

Selecting a Good Password The objective of a password is to be Secure i.e. not easily guessed or hacked by a computer, however a password should always be something which you can easily remember or deduce.

Secure Security of a password particularly online is crucial, especially since hacking programmes are more sophisticated that they can try various combinations to break them.

It is noted that men often choose a passwords associated with nicknames, sports or other hobbies, while women often use real names and anniversaries. People are creatures of habit so if someone realizes you choose an actors name

Some habits people have is to just add 1 at the end of a password when the system demands that a password be composed of alphanumeric and at least one number. Another is to substitute “1” for “i” or “3” for “e” or “0” for “o”, eventually “crackers” - systems to break passwords will try such obfuscating.

Memorable There is no point in having a secure password if you don't remember it. But how to be memorable whilst still being secure, one method is to say use the first letter of a line of a poem, song, title of a book, e.g. wifmsitot (let it be) since the letters do appear random, another enhancement could be to alternate capitals, or capitalise vowels e.g. wIfmsItOt another trick to use, is to have a number which is memorable to you, year of birth, age at last birthday, part of phone number, car licence number and append it to your password. The key is to have a system which you can recall and deduce your password even if you forget the actual word.

Good Practice

- Have different passwords on different systems, limits damage if a password is exposed
- Have character sequences which appear random
- Use a combination of upper and lower case letters
- Use Numbers and other characters
- 6 characters long minimum, 8 is better (the limit on our Unix system is 8)
- Change your passwords frequently (some systems prompt you to update your password periodically)
- And remember your password (or the system you use to create it).
- If your password has been compromised, or a system upon which you used it was, change your password, and if you have used the password on a different system(something which you should avoid doing) change it there aswell.

Bad Practice

- Don't write your password down on a post-it note and have it beside your PC
- Don't tell anyone your password
- Don't use the same password on multiple systems
- Don't use an obvious name, or word, which is easily guessed
- Don't use your name, maiden name, spouses name etc.
- Don't just add single number at the start or end of a password if you need a numeric in your password.
- Don't use a common word spelt backwards because "crackers" are clever enough to break this.
- Don't use "1234", "0000", or "password". (Phone hacking in the UK was made easier, by public figures not changing their voice-mail passwords from the default)

Summary Have a system in composing your passwords, and use a number of obfuscating techniques and not just one. Remember your passwords, and keep them secret.