How to Choose a Secure Password

Choosing a secure password is a matter of creating unlikely letter and number combinations. The more obscure your password, the tougher it will be to crack.

1. **Do not use words or phrases that have personal significance**.

2. **Mix letters, numbers and symbols, and use case sensitivity (upper and lower case letters)**. This mixture is known as "pseudo-random alpha-numeric combination"; using this, it is almost impossible to "crack" somebody's password. (i.e. instead of "password," try "pAsS34%(6*2woRd," etc.)

3. **Find a good way to remember**. A good way to do this is to choose the first letters of a sentence that you will remember. e.g. *"I have 2 dogs called Rover and Fido"* gives: Ih2dcRaF

   - Use punctuation to your advantage. To incorporate a colon into the previous example, remember the sentence as *"I have 2 dogs: Rover and Fido"*, which would give: Ih2d:RaF

4. **Use a base password.** Use the sentence from above as a base password, and add an increment to the end (e.g. Ih2d:RaF01). When the password expires, just increase the increment. This way you can remember the base password, and write down the increment. If someone finds the increment, they won't be able to guess the base password.

5. **Try to memorize the password, and avoid writing it down**. Somebody could very easily find the slip of paper that the password is written on.

6. **The longer the better**. Don't make a password that's less than 6 characters. Anything less can be cracked from brute force software.

7. **Take the street you grew up on, and your first pet/something hard to guess from your past, put a number sign in between, substitute some letters for numbers, and, voila**! A great password. For example: Bill grew up on Ocean Avenue, and his first pet was Rocky. His password would be: 0c3an#r0cky. You can add random capitals to make it more secure.

8. **Do not use the same password for everything**. If someone finds this password, they would have access to everything. At the very least, make at least one password for sensitive things (i.e. online banking, etc.) and one for everything else (AIM, email, etc.). Here is an example:
   a. Let us suppose you have 5 email accounts, 3 operating system passwords, 3 bank accounts (each with user name, password, extra security pin), 10 internet forum user/passes, 1 cellular phone (uses 2 to 4 pins). (If you are a programmer or db administrator, multiply the total by 3). Say for each of these, you chose a variation of "pAsS34%(6*2woRd,". Try to memorize 20 of those gibberish sequences! It's quite difficult, but if you make your sentences relevant to each situation, it will be easier - for example, for banking, your sentence could be *"I want to have 1 million dollars every day"* (Iw2h1m$ed), and for your emails it could be *"I hope no one reads my emails!"* (Ihn1rme!).
   b. Use something you see whenever you need this password to generate the password. Federal Security Bank might lead to FsBmA3456.
   c. Use a telephone keypad or 10 character phrase (i.e. blackstump) to encode numbers as letters or vice versa.