

## A safe (= difficult to crack) password should meet the following criteria

1. It must be at least 8 characters long. (all words of up to seven characters are deemed able to be generated and tested by machine within a reasonable amount of time). We recommend that the password consists of the following characters: a-z, A-Z, 0-9, !, +, -, : ; < = > \_

Generally it is good to use special characters, but the following should be avoided: å ä ö @ €

2. Do not use passwords that are directly related to yourself, your family or your workplace and that others might know, such as a social security number, phone number, license plate, your initials, user ID or other accessible information.
3. In addition to letters, you should also use numbers and special characters. Both capitalized and lowercase letters should be included. (Some net based software may however lead to problems.)
4. The password should not consist of words in a glossary or dictionary. Also, do not concatenate two simple words to create the password. Personal names (concatenated), should be avoided for the same reasons.
5. Do not use simple keyboard patterns such QWERTYU or 1qaz2wsx
6. If the intended password contains parts of words, then replace, remove, or append one or more additional characters. Using a normal, full word or name with a character exchanged, deleted or inserted does not give sufficient security, it is not good enough to write a word or name backwards.
7. Obviously, one should also avoid letting the computer save the username and password for automatic login. In systems with very important or sensitive information, the system administrator should ensure that all new passwords are tested with CRACK or similar programs. It is also

desirable that the system is configured in such a way that frequent login attempts are not allowed.

## Recommendations

To help you remember the password, while being safe enough, one of the two following methods are recommended:

- A. Construct the password from the first letters of each word in a phrase taken from a poem, book title, literary quotations, lyrics, psalm verse, theater replica, chant, slogan or an ordinary sentence. (The result should of course not be a normal word, etc., mentioned earlier.

Also avoid famous quotes. Use a mix of uppercase and lowercase letters, plus any numbers and special characters.

For instance you can from the phrase, "*time may change you, but you can't change time*" form the password *Tmcy8y2ct!*

Note, we change the b from *but* to an eight since capital letter B looks almost as an 8. And the words *can't change* are two c = 2c

- B. Another method is to select a substring of 8 characters (without spaces) out of such a phrase, beginning at any location. Moreover, at least one upper case and number or special character should be included.

For example, password *t!me-5+ch* formed from the aforementioned phrase by adding special characters and by replacing certain letters with special characters (*may* is for instance the fifth month)

You should put a lot of care in designing a secure password. It is better to keep a good password for a long time than frequently changing between bad passwords. (If you suspect that an unauthorized person may have had knowledge of a password, it must be changed immediately.)

A new password should be planned carefully, rather than quickly constructed. If you have a good rule for how to create a password, then it will be easy to remember and need not necessary to be written down.