Batna 2 University
Faculty of letters and Foreign Languages
Department of Translation

1st year
Module: ICT
Teacher: Mrs. BOUSSAAD

RISKS AND PROBLEMS OF ICT

Information and Communication Technologies (ICT) have brought many benefits to education. Despite these benefits, teachers, learners, and users should be aware of the potential risks posed by the use of ICT systems in schools, companies, and other institutions.

Although computers are expensive and valuable machines, data is the most important thing that is very hard to replace if it gets lost or stolen.

There are many causes of data loss, classified as follows:

I- Users / employees:

One cause of loss or damage of data is the *data user* such as students, teachers, and employees. A vast amount of data is lost due to users mistakes:

a- Carelessness:
- Not saving work as it is being created.
- Saving over a file.
- Deleting a file by accident.

b- Data theft.
c- Data damage.

II- Physical risks:

Besides people, there are plenty of other ways to lose/ damage data.

a- Fire , floods and lightning damage:

Although thankfully a rare occurrence, fires and floods do happen. They can cause immense damage and even total destruction of the computer equipment.

b- Theft of equipment.
c- Scratches on the hard disk.

III- Crime:

1- Malware:

Malware, short form for **malicious software**, is software used or programmed by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Malware includes: viruses, worms, spywares, spams…

- Viruses:

A virus is a simple program designed to cause harm to someone else's computer. A virus spreads by duplicating and attaching itself to other files. The extent of the damage depends on the virus. There are tens of thousands of viruses. Some virus damage is insignificant but inconvenient. Some virus damage is disastrous, putting the computer system out of action by erasing files or corrupting data.

How do you get a virus?

Viruses are written by malicious programmers who wish to cause problems for other computer users. The primary source of infection these days are email attachments followed by **illegal** software and infected files from the Internet.

- Worms:

A worm is a computer program that makes lots of copies of itself, like a computer virus. The main difference between the two is that a computer virus attaches itself to another computer program, but a worm works by itself. As well as copying itself, a worm can be made to do all sorts of things, like delete files on a computer, or send e-mails to everyone the owner has in their address book.

- Spams:

Spam means sending massive amounts of electronic junk mail that people haven't asked for. In legal terms it means to send 'unsolicited commercial email'. This term is used because the vast majority of spam is sent in order to try and persuade you to buy something.

- Spyware:

Spyware is software designed to collect information about what you are doing on the computer. Spyware may be installed without your knowledge by downloading some shareware or other software that does seems to something useful e.g. a free game or utility.

2- **Hacking:**

Hacking means to illegally access other people's computer systems in order to destroy disrupt or carry out something illegal.

Hacking is usually carried out remotely, i.e. someone outside a company wants to try to break into the computer system. Even if the hacker only does it as a challenge or for a bit of fun, it is still illegal.

Types of hackers:

A white hat hacker is a computer and network expert who attacks a security system on behalf of its owners or as a hobby, seeking vulnerabilities that a malicious hacker could exploit. Instead of taking malicious advantage of exploits, a white hat hacker notifies the system's owners to fix the breach before it is can be taken advantage of.

A black hat hacker is a person who compromises the security of a computer system without permission from an authorized party, typically with malicious intent. A black hat will maintain knowledge of the vulnerabilities and exploits they find for a private advantage, not revealing them to the public or the manufacturer for correction.

A grey hat hacker is a skilled hacker who sometimes will act legally and other times may not. They are a cross between white hat and black hat hackers. They usually do not hack for personal gain or have malicious intentions, but may or may not occasionally commit crimes during the course of their technological exploits.