6 Information and Communication Technology and Society

The chapter concerns the following;

- Contribution of ICT to entertainment
- Ethical and legal issues in ICT
- Precautions related to ICT infrastructure protection
- Health and safety issues inherent in the use of ICT

6.1 ICT in entertainment

Society is driven towards various forms of entertainment facilities for relaxation from everyday stress. However, most people prefer watching a film for relaxation. Unlike in the past, film producers nowadays enjoy the advantage of producing films of high quality with the use of ICT. Some of these modern facilities that film producers enjoy are as described below:

i) 3D – three Dimensional

With the use of advanced technologies producers can now make life look real on films using three dimensional technology as against the two dimensional, in use, once.

To view films using 3D technology the user needs to use 3D spectacles available for the purpose.

Figure 6.1 - movies created by 3D technology

ii) Holographic Image processing Technology

A scene from a set shot in some place is recorded on camera. Holographic image processing technology is used to display this image elsewhere. This technology is mostly used with scenes depicting horror.

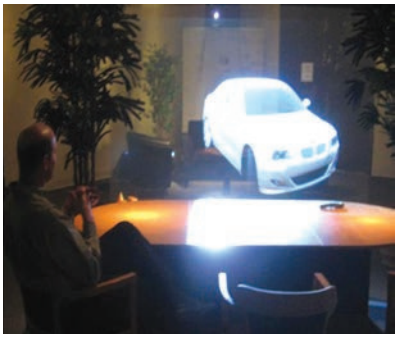

Figure 6.2 - Holographic Image processing Technology

iii) Cartoon films

Cartoon films are popular among both adults and the young. This is due to the 3D feature (3D-three dimensional) contained and the development of technologies in the relevant software. (Fig 6.3)

Figure 6.3 - Cartoon films

iv) Digital audio materials

The use of the computer is evident with modern music and related editing. Recording of songs, creating rhythm and mixing are freely done using modern software to entertain audiences. (Fig 6.4)

Songs recorded in this manner can easily be stored in compact discs (CDs).

Figure 6.4 - Digital audio materials

It is also possible to listen to or view them using home theatre systems. (Fig 6.5).

Figure 6.5 - Home Theatre systems

v) Digital games

Digital games have become very popular today. Digital games can easily be played on computers or cell phones for entertainment. Digital games in both 3D and 4D are the most popular today.

Figure 6.6 - Digital games

vi) Simulation games

Simulation games are based on an everyday activity in a natural setting created artificially.

Simulation games are mostly used with training for sports activities, investigations, planning, military training, mercantile activities, and miming.

Figure 6.7 - Simulation games

6.2 Problems associated with the use of ICT

It is possible for Information Communication Technologies (ICT) to be mankind's closest friend providing many facilities to make life comfortable. Yet, with the use of ICT, mankind faces many unforeseen problems. These problems can be related to the following:

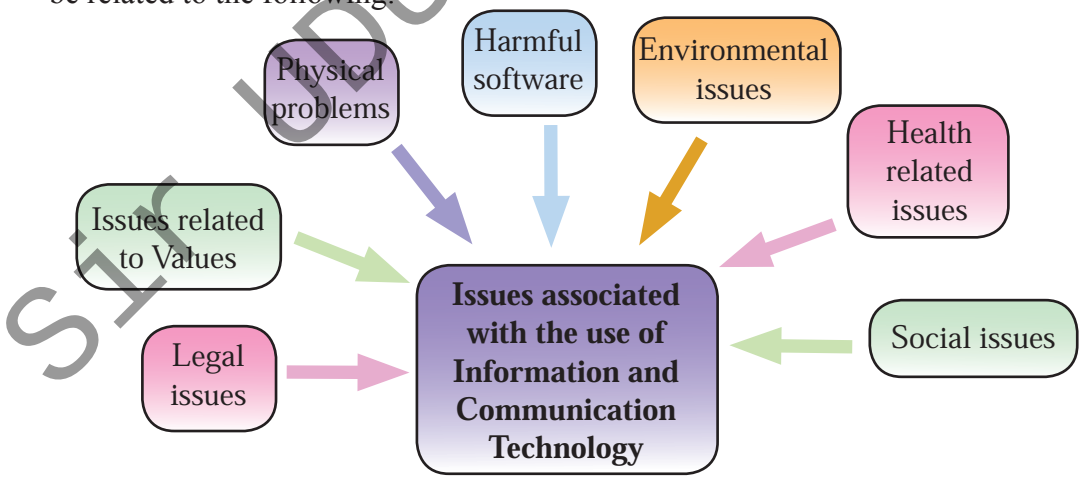

Figure 6.8 - Issues associated with the use of ICT

These issues and likely solutions are detailed in the following section.

6.2.1 Legal issues

i) Data thefts -

Personally Identifiable Information (PII) is stolen from a computer or other device can be considered as data theft.

E.g. - stealing or keeping flash drives, digital camera, mobile phones that contain personal names, telephone numbers, photoes etc. without permission or legal rights.

Figure 6.9 - Data thefts

ii) Unauthorized access into computer systems -

It is possible to access computer systems unlawfully with the theft of or manipulating user name and password of a computer. An organization's data can easily be stolen in this manner.

iii) Intellectual property rights -

1. What are intellectual property rights?

Intelectual property usualy reletes to creation in mind. Intellectual property rights relate to an innovation or a completely new product from a person or an organization currently not in use. Such innovations or brand new products to enter the market are the property of the first person or organization to develop and release the product. They claim ownership to the innovation. It is their right to identify themselves as the legal or lawful owners.

Presenting such products in the names of others or using such products for other developments or sale of such products without the knowledge of the first person or organization is illegal. Such claims belong to the category of stolen intellectual property.

2. It is possible to obtain patent rights for protection of intellectual property.

A patent is a license issued by the state for innovations. To receive a patent license the innovator must apply to the national office governing the product.

iv) Fraud

Copying or impersonating with personal documents (bank account numbers, signatures) contained in a CD, or over the Internet, copying literary works or their use them for personal benefit, cheating people with likely business transactions or credit card fraud.

6.2.2 Issues related to values

i) Plagiarism

Plagiarism is the act of stealing another's creative work and displaying it as one's own. Plagiarism is very common among users of computers today with the stealing of data and other related information from the Internet.

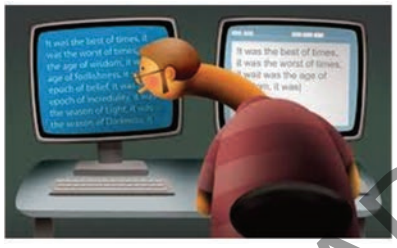

Figure 6.10 - Plagiarism

It is possible to use data and other information collected from the Internet in better accepted ways. Better accepted ways refer to the correct use of such collected information without in any way harming the reputation of the correct owner. This, can be done by,

1. Citing - mention the rightful owner and his information.
2. Quoting - the use of inverted commas ("…") to identify a selected or borrowed section.
3. Referencing - the listing of resources from which the information was collected. This is usually done at the end of an essay or article.

6.2.3 Physical and logical issues

Computers need to be used carefully. Careless use of computers is likely to bring about both physical and logical issues.

Sudden power failures may lead to damaged computing devices. There may be computer thieves. It is also possible to experience a complete network breakdown with malware coming through the Internet. Computer hacking and environmental factors also contribute towards physical damage to computers.

If so, how can computers be made secure and free ourselves from physical and logical issues that are likely to arise?

➢ Physical Security

i) Uninterrupted Power Supply (UPS)

In case of an electricity breakdown, there has to be some alternate arrangement to supply power to the computer so that the network and the documents face no harm. Here, the alternate arrangement to supply comes with the battery contained in a UPS. This prevents interruption to the supply of power to the computer. (Fig. 6.11)

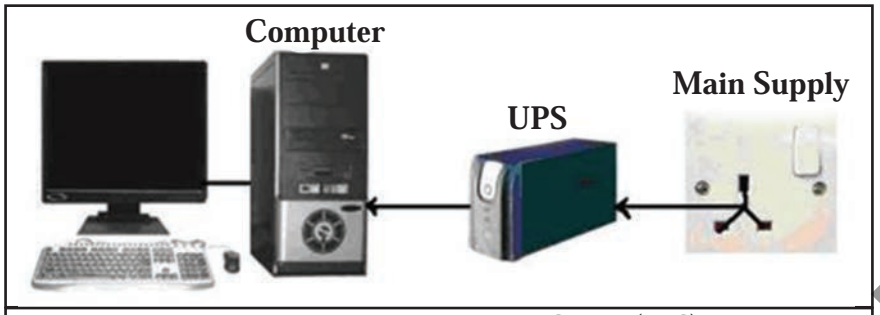

Figure 6.11 - Uninterrupted Power Supply (UPS)

ii) Hardware Firewalls

Hardware firewalls bought as a separate unit have now been built into broadband routers. Hardware firewalls are essential especially with computer networks connected to the Internet. The firewall filters access to and provide connection from the Internet for information with every network. A firewall protects a network from unauthorized access. (fig. 6.12)

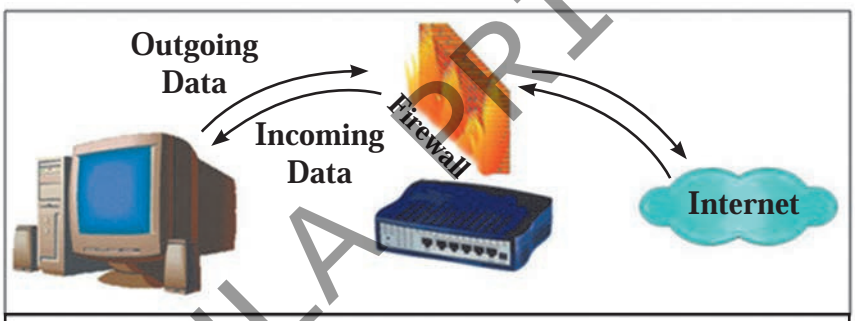

Figure 6.12 - Hardware Firewalls

Controlled access through locked doors

Closed and locked doors are essential to ensure security of a computer laboratory. Closed and locked doors prevent or limit unlawful entry of people. It can also improve safety of computer systems and other accessories while protecting the information contained. (Fig 6.13)

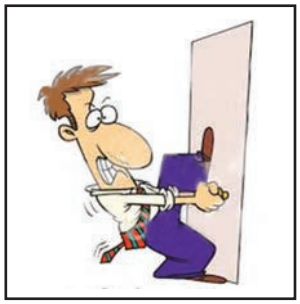
Figure 6.13 - Controlled access through doors

iii) CCTV

It is possible to install CCTV cameras inside a computer laboratory and monitor movement from outside or arrange for the day's proceedings to be recorded as a video clip for viewing later. (Fig. 6.14)

Figure 6.14 - CCTV

iv) Surge protector

The surge protects computers and other accessories inside a laboratory controlling the voltage in the power supply. The local voltage supply for houses or offices is 240 V. The surge protector acts in situations where the power supply exceeds this limit, to control the destruction that could happen to electronic devices (Fig 6.15)

Figure 6.15 - Surge protector

v) Environmental factors

Environmental factors can affect the proper function of a computer. Therefore, it is important to maintain a laboratory or a private computer in a safe environment free from dirt, dust, moisture and the like. (Fig 6.16)

Figure 6.16 - Environmental factors

➢ Logical Security

i) Passwords

Passwords are used to secure data stored in a computer. Passwords protect unauthorized entry or use of a computer. In using a password, it is advisable to mix letters, symbols and numbers to make the password stronger. (Fig. 6.17)

Figure 6.17 - Passwords

ii) Software Firewalls

Software firewalls help protect a network system from unauthorized access when surfing the Internet. The software firewall is part of the operating system and has to be active at all times. The software firewall checks all incoming data for authenticity and prevents suspicious data from entering the system. This way, it helps protect the network from harmful software. (Fig 6.18)

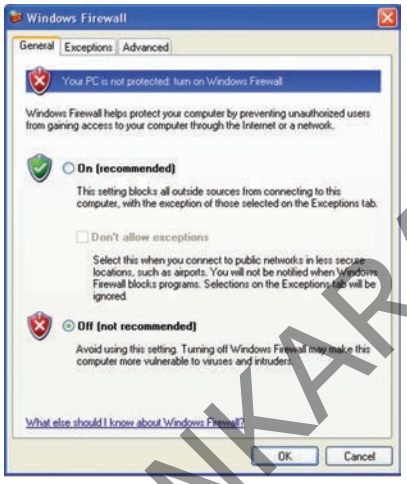

Figure 6.18 - Software Firewalls

iii) Backups

In the event of a failure of a computer system, essential data and information in the computer can be lost. Therefore, a backup is essential towards securing protection of data and information. A backup can be maintained in an external hard disk, CD, DVD, a flash drive or a memory chip. It is also advisable to keep such backups securely in another physical location. (Fig 6.19)

Figure 6.19 - Backups

6.2.4 Malicious software / Malware

i) The use of a computer involves various threats. Malicious software/Malware or malicious codes cause serious harm to computers and networks in many ways. Some examples of such effects are listed below;

- Affect the efficiency of the computer. (Improper function, unnecessary attempts or re-start again and again)
- Destruction or mal-function of software
- Inability to install other software
- Weaken computer hardware

Figure 6.20 - Malicious software

- Sabotage of computer networks
- Data theft and destruction
- Reduction of the storage capacity of the hard disk by the storing unnecessary documents and files.

Harmful software and resultant damage

A few types of harmful software and resultant damage are as described in the Table.

Harmful software	Resultant damage
Computer Virus	Computer viruses gain entry into the computer through a computer program and spread rapidly within the computer causing enough harm. Viruses can enter a computer through networks, a USB flash drive, external devices like memory chips, or through e-mail. Viruses enter the system as executable files. In other words the viruses always remain active within the computer.
Computer Worms	Computer worms also act similar to computer viruses. Worms, however, are capable of acting and spreading alone using e-mail attachments, false websites and instant messages. Worms are produced using social engineering strategies.
Spyware	Trojan Horse The Trojan Horse is a harmful software based on the Greek Trojan Horse constructed using wood. It presents itself as harmless and enters the system without the knowledge of the user. Trojan Horse spyware makes the user uncomfortable by unnecessary opening up windows, producing different desktops, deleting documents and stealing data. Further, it allows other harmful software to gain entry. Trojan enters computer with e mail attachments. However, unlike computer viruses and worms, the Trojan Horse does not spread by itself.
	Adware The adware is displaying unnecessary notices on the computer screen. Using these advertisements, adware collects commercial information. Adware is not harmful as other computer viruses but disturbs the user mentally.

Bots	Bots are derived from the word 'robots'. Bots is harmful software that functions on its own communicating with other networks. Bots are used to collect personal information through Internet messages and conversations.
Hijacker/ Browser Hijacker	Hijacker/Browser Hijacker is capable of misdirecting a user to a different website through the Internet, to collect information regarding trade, commerce and advertisements. Hijacker, is similar to adware.
Phishing	Phishing is the art of deceiving users to collect information about bank accounts or electronic accounts. E-mail is used for the purpose. Such mail is sent through a popular organization or a friend together with a link for access. With a click on the link, or by filling forms, valuable information and cash deposits related to the unsuspecting user get stolen.
Spam	Spam is unauthorized e-mail. Most often, spam relates to advertisements about products or a mail from an unknown person. The mail box can get filled with such mail and make the user uncomfortable. Also, Spam may collect e-mail addresses that can be used unlawfully for frauds.

Safeguarding computer and a computer network from harmful software

- Install a virus guard into the computer. Update the virus guard as is necessary. Keep Guard/Shield/Auto Scan/Update always active.
- Be careful with the use of a USB memory. Check USBs for possible viruses using anti virus software.
- Always install authorized software
- Instead of an administrator account, maintain a user account

If the computer is connected to the Internet,

- Access secure websites. Check URL for verification.
- Select only secure websites for the download of software or other material.
- Before a download, check with a virus guard.

- Be careful with opening up e-mail. Where necessary use a virus guard before a downloading and attachment. Do not click on suspicious links in e-mail. Avoid opening suspicious e mails.
- Avoid suspicious advertisements or messages.
- Do not enter personal information without checking on security.
- Use firewall, virus guards, email filters to avoid the risk.

Some secure, popular virus guards to be installed on a computer are as follows.

- Avira Antivirus
- Avast Antivirus AVG Antivirus
- K7 Antivirus
- Digital Defender Antivirus
- Norman Antivirus
- Kaspersky Antivirus
- Panda Cloud Antivirus (B)
- Microsoft Security Essentials
- Norton Antivirus
- BitDefender Antivirus
- McAfee Antivirus

Prevention is better than cure

Activity

Make a list of virus guards from the Internet other than what is mentioned above. Tabulate the names of the manufacturer and the dates of manufacture.

Agencies in Sri Lanka responsible for the security of information exchange

There is hardly any individual or an organization in Sri Lanka who/which is not connected to the Internet. Over the last few years, unauthorized access into social networks, financial websites has been observed over the world. Sri Lanka is no exception. Therefore, the necessity for responsible agencies to secure Internet access has arisen. This is also called 'Cyber Security'.

Cyber security is not limited to e-mail, Internet solutions, or social networks. They are useful for personal networks and operating systems (OS). Some organizations responsible for cyber security are as follows.

- Institution for Information Security of Sri Lanka

Information and Communication Technology Agency (ICTA) is responsible for the establishment of this institution in Sri Lanka. It provides facilities to various organizations as listed below:

  - Citizens
  - Business establishments
  - State institutions.

- ICTA, Sri Lanka Standards Bureau and the Sri Lanka Emergency Computer Services have together organized to certify Information Security Management Systems (ISMS) to ensure security of information. Individuals and organizations can register for this.

Activity

Access the websites given. Make a list of computer related services you can obtain from them.

http://www.gov.lk/web/
http://www.engage.icta.lk
https://www.techcert.lk/si/

6.2.5 Health issues related to use of Information Communication Technology

- Ergonomics and health issues

Ergonomics is a word made with the use of two words in the Greek Language. According to Greek Language "ergon" is job or action. "nomos" is law. Therefore, the simple meaning to be collected from this word is:

"a job must be created to the comfort of the worker and the worker must not be forced to adjust himself/herself to the work. If not, the worker will subject himself/ herself to various tensions and illnesses."

As of today, technology has become indispensable to mankind. Technology and mankind are now interconnected as inseparable. Daily, the numbers using technology keep increasing. As a result, technology related health issues too keep increasing. Issues arise as a result of the continuous use of a computer for over four hours at a stretch. Let us take a look at these health issues:

i) Musculoskeletal Problems

Non-stop use of a computer can bring about pain in different muscles and bones of the human system. The main reason for this is the wrong posture taken with the use of the computer (Fig 6.21).

Figure 6.21 - Musculoskeletal problems

ii) RSI – Repetitive Stress Injury

Repetitive stress injury is the pain extending from the shoulder to the fingers of the body. The affected areas can show swelling and hardness that brings out the pain. The difficulty to move the mouse is a result of this pain. The cause of the pain is incorrect posture (Fig. 6.22).

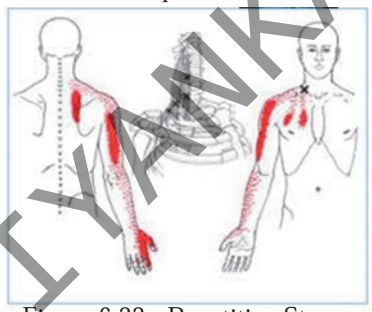

Figure 6.22 - Repetitive Stress Injury

iii) CTS – Carpel Tunnel Syndrome (Fig.6.23)

Carpel tunnel syndrome is the feeling of a numbness and pain in the fingers. The pain arises due to the pressure exerted on the wrist. Incorrect use of the key board and the mouse or placing them in the incorrect positions are reasons for the syndrome.

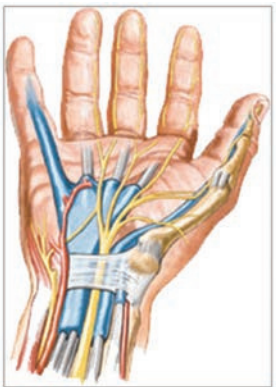

Figure 6.23 - Carpel Tunnel Syndrome

iv) CVS - Computer Vision Syndrome

Sticking to the computer continuously for 6 to 7 hours can cause irritation of the eyes and is identified as the Computer Vision Syndrome. Dry eyes, redness in the eyes, tearing, blurred vision, or pain in the head, neck or back are symptoms of the discomfort. (Fig.6.24)

Figure 6.24 - Computer Vision Syndrome