

## How do I Create a Good Password?

**NOTE:** This document is intended as a set of guidelines for creating secure passwords. Please **DO NOT** use any of the password examples mentioned here.

Please see the ECSM Service Level Agreements (SLA) for basic password requirements for [Students](#), for [Staff](#), and for [Faculty/PhD](#) Candidates.

In addition to the requirements in the SLA, the following paragraphs describe "good" password practices:

Passwords are annoying. It's hard enough to remember one password, but nowadays you've got your e-mail password, your database password, your file server password, passwords on all kinds of different web sites, and what's more, some of them make you change your password all the time, and then they complain about the password you choose!

There are good reasons for all the restrictions. Your e-mail password protects more than just your e-mail; in most cases, if an intruder figures out your e-mail password, he becomes a threat to the entire e-mail server. He/she can break into other people's accounts or even the system administrator (or "root") account. Once he's done that he can read, change, or delete any e-mail on the system.

Now days intruders can use many different programs to crack passwords. One of these programs is called Crack. Crack takes a list of words--usually a big English dictionary combined with foreign dictionaries and lists of people's names, cities, etc.--and tries to match the words in that list against your password. Crack also permutes the words in several ways, such as replacing o's with 0's.

A good password is one which can't be discovered by any of the currently available cracking programs, so don't use a password which is based on a word or a name, English or foreign. All-numeric passwords are also unsafe, because they can be discovered by brute force. Passwords which contain special characters (such as punctuation marks) tend to be stronger, but some of these cracking programs also use special characters in some of their permutations.

Another note that while many systems will accept passwords longer than 8 characters, most of them ignore all characters after the eighth. So when judging the strength of a password, think of only the first 8 characters. (For example, "password!" is equivalent to "password"-- a very weak password--on most systems).

### DO's

- All passwords must be at least nine characters in length. However, you can strengthen your password, depending on the operating system, by increasing it to:
  - (UNIX) nine characters in length
  - (Windows) fourteen characters in length.
- Passwords must contain a minimum of one character from at least three of the following four classes:
  - Lower case letters
  - Upper case letters
  - Arabic numerals (i.e. 1, 2, 3, 4, etc)
  - Special characters such as !, #, %, \$, \_, @, \*.

### DO NOT DO

- A password should **NOT** be derivable from any public information about you such as:
  - Full name
  - Calnet directory information
  - Account or login name
  - Office number
  - Phone number
  - Active Directory Information
  - Etc...
- A password should **NOT** match or resemble any word found in any dictionary or any list of words, English or foreign. This includes names also.
- A password should **NOT** be reused.
- A password should **NOT** use a word with a single number or character before or after it. (i.e. **gobears!** is not a good password)
- A password should **NOT** use a word with any number that can be easily substituted for a letter. (i.e. 0's substituted for o's, 1's for l's, etc.)
- A password should **NOT** use a simple word with just one capital letter. (i.e. **Gobears** is not a good password)
- A password should **NOT** be based on:
  - Modifying any part of your name or name+initials;
  - Modifying a dictionary word;

- Popular acronyms;
- Any systematic, well-adhered-to algorithm or pattern whatsoever.

### Bad passwords:

- alec7 - it's based on the users name (and it's too short anyway)
- gillian - name (in a dictionary)
- naillig - name backwards
- PORSCHE911 - it's in a dictionary
- 12345678 - people can watch you type it
- abcxyz - people can watch you type it
- 0000000 - people can watch you type it
- Computer - just because it's capitalized doesn't make it safe
- wombat6 - ditto for appending some random character
- 6wombat - ditto for prepending some random character
- merde3 - even for french words...
- mr.spock - it's in a sci-fi dictionary
- zeolite - it's in a geological dictionary
- ze0lite - corrupted version of a word in a geological dictionary

These examples emphasize that a password derived from a dictionary word (or personal information), modified in some ways, constitutes a potentially guessable password. Modern password cracking programs are equipped with dictionaries of a dozen languages, proper names, religious texts (e.g. the Bible and the Koran), myths, phrases, almanacs and whole major texts (e.g. Paradise Lost). Additionally, modern password crackers test for rotations (e.g. anHalenV), reversals (e.g. yelekreb), numerical padding (e.g. student9), letter

replacement (e.g. ball00n) and dozens of other rules. A secure password should avoid all the above weaknesses.

### Good passwords:

The problem with following these guidelines is that they make passwords difficult to remember. Creating a strong password and then putting it on a sticky note on your monitor defeats the purpose. However, it is possible to create memorable passwords and still follow these rules. One trick is to make acronyms of phrases or sentences. For example, "ain't nobody's business if I do" could become "a't0bild", which was a very strong password until it was printed in this tip.

It is possible to "adapt" perfectly ordinary words into passwords by being "creative". For example (and please do **NOT** use this or any of these examples as a password), the word "ordinary" can be changed to "Ordi^NarY" by changing the "o" to "0" (zero), "n" to "ctrl-n", and capitalizing Y.

- Hbs@B#1! - Haas Business School at Berkeley is number one!
- 65ma>80+ - '65 Mustangs are better than anything from the '80s
- F242'sue - Front 242's (some stuff)
- 44\$Tnitc - (some stuff) the network is the computer
- 8ILMHIsf - (some stuff) I left my heart in San Francisco

If you have any questions about or need assistance in changing your password, please contact the ECSM Helpdesk at:

[helpdesk@haas.berkeley.edu](mailto:helpdesk@haas.berkeley.edu)