What the Tech?!: Pa$$w0rd$

by Joe McCormick

If you're just starting to use Internet, computer networks, or other account-focused services, you will find that a lot of the use you get out of them will be through a personal account that you make. Whether you want to create your own e-mail, gaming, or social-network account, protecting your information and identity is very important. As the Internet grows, its users are finding new ways of applying programming technology to both good and bad uses.

Creating a strong password is the most important thing you can do when protecting the online identities you create. Techniques such as guessing, precomputation, and brute force attacks can give an experienced hacker easy access to your passwords, if you leave yourself vulnerable; the best thing to do is create a password that makes these techniques impractical.

When creating your password, there are a few key ideas to keep in mind. Many password-cracking applications can easily get past simple, every day words. For example, the word “dinosaur” is a weak password because it can be found in the dictionary. Another thing to remember is that just because you change a few letters in the password does not make it any stronger. For example, “dinosore” is just as weak as “dinosaur” because hackers can attempt to crack multiple letter combinations in less than a second.

So what makes a good password? Ideally, you want to make it as complex as you can. Companies such as Microsoft and Google suggest the following important factors: include punctuation marks (!,”?.') and numbers, mix capital and lowercase letters (diNoSAur), use symbols to substitute for alike letters ($ for S, 0 for O), create a unique and personal acronym, and use phonetic sounds to spell instead of the letters they represent (“kat” for “cat”).

Using our example and these tips we can come up with a stronger password: “|)!n0$@Ur” will only rank medium on some password checkers because, although it may seem complex, it is not very long. If a website gives you the option to make your password as long as you want, 16-20 characters long with the complexity of our example “|)!n0$@Ur” will make your password virtually impossible to crack; however, some websites have limits on length and which characters you can use, so be aware.

When creating a password you may be able to see a meter on the page that will tell you how strong your password is, but if you don’t you can find one on Microsoft’s website (https://www.microsoft.com/protect/fraud/passwords/checker.aspx) which will allow you to know exactly how strong your password is. When you do create a strong password, only write it down until you have it memorized-but it’s best if you can never write it down at all-and never send your password in an e-mail. Never tell it to anyone under any circumstances because at that point you lose full control of your information. And finally, test your password occasionally and even change it from time to time; this will ensure that your data is protected.

Do you have any questions about this article or a suggestion for another one? Send your e-mails to wtt.globe@gmail.com