Maastricht University

Safe use of passwords

This document helps you find out how to create and use safe passwords. The information is organized as follows:

1. Safe passwords
2. Managing and remembering multiple passwords
3. Strong authentication for the administrator and other sensitive accounts
4. Be Aware

1. Safe passwords

A password's safety depends on its length and its complexity.

General guidelines are:

- The longer the better
  - è Less complexity needed
  - è Easier to remember
- The shorter, the more complexity needed
  - è More difficult to remember
  - è More difficult to type (especially on smartphones and tablets)

UM's password policy is a compromise between usability and technical constraints within the UM-account environment (Windows).

General UM policy

- The minimum length of a password is 15 positions;
- A password may not contain your username;
- A password must be different from your last 5 passwords;
- An initial password has to be changed at first logon;
- A password has to be changed if it might be compromised (e.g. through phishing);
- A password has to be changed at least once a year.

Additional UM complexity rule

A Password must meet at least 3 out of 4 of below criteria:

- Minimally 1 uppercase alphabetic character
- Minimally 1 lowercase alphabetic character
- Minimally 1 numeric character
- Minimally 1 other symbol (e.g. space, dot, @, %, etc.)

Maastricht University

Strong passwords are not always easy to remember. For this reason, it can be useful to choose a password in the form of a short phrase that has meaning to you. Examples of strong passwords phrases are: “I like football.” (meets 3 out of 4 criteria) or “We went 2 school” (meets even 4 out of 4 criteria).

2. Managing and remembering multiple passwords

As a user you generally have access to various systems both at the university (Wifi-access, email, web applications, etc.) and in your private environment (Internet banking, email, chatting, online shopping, etc.), requiring different access codes and passwords. Below are some tips on how to manage various passwords safely.

Choose different passwords

Choose different passwords for each system, and be careful not to use easy “guessable” variations.

Choose strong passwords

Even if a specific system has no mandatory complexity or length rules, choose a strong password.
If long passwords are not possible, increase the complexity for instance by compiling your passwords using easy-to-remember sentences, from which you can then derive letter/digit/symbol combinations. To increase complexity, use easy-to-remember substitutions such as “!” instead of “i” or “3” instead of “E” and special characters like “%”or “@”.

Example: With the sentence “A strong password which has only 8 positions", you can compile the password “@SpWh08p”;

Make sure your password is YOUR secret.

- Never write down or store passwords in directly readable form;
- Avoid situations where others can watch you type in your password;
- Change passwords sent to you by letter or email as soon as possible;
- Should you wish to write down your passwords safely, use a code in which parts of the password need to be replaced by codes known only by you;
- Never store passwords in devices (e.g. tablets) or browsers used by multiple users;
- Change your password if you suspect that it could be compromised (e.g. through phishing or a virus infection) and at least once a year.
- Never share your passwords with others!

Use a password manager
Choose a safe password manager to generate and store your web-passwords.
More info on: https://en.wikipedia.org/wiki/Password_manager

3. Strong authentication for the administrator and other sensitive accounts

Your PC or laptop has a special access code for administrator tasks (the 'administrator'). Do not use this access code for your daily computer activities, and take additional security measures for this code. The same applies to other sensitive systems, such as Internet banking, medical databases, etc.
Your system manager may enforce you to use a strong authentication, which is based on two or three criteria (2 or multi factor authentication):

- *Something you know:* your access code and corresponding strong password;
- *Something you have:* a smartcard with pin code; a mobile telephone for SMS reception or a special App; a token or special calculator aimed to create one-time passwords;
- *Something you are:* for instance your fingerprint, iris-scan or face recognition.

If no provisions for strong authentication are available, you should create an extra-strong password
and use it very carefully. In doing so, follow the general guidelines for strong passwords, and:

- create a password that is as long as possible, but at least 20 characters.
- change the password more often, e.g. every three months.

4. Be aware (of phishing):
Never be tempted to reveal your password!
No one, not UM (ICT-staff), nor banks, nor web shops will ask you for your password via email or in a phone call. So, never give it away. If you do not trust the situation, contact the organization involved through one of their publicly known contact channels.
(Do not copy-paste the URL of their website, but use your bookmark or type it in yourself).