Secure Password Thinking

Last Updated Monday, 26 November 2007

Secure Password Thinking

Any password you create for Joomla!, MySQL, Apache, or in fact any passwords you ever create, should be made as secure as possible.

Typically this would mean:

- using a minimum of 6 characters - the more the better but 8-10 should be an ideal

- a mixture of upper and lower case alphabet characters, numbers, and permitted special characters for example -, _, *, $, !, %, although the use of these may be governed by the host settings on shared or virtual hosted, remote servers

- do not use easily identifiable passwords for example, birthdays, children's or family names, or words that could be easily associated with you

- in fact try not to use real words at all, replace letters with their numeric equal so the word ocean could become 0c34n (yes â€“ I know it is a real word and there are only 5 characters but it is just an example) try 0c34n!c â€“ and no do not now use that either

- another way is to think entirely off-the-wall. Think of a favourite novel for example, The Hitch-hikers Guide to the Galaxy, and then take say the first and last letter from each word giving a sequence of letters (as indicated by the underscores):

Example 1: t e h s g e t o t e g y

Â this clearly means absolutely nothing but it could still be traced â€“ eventually â€“ by a determined cracker so let us mix it u a bit more:

Example 2: T 3 h $ 9 3 t 0 T 3 g Y

(again ignore the spaces) but you can now see that it would be a pretty illogical logic that would need to be applied to even come close to cracking that and when the additional security features of the various platforms is then laid over the top of this â€“ we would not want to say it is impossible to crack, but they would take a very long time,

- you should regularly change your passwords certainly on critical sites

- if you keep a written record of your passwords, always ensure they too are kept secure and safely out of the way of prying eyes

- despite the temptation, try to avoid using the same password for all your various access requirements, both at home and at work

The spaces
are included in the two examples solely for clarity and should not be
included and in fact spaces are generally not accepted in passwords

Password Managers

One of the issues that can be experienced particularly when there are a lot of passwords that have to be maintained - especially as more and more services and utilities switch to, or offer, the option to deal with your accounts online -Â is actually remembering what all of these passwords are.

Most of todays browsers have an inbuilt facility to remember passwords and form completion details but there have been concerns raised over the security of these facilities in the past. It is a case of one program trying to do too much. If you feel this way and don't trust yourself (or your environment) to write down passwords properly and maintain this in an accessibe format then you might consider using one of the dedicated Password Managers that have been developed.

These can often be found as an integrated part of your Internet Security Software or you might consider one of the many commendable Open Source or indeed Commercial alternatives.

Password Managers are dedicated software programs that apply high levels of encryption to secure your passwords and other data, yet give you an easily accessible repository for the information when you need it. Essentially you only have to remember the one password, which should be the most secure you can make it as described above, and the program holds all of the other information ready for when you need it.Â

Â For details on the available options check out the many Open Source and other format download sites and check out the customer & industry reviews that accompany the software and make your choice.

Password GeneratorsÂ

One of the benefits of this type of program is that they will often have a Password Generator that will create a completely random password for you. Takes a bit of the brain strain out of it all! These are also available as a separate standalone application.