English

Data Access

When you store information electronically you are leaving information on resources that are easily accessible. Restricting access to non-authorised persons is vital when it comes to your data. It does not really matter what data you store, what is important is that access to the information is only granted to you (or whoever is supposed to have access).

The authentication mechanism works based on 3 (most usually) elements

- A user identification or piece of information that will identify the user as part of the system to access. This is usually referred to as the login or user id. It is also common to have the email of the user substitute a login due to the uniqueness of this information.
- A user secret value or key (commonly referred to as password) that is used to authenticate the person attempting access.
- An algorithm that somehow combines the user id with the password and produces a unique piece of information (that no other combination can produce). This information is stored in the protecting entity database and is used to verify the identity of the person attempting access.

Here is how it works. When the original user created the account they selected (or were assigned) a user name and a password. The algorithm generated the unique value and it was stored. Later, for the user to gain access, they need to enter their user id and password. The protecting entity reads in the information and, using the algorithm, generates a unique value. The generated unique value is then compared with the unique value stored in the database. If the two values match, the user is authenticated and access is granted. If the two values do not match then access is denied.

The importance of the password

In everyday usage of technology we have to authenticate ourselves in order to gain access to our data. Unlocking your mobile phone (code, fingerprint, and face recognition); logging onto windows (code, fingerprint scan); accessing online banking (code, 2-way verification); we are entering password after password in order to open machines, start applications or access services and/or resources. Choosing, using and safely keeping your multiple passwords is very important.

<u>Choosing a password</u>

Many systems can generate and supply a password (usually difficult to remember) or they will allow you to select your own but can request that the selected password must meet certain requirements. Usual restrictions include:

- Length of the password. The longer the password the more difficult it is to guess. A usual restriction is a minimum of 8 characters
- Including lower as well as uppercase letters. Passwords are **always** case sensitive so using lowercase and uppercase complicates the password more
- Including at least one digit. Mixing letters and digits further complicates the password, thus making guessing more difficult
- Including symbols (like !, _, @, #, %, &,), (, [etc.). Incorporating (one or more) symbols complicates the password more.

Choosing a password is important. Combining letters (upper and/or lower case) and digits and symbols ensure a high complexity password. The more complicated the password is the more difficult it is for it to be guessed / discovered.

<u>Using passwords</u>

It is a fact that in modern society users are required to remember and use a considerable number of

passwords.
It is tempting to use and reuse the same password(s) for a number of applications and services. However, such a practice is not advisable. If your password is discovered then your accounts are in danger.
Modern computer systems and browsers can store your passwords and use them when you visit specific pages. This is something that can be used but only if you are the only one using the computer. If you are using a shared computer in a lab or an office then you should not allow any application to store your passwords.
One more approach is to write down your passwords either in a hard copy file (on paper) or in electronic format and save it in a location that you are aware. Both these approaches are **not advisable** since the information can be compromised.

Safe keeping passwords

Due to the number of passwords that must be remembered, a common approach to use is to install some password management software application. Applications like these give you the ability to save as many passwords as you like in a database and look them up whenever you need them. Password management applications use what is called a 'master' password, which is needed in order to start up the application and access the database (and remaining passwords).
One other, a little bit more manual approach, is to create a file to store your passwords and then either encrypt the file using some encryption application or add the file to a compress archive and use a password to protect the file.