cause of crashing computer system. The best way to protect computer viruses is installing antivirus software.



REVIEW QUESTIONS

Fill in the Blanks

- 1 Computer laboratory contains and equipment.
- 2 In computer laboratory, the students must not touch any connections for any reason.
- 3 A is a malicious program that is designed to corrupt or delete the information stored in the computer.
- 4 The software protects your computer from virus attacks.

State Whether True or False

- 1 Security of information and computer systems is not a big concern for the computer users.
- 2 Students must have safe on-line behaviour.
- 3 Students may or may not live with school ICT policy.
- 4 Computer virus is never harmful to your computer.

Multiple Choice Questions

- 1 Which of the following is/are included in the responsible behavior in the Computer Lab?
 - (a) Never share your password, even with your best friend
 - (b) Listen to directions given by your computer teacher
 - (c) Only use the Internet as instructed
 - (d) All of these
- 2 Which of the following must be included for implementing the school ICT policy?
 - (a) All pupils have equal access to ICT according to their needs
 - (b) Gender issue not handled
 - (c) No support for gifted students
 - (d) Assessment of students not required
- 3 Which of the following is not an antivirus?
 - (a) Norton
 - (b) Spamming
 - (c) Avast
 - (d) AVG
- 4 Which of the following is not a safety rule to protect against viruses?
 - (a) Do not open unsolicited e-mails
 - (b) Never download an attachment to an e-mail without scanning it for viruses first
 - (c) Never use a firewall
 - (d) Do not download free software or music

Match the Following

Column A

Column B

- | | |
|-------------------------------------|-----------------------------------------------------------------|
| 1 Information and computer security | (a) Antivirus |
| 2 Computer Lab | (b) A big concern for the computer users |
| 3 School ICT policy | (c) A place where students must behave in a calm manner |
| 4 Quick Heal | (d) Rules prepared by the school and students must live with it |

Answer the Following

- 1 Explain about the responsible behaviour in the computer laboratory.
- 2 What is safe on-line behaviour? Explain.
- 3 What is school ICT policy? Explain.
- 4 Describe computer virus and the measure to protect computer virus.

Suggested Activities

- 1 Explain and demonstrate school ICT policy.
- 2 Discuss what a computer virus can do to a computer system and demonstrate the measure to protect the computer.

Field Trip

Students should visit some big educational organization in their city. Interact with faculties there and prepare a report on 'Information and Computer Security'. Discuss it in the class also.