http://www.marksanborn.net

Picking Strong Passwords that you can Remember

by Mark Sanborn

Passwords are needed for just about everything now. How do can you remember them all? Some sites force you to have 8 character password some 6 some even force you to have numbers in it. So how do you come up with a password that is strong yet easy to remember possibly even a different password for each site you visit?

So what is a weak password?

Here is Wikipedia's short list of passwords or types of password that shouldn't be used.

- admin — too easily guessed
- 1234 — too easily guessed
- abc123 — too easily guessed
- susan — common personal name
- password — trivially guessed, used very often
- p@$$\V\/0rd — simple letter substitutions are pre-programmed into cracking tools
- rover — common name for a pet, also a dictionary word
- 12/3/75 — date, possibly of personal importance
- December12 — Using the date of a forced password change is very common
- nbusr123 — probably a user name, and if so, very easily guessed
- asdf — a sequence of adjacent letters on many keyboards
- qwerty — a sequence of adjacent letters on many keyboards
- aaaa — repeated letters, can be guessed

Strong Passwords you can Remember

A strong password contains a non dictionary word and has both alpha and numeric characters. It may look like this.

j7ayaYY88v

But how do we come up with a password that appears entirely random yet easy to remember?

I will show you a way that I think is easy to remember strong passwords or even one separate password per site.

Start by choosing a base password a set of characters or mini password that all your password will contain. This may be a password that you already have memorized and have been using for years. Or it could be something that you just thought of that would make for a good strong password. It is critical that this base password meets the following rules.

- Not a word in the dictionary
- Contains at least one number and/or symbol
- At least 8 characters long

A way to come up with this type of password that is easy to remember is to use acronyms to your favorite poem, movie, or simple phrase. One example may be: *YdkmPa!* Which converts to *You don't know my Password anymore!*.

You can also come up with a password that is completely random that is based off of your old password. Lets say your old password was *password*. This very common password can be made more secure by substituting each letter or every third letter for a number. Lets start with the first letter, 'p'. This letter may represent a 9 since it looks similar. The next letter to convert is a 's'. Since this litter makes a ssss or zzzz sound I will make this letter a zzzero or 0. The next letter would be an 'o'. This also can be a 0 since it is similar shape. So our end password would look like.

9a0sw0rd

This of course is an example. You should think of your own way of substituting letters and numbers to come up with an even more secure password. Also when you come up with your own way up substituting you will be more likely to remember it. Here are a few substitution examples.

- Change every 2nd letter to the 4th one down the line in the alphabet
- Change only the letters in the top row of the keyboard that corresponds to the number above it. Example q=1, w=2, e=3 etc..

(This may vary on different keyboards)

- Change letters to numbers based on sounds or down strokes. Example l=1, n=2, m=3

Different Passwords for Different Sites

You may not want the same password for every site you visit in case one of your passwords were ever compromised. What comes to mind for most people at this point is, oh no now I have to remember a new password for each site. It actually is quite easy to have a different password for each site and have it easy to remember. Here is an example.
Site: gmail.com
Base password: *password* which translates to *9a0sw0rd*.
You need to pick something from gmail.com that every site you visit in the future will have but will be different. An example of this would be the 2nd letter and third letter of the url. Or maybe a more obsecure one could be the 5th – 8th letters of gmail's SSL certificate (I think this changes about once a year so be careful).
Once you have some letters/numbers that are specific to the site you visit (in this case gmail.com) you can then directly append them to your password or do the same substitution you did before or come up with an entirely new one.
Site: gmail.com
Base password: 9a0sw0rd
New password: 9a0sw0rdma (taken directly from the 2nd and 3rd letters of the domain)
Again come up with your own substitution that makes sense to you.
I understand that most of the time simple passwords are fine because most modern sites will allow only a few attempts before kicking you out of the login page; however, password cracking techniques are always improving and I think this method of generating multiple passwords for different sites is quite easy and sometimes fun . So I encourage you to stretch your imagination and come up with ways of making your passwords more secure.

Using Hints

If the site offers you a hint – USE IT! This can help with easy recovery of a password. Use a descriptor of what the password is 2nd letter.