

4. SAFETY AND SECURITY IN DIGITAL TECHNOLOGY

LEARNING OUTCOMES

By the end of this module, you should be able to:

- Know the various security threats facing technologies
- Know the health and safety hazards of using technology
- Appreciate the right use of digital devices
- Know the social & human issues arise on use of technology

LESSON PLAN

- I. Security
- II. Health and Safety
- III. Ethics
- IV. Social and Human Issues

I. SECURITY

When you use digital technology there are a number of threats that come with it. For example with computers, mobile phones and tablets, there are various kinds of viruses, malwares, spywares, etc., that pose threat to your personal and professional data. They can be used to access your confidential details by using malicious software.

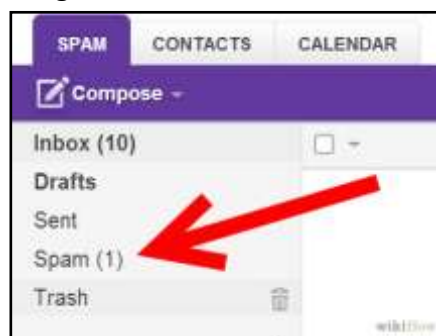
There are number of security threats out of which the most common are mentioned below:

1. Virus: It is a malicious program where it replicates itself and aims to only destroy a computer, mobile phone or a tablet. The ultimate goal of a virus is to ensure that the victim's device will never be able to operate properly or even at all.



2. SPAM/SPIM/SPIT:

- **SPAM** is electronic junk email. It targets individual users with direct mail messages. Email spam lists are often created by stealing Internet mailing lists or searching the Web for addresses.
- **SPIM** is spam sent via instant messaging systems such as Yahoo! Messenger, MSN Messenger, etc.
- **SPIT (Spam over Internet Telephony)** are unwanted, automatically-dialled, pre-recorded phone calls using Voice over Internet Protocol (VoIP).



3. Trojan Horse: Users can infect their computers with Trojan Horse software simply by downloading an application they thought was genuine but was in fact malicious. Once inside

your computer, a Trojan Horse can do anything from recording your passwords by logging keystrokes (known as a keystroke logger) to hijacking your webcam to watch and record your every move.

4. Malicious spyware: Malicious spyware is used to describe the Trojan application that was created by cybercriminals to spy on their victims. An example would be keylogger software that records a victim's every keystroke on his or her keyboard. The recorded information is periodically sent back to the originating cybercriminal over the Internet. Keylogging software is widely available and is marketed to parents or businesses that want to monitor their kids' or employees' Internet usage.

5. Computer Worm: A computer worm is a software program that can copy itself from one computer to another, without human interaction. Worms can replicate in great volume and with great speed. For example, a worm can send copies of itself to every contact in your email address book and then send itself to all the contacts in your contacts' address books.



6. Phishing: A fake website which is designed to look almost like the actual website is a form of phishing attack. The idea of this attack is to trick the user into entering their username and password into the fake login form which serves the purpose of stealing the identity of the victim. Every form sent out from the phishing site will not go to the actual server, but the attacker controlled serve.

7. Fake AV: FakeAV or Fake AntiVirus is a class of malware that displays fake alert messages to the victim about the security threats to their devices. These alerts will provoke the users to visit a website where they will be asked to pay for these non-existing threats that need to be cleaned up.

Do's and Don'ts



1. Do install a reliable antivirus in your devices and keep it updated in order to protect your device from antivirus attack, spam and other security threats.
2. Do not respond to emails or phone calls requesting confidential information such as your bank account number, ATM pin, your passwords, etc.
3. Be cautious while making online transactions such as internet banking, online shopping, and funds transfer, etc.
4. Do not leave printouts containing sensitive or confidential information on your desk or in a common printer. Keep it safely or shred them when no longer needed.
5. Always password-protect sensitive files on your computer, USB, Smartphone, Tablets, etc. Losing items like phones, USB flash drives, and laptops can happen to anyone. Protecting your devices with strong passwords means you make it incredibly difficult for someone to break in and steal data.
6. Don't plug in personal devices like USB flash drives, MP3 players, and smart phones without permission from the IT Service Desk. These devices can be compromised with code waiting to launch as soon as you plug them into a computer. Talk to the IT Service Desk about your devices and let them make the call.
7. Do not install unauthorised programs as malicious applications often pose as genuine programs, like games, tools, or even anti-virus software. They aim to fool you into infecting your computer or network.

II. HEALTH AND SAFETY

Regular and excessive use of digital technologies such as computers, mobile phones and tablets can cause various health problems and can be a concern of safety. It is important that you familiarize to these concerns so that you can use them safely.

HEALTH ISSUES

1. Radiation: Since computers, mobile phones and tablets emit radiation in small quantities, excessive use of these can lead to dry eyes, floaters, blurred vision, headaches, dehydration,

irritability, skin rashes and fatigue. Long term exposure has been linked to various cancers, birth defects and miscarriages, fertility issues with both men and women.

2. Eye Strain: Eyes can become strained after staring at a computer screen for a long time, particularly if working in bad light, in glare or with a flickering screen especially in low light.



3. Back and Neck pain: Many users of computers, mobiles phones and tablet can suffer from serious back and neck problem. This is probably due to a poor posture or an awkward position while using them.



4. Repetitive Strain Injury (RSI): RSI is the damage to the fingers, wrist and other parts of the body due to repeated movement over a period of time. It might result in aching/ pain in the arms and wrists, weakness, swelling, tenderness, numbness, pins or burning sensation. In the shoulders and neck it might lead to stiffness and aching. While texting too much on the mobile phones it might lead to joint ache in your thumbs.

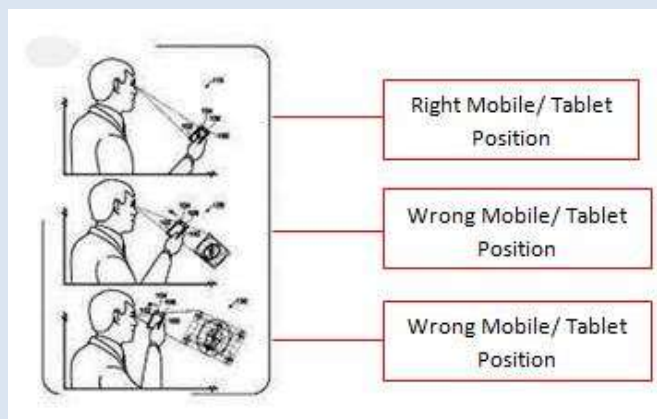


5. Deep Vein Thrombosis: Sitting for a long period of time can cause compression of the veins deep inside your legs. This might hinder the natural pumping of the blood. If this compression continues the blood can begin to stagnate and form a clot. This clot is known as Deep Vein Thrombosis. The might lead to swelling and pain in the legs.

Do's and Don'ts



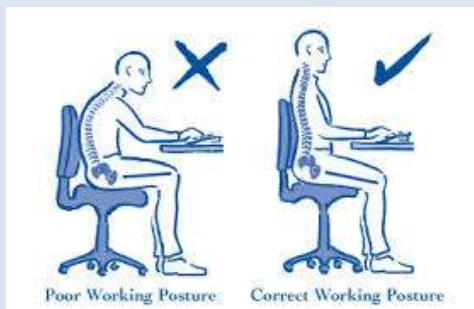
1. Keep enough distance between you and your digital devices while using them to minimize strain. In case of a computer, your desktop should be on the right height for you (Usually about 70 cm from the floor) and wide enough for your computer and keyboard. It should be deep enough to support your arms when you work on the computer.



2. Sit with suitable posture, do not cross your legs for long period of time. Sit up straight in your chair. Keep your feet flat on the floor and your knees slightly lower than your thighs.



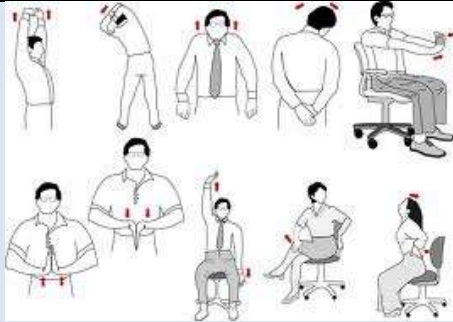
3. Position the devices in such a way that the neck does not have to bend too much. Use a monitor, especially in the case of computers, that is adjustable. Sit with the head up and do not slouch while working on the devices.



4. While using the keyboard and mouse tilt the keyboard using small feet at the back so you can type with the wrist straight – your hands in line with your arms. Rest your wrist on the desk when not keying.



5. Do not use screens/ monitors that flicker too much.
6. Move your arms and legs and stretch the muscles in your back, shoulders, arms and legs. You will be less tired and more alert if you keep active and fit.



7. Take 5 minutes break every hour of work especially in the case of computers. Stand up and move around to allow the blood flow in your legs to return to normal.



8. Keep your eyes healthy by using the right amount of light when using digital devices as it reduces eyestrain, neck strain and headaches. Sunlight is the best light, but make sure it does not create glare on your computer screen.
9. Have regular eye tests and wear glasses if prescribed.
10. Use headphone while talking on mobile phones to minimize radiation exposure.

SAFETY ISSUES

Dealing with digital devices can sometimes be dangerous and may cause accidents. Therefore, you should take certain precautions to reduce the risk of accidents.

- Ensure that there are no trailing wires across or around the room that can cause people to trip or cause accidents. Cables should be placed inside cable ducts or under the carpet/flooring.



- Ensure that sockets should not be overloaded. Plugging too many power cables into a socket can result in the socket being overloaded, overheated and causing fire. Hence, never plug too many cables into a socket. Always



make sure there are fire extinguishers nearby.

- Keep liquids away from your digital devices to avoid spills and the danger of electrical shock.



- Do not use Mobile/ Tablets while driving or walking to avoid accidents.



- Remember to follow any special regulations in force in any area and always switch off your phone whenever it is forbidden to use it, or it may cause interference or danger. For example, while travelling in aeroplanes one should switch off all digital devices especially during takeoff and landing.
- While charging any Mobile/ Tablets do not use them as there is an increased risk of accidents.

III. ETHICS

Digital ethics is a set of moral principles that regulate the use of digital devices such as computer, tablets and mobile phones.

Some common issues of digital ethics include:



1. Intellectual Property Rights

It is similar to any property and refers to the ideas, knowledge, invention, innovation, creativity and research, etc., of an individual.

Common types of Intellectual Property include:

- **Copyright:** This protects written or published works such as books, songs, films, web content and artistic works.
- **Designs:** This protects designs, such as drawings or computer models.
- **Trademarks:** This protects signs, symbols, logos, words or sounds that differentiate your products and services from others.

2. Theft and Fraud

- **Theft:** It may refer to either unauthorized removal of physical items such as hardware or unauthorized removal or copying of data or information from your device.
- **Fraud:** Fraud on the Internet may occur by following ways:
 - To credit card offers which are utilized only to capture personal information.
 - To investor postings which promote a stock or investment offer to encourage investment which will benefit the person posting the information.
 - To medical and pharmaceutical related sites which purport to provide correct medical advice or sell altered medications.

3. Stalking through digital device

Stalking is a pattern of repeated and unwanted attention, harassment, contact or any other course of conduct directed at a specific person that would cause him.

Stalking can include:

- Repeated, unwanted, intrusive and frightening communications from the perpetrator by phone, mail, and/or email.
- Following or waiting for the victim at places such as home, school, work, or recreation place. Harassing victim through the internet.
- Posting information or spreading rumours about the victim on the internet, in a public place.
- Obtaining personal information about the victim by accessing public records, using internet search services, going through the victim's garbage, following the victim, contacting victim's friends, family work or neighbours.

4. Software and Multimedia Piracy

Software piracy or multimedia piracy is the unauthorized use of proprietary software and multimedia resources. By buying the software, you become a licensed user rather than an owner and thus you are allowed to make copies of the program for back up purposes or to share it with other individuals.



5. Plagiarism

Plagiarism is an act of using or copying someone else's ideas, language or any other work and presenting it as one's own without acknowledging the owner. This includes work represented in hard copy, on disk or on the Internet.



Do's and Don'ts



1. Privacy: Do not in any way examine or change files or passwords belonging to others. Do not violate the privacy of individuals or organizations.
2. Plagiarism: Following points should be kept in mind while using or copying someone else's work:
 - Summarize or change the order of the words when using it as a reference.
 - Always give citations or references when using someone else's work.
 - Anything that is directly quoted from any source must be put in quotation marks and cited as well.
3. Integrity of the computing systems: Do not develop or use programs that invade, damage or alter computing systems or software. Do not in any way harass other users.
4. Never use someone else's account. Do not use deceptive means to avoid accounting for the use of computing services.
5. Copyrights and Licenses: To copy a licensed computer program is illegal; it is indeed theft. Try to use free and open source softwares.
6. Respect the intellectual property of others: Individual programming assignments are expected to be done by individual. Do not take another's work or ideas to call your own.
7. Make responsible, sensible use of computer hardware, software and data.

IV. SOCIAL AND HUMAN ISSUES

Digital devices have made modern life much easier. Modern society and individuals are becoming too reliant on these devices for all their needs. They help in easy access to information, communication and education. It has created a bridge across geographies and culture. However, there is always a positive and negative side of every phenomenon and it is important to know how they impact us and our society.

The various Human and Social issues of Digital Devices include:

1. **Increased Stress:** In the digital world, people consume more information through different devices than ever before. People have a tendency to multitask with laptops, mobile phones, the internet, social networks, games, etc., all giving unwanted hassle from time to time. This takes a toll on people causing stress both

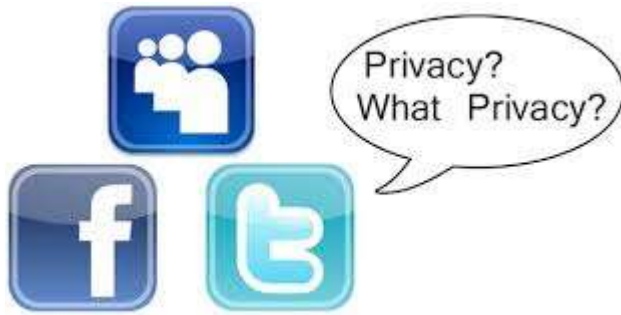
physically and mentally. Hence, it is important to be balanced in the use of these devices and take regular breaks.



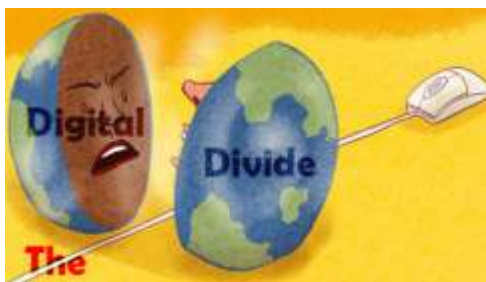
2. **Alienation and Isolation:** The digital devices limit the face to face interaction with people. Most people need some form of social interaction in their daily lives, a lack of which might reduce their understanding of and participation in society and culture as the social environment is reduced to the people you want stay in contact with.
3. **Reduced Physical Activity:** The users may adopt a more inactive lifestyle. This can lead to health problems such as obesity, heart disease and diabetes. Many countries have workplace regulations to prevent problems such as repetitive strain injury or eyestrain, but lack of physical exercise is rarely addressed as a specific health hazard.
4. **Information Overload:** Simplicity of use, abundance of information, absorbing users with the excessive information search may lead to the decline of creative thinking. The way we are currently using the technology is reducing our desire to be inquisitive, think, comprehend and ultimately retain information.



5. **Loss of Privacy:** Privacy refers to the right of individual/s to determine when, how and to what extent his or her personal data will be shared with others. Breach of privacy means unauthorized use or distribution or disclosure of personal information like medical records, sexual preferences, financial status, etc.



6. **The Digital Divide:** The increasing use of computers has increased the separation of rich and poor, creating a digital divide between the information “haves” and “have-nots.” The digital divide has in many ways separated the people with access and people without access. People in many parts of the world lack the resources to follow the new digital world they are alienated in many ways. The costs of these devices are beyond the reach of many thereby creating social differences.



7. **Cyber Crime:** The use of digital devices has opened up new windows to the way crime occurs in society. There are new methods and efficient tools available for crimes to take place, e.g., theft, hacking (for personal information), fraud, gambling, stalking, bullying, etc. This results in moral decadent and generates threat to the society in new and challenging ways.

