## Creating and Maintaining Secure Passwords

In my day I’ve seen more than my share of passwords taped to the bottom of keyboards, written on sticky notes on the monitor, or scribbled hastily on a notepad. I’ve even see text files on peoples desktops containing the passwords to their banking websites. If anyone reading this things that’s a good thing you definitely should put into place the practices I’m about to outline in this article. The basic premise of a password is that it is a SECRET. No one else should know your passwords. And yes, I said passwordS plural, with an “S” on the end. Every password you have for every site that you deem important should be different. And your throwaway password should be different from all of those. I can already hear the gnashing of teeth after that last sentence, “remembering all of those passwords is impossible! I’ll forget them all and be locked out of everything!”. SILENCE PEASANTS! The Emperor will show you the way. The secret to maintaining secure passwords and still being able to remember them all is a Password Schema. To create a Password Schema you first choose a five word phrase, our example will be “The Best Five Word Phrase”. Now we head on over to the “Leet” Speak Translator , www.brenz.net/l337Maker.asp and convert that phrase into letters, numbers, and symbols. What I get for our example phrase is “7|-|3 b3$7 pH1\/3 \/\/0rD p|-|r4$3″. Some of those symbols aren’t valid password characters, so we will have to clean it up a bit. The final result is “7H3 b3$7 pH1V3 W0rD pHr@$3″. This is the basis for every password we are going to make. This is what you can write down. Ideally you only write down the unconverted phrase, but if you aren’t familiar with “Leet” speak conversions you can safely write down the converted phrase. The next step is to choose a separator character. I like to use ! for my separator. You can use any symbol which is valid for a password field. Generally ! @ # $ % ^ and & are all valid. Now to generate a password with this phrase. I chose as our example website Bank of America. We have 3 words to work with, Bank, Of, and America, so our password will have three sections. We start it off with our separator character !, then we take the first vowel in the first word, bank. So we use the first word in our phrase 7H3. So far our password looks like this !7H3. Now add another ! and take the first vowel in the second word, of, so our next password part is the fourth vowel (A E I O U) which means it will use the fourth word in our phrase, W0rD. The password has become !7H3!W0rD. Now the last word is America, the first vowel is A again. So one more separator character and the final part of our password is 7H3, then the closing ! and you have your new Bank of America password which is “!7H3!W0rD!7H3!”. That password will pass even the most rigorous security analysis. It is impossible to guess and very resistant to cracking attempts. It’s also easy to remember. You know your phrase, and you know how the phrase is applied so you never need to remember a password again. Just write down your pass phrase and start generating secure passwords. For a quick reference breakdown here is how the schema works in a nutshell: Separator: ! Base Phrase: The Best Five Word Phrase Translated Phrase: 7H3 b3$7 pH1V3 W0rD pHr@$3 Vowel Assignment: A     E         I     O     U Site Name: Bank Of America Final Password: !7H3!W0rd!7H3! If your banking and personal information is really important to you, then I strongly recommend using this approach. Your middle name and the last 4 digits of your SSN is NOT a secure password.

## About the Author

The Emperor from The Tech Empire is a ten year veteran of the IT field, and has worked with companies from Orlando to Maryland along the east coast including projects with IBM and NASA.

Source: http://www.citylinkpcs.com.au