# Data protection

Companies gather a large quantity of confidential information and sensible data concerning employees, customers, products, research and financial status. 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**, which prevents or minimises unauthorised access and disclosure of data. It is taken for granted that a person who receives personal information takes measures to protect the same information from unauthorised disclosure, either accidental or intentional, and that the information will only be shared among authorised people. In order to protect it, data need to be classified according to a company policy. The most common labels are: public, sensitive, private and confidential. When confidential data are sent through the Internet, they are often encrypted. **Encryption** is a way of transforming a plain text using a process or algorithm. The receiver will have to decrypt the file, i.e. recover the original text with the use of a key;
- **Integrity**, which makes sure that the data being worked with are the correct data. The data cannot be created, modified or deleted without authorisation. 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**, which 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, as in the case of accidental or deliberate damage, or theft;
- **Authenticity**, which 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 person's rights, in other words what he/she will be able to see or if just he/she can read or modify data. **Authentication** verifies if the user is really who he/she should be in order to prevent unauthorised access. The most common types of authentication are passwords and PINs (Personal Identification Number), although in some case they are not considered adequate and replaced by biometrics. Biometrics authentication is a type of system that relies on the unique biological characteristics of individuals such as fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, keystroke dynamics, DNA and signatures.

**1** BEFORE READING. What do you do to protect your files? And what about your PC, tablet or smartphone?

**2** Read the text on the left and decide if these statements are true or false.

T F

1. Companies store all documents in electronic format. □ □
2. There are different levels of confidentiality. □ □
3. Sensitive data require stricter protection than private messages. □ □
4. Encryption uses strange symbols to change the original message. □ □
5. Malicious cancellation is a threat to data integrity. □ □
6. A computer system should always be on stand-by. □ □
7. Identification and authentication are synonyms. □ □
8. A user ID establishes what the user can do on a file. □ □
9. Using passwords is the best way of authentication. □ □
10. Biometric authentication uses footprints. □ □

**3** PAIR WORK Agree on the characteristics of a strong password.

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

**4** Read this text and complete it with the given words.

algorithm ▪ computers ▪ cryptography ▪ decode ▪ encrypt ▪ keys ▪ public

### Security encryption systems

Computer encryption is based on the science of **1.** .........................., which has been used as long as humans have wanted to keep information secret. Before the digital age, the biggest users of cryptography were governments, particularly for military purposes. Most forms of cryptography in use these days rely on **2.** .........................., simply because a human-based code is too easy for a computer to crack. Ciphers are also better known today as **3.** .........................., which are the guides for encryption – they provide a way in which to craft a message and give a certain range of possible combinations. A key, on the other hand, helps a person or computer figure out the one possibility on a given occasion.

Computer encryption systems generally belong in one of two categories:

- Symmetric-key encryption
- Public-key encryption

In symmetric-key encryption, each computer has a secret key (code) that it can use to **4.** .......................... a packet of information before it is sent over the network to another computer. It is essentially the same as a secret code that each of the two computers must know in order to **5.** .......................... the information. The code provides the key to decoding the message.

Also known as asymmetric-key encryption, public-key encryption uses two different **6.** .......................... at once, a combination of a private key and a **7.** .......................... key. The private key is known only to your computer, while the public key is given by your computer to any computer that wants to communicate securely with it. To decode an encrypted message, a computer must use the public key, provided by the originating computer, and its own private key.

Adapted from: *http://computer.howstuffworks.com/encryption3.htm*

**5** Summarise the most important facts about data protection. Include an example for each category.

Start with: *The concepts of data protection are...*

**6** You need to send a confidential file through the Internet. As prevention is the best way to act, decide what you would do to ensure the following.

- Confidentiality
- Integrity
- Availability
- Authenticity