

How to choose a secure Password

While all passwords are stored encrypted in our database, it is generally recommended that you use a **unique** password for each Internet site you register with. Some available tools that assist you in password creation or provide secure password management are:

- ◆ [PasswordSitter](#) by Fraunhofer-Institut für Sichere Informations-Technologie (Fraunhofer SIT), Darmstadt, or
- ◆ the [PasswordSitter online version](#) provided by Swiss security specialist e•siqia based on the Fraunhofer SIT's technology.
- ◆ [Keepass Password Safe](#)

Disclaimer: While we recommend the above software, we cannot guarantee that these will work on your system correctly or are free from any faults. If you are having any problems, please contact the respective development team.

Further tips on creating your password:

- ◆ You might consider using an easy to pronounce password that is **not an actual word**, such as veminad - achieved in this case by **alternating consonants and vowels**.
- ◆ Combine this with some **numbers** and/or **special characters** to get an even more secure password, e.g. veminad21%.
- ◆ Additionally alternate between **lower-case** and **upper-case**, vEmInAd21%.
- ◆ You might also want to consider a memory hook or sentence related to the site in question. For example "Combat the signs of ageing", but use for your password just the first two letters of each word and once again alternate between lower- and upper-case and add some numbers and/or special characters to the mix, i.e. CoThSiOfAg66\$.
- ◆ Instead of adding a number at the end, you might want to consider replacing some letters with numbers, i.e. T with 7, I with 1, E with 3 in which case vEmInAd looks like v3m1nAd.
- ◆ But always keep in mind that your password should at least consist of 8 characters.
- ◆ However, do **not** just choose a simple password with words that come straight from a dictionary, e.g. MyNameIsJoe21.