Data protection

Companies gather a large quantity of confidential information and sensitive data concerning employees, customers, products, research and financial situations. Most information is stored in electronic form and transmitted across networks to other computers. This information needs protection against unauthorised access and use, modification, damage or loss.

The key concepts of information security are: confidentiality, integrity, availability and authenticity.

Confidentiality

Confidentiality prevents or minimises access to data and its disclosure, either accidental or intentional, among unauthorised people. According to company policies, data is classified as public, sensitive, private or confidential. When confidential data is sent through the Internet, it is often encrypted. **Encryption** is a way of transforming a plain text into a crypted text using a process or algorithm. The receiver will then have to decrypt the file, i.e., recover the original text with the use of a key.

Integrity

Integrity makes sure that the data being worked on is the correct one. The data cannot be created, modified or deleted without authorisation and the information stored in one part of the database system must be in agreement with related information stored in another part of the database system.
A loss of integrity can be caused by an accidental or malicious cancellation of files or by a computer virus.

availability: *disponibilità*
disclosure: *divulgazione*
to gather: *raccogliere*
keystroke: *azionamento di un tasto*
loss: *perdita*
proactive: *di protezione*
ransom: *riscatto*
wave: *onda*

Availability

Availability is the property of a system or resource of being accessible and usable when requested. It means that the technology used to protect data is available and working properly. Hardware is the most vulnerable to attack, such as in the case of accidental or deliberate damage or theft.

Authenticity

Authenticity makes it possible for a computer to identify the user. A basic access mechanism includes identification and authentication.

- **Identification** takes the form of a **username** or **user ID** and defines the users' rights, i.e., what they can see or if they can modify data;
- **Authentication** verifies if the user is really who they should be in order to prevent unauthorised access.
  The most common types of authentications are with:
  - **passwords;**
  - **PINs (Personal Identification Number)**;
  - **biometrics,** a type of system that relies on the unique biological characteristics of individuals such as fingerprints, hand geometry, retina and iris patterns, voice waves, keystroke dynamics, DNA and signatures.

1 Decide if the statements are true or false and correct the false ones.

		T	F
1.	Companies store all documents in electronic format.	☐	☐
2.	There are different levels of confidentiality.	☐	☐
3.	Sensitive data requires stricter protection than private messages.	☐	☐
4.	Encryption uses mathematical formulae to change the original message.	☐	☐
5.	Malicious cancellation is a threat to data integrity.	☐	☐
6.	A virus cannot damage the integrity of stored data.	☐	☐
7.	Identification and authentication are synonyms.	☐	☐
8.	A user ID establishes what the user can do on a file.	☐	☐
9.	In order to prevent unauthorised access, a password is required.	☐	☐
10.	Biometric authentication uses footprints.	☐	☐

2 PAIR WORK Agree on the characteristics of a strong password.

1. Length: .....
2. Characters: .....
3. Words or phrases: .....
4. Technique for creating it: .....
5. Where to keep it: .....
6. Security: .....

3 GROUP WORK Cyberattacks are an unfortunate fact of modern business, mainly motivated by money or political issues. Choose one topic from the following list, go online and find some information on it. Then report to the class.

1. RockYou2021 – 2021
2. Cyberattack on Yahoo – 2014
3. Cyberattack on Marriott Hotels – 2014
4. Sony's PlayStation Network attack – 2011