SoHo E-spirin E-zine
brought to you by Funai Pty Ltd IT Handyman Services
For Small Office/Home Office and Small Business. IT Tips & Tricks.

Learning to Swim with Passwords

by Allan Naguit. August 2005.

Are you drowning in passwords? They seem to be a necessary evil. Passwords take many forms. There's the password for your phone BPAY account. There's your ATM PIN, your work building keypad combo, bike chain lock, briefcase lock, online-banking password, email password, PC logon password... the list goes on and on. The other day, I decided to count just the number of my internet-related passwords: sixty-one. That's right, sixty-one! Of course, some of those are for one-off sign-ups to forgotten internet accounts and such, but the rest are ones I really need to remember. How in the world do I keep them under control?

Commit them all to memory and burn the evidence. Hmm. My memory's not bad, but 61? Too hard for me.

Write passwords down on paper. Be aware, doing this is against the security policies of many companies. However, Jesper Johansson, a Microsoft security guru, recently said it was okay to do just that:

"I have 68 different passwords. If I am not allowed to write any of them down, guess what I am going to do? I am going to use the same password on every one of them."

You can read the full article here (Cnet News.com):
http://news.com.com/Microsoft+security+guru+Jot+down+your+passwords/2100-7355_3-5716590.html?tag=nefd.ac

As he implied, doing this is a bad idea because, once such a one-for-all password is broken, you've effectively left all your "doors" wide open for the bad guys.

Write down reminders or questions to passwords. For example, "What was the name of your first pet?" "What was the full street address of your first flat?" "What's your 'porn name'? (That is, what was the name of your first pet and the name of your first street address?)" "Where did you have your first kiss and how old were you?" The last few make for slightly better passwords because the answers are a combination of letters and numbers. This leads us to the issue of how to make **strong passwords**. (Later, we'll go back to looking at how else you can manage your list.)

Why Should You Come Up With Strong Passwords?

There are password-cracking tools out there that make mince meat out of those composed of normal words. There's a method called a **dictionary attack** or **brute force attack** where a hacker tries word after word until they guess your password. This means, you should never use anything that can be found in the dictionary. And choosing a non-English one doesn't necessarily help either. The people at the Network Security Center for the University of Chicago claim they've seen the use of non-English dictionaries including for Finnish, German, Chinese, Yiddish, Dutch, even "jargon lists" in Biology, Physics, Computers, movies, place names, etc.

So How Do You Make Strong Passwords?

There are several dos and don'ts in the making of a strong password.

DON'T:
- ✗ Don't use dictionary words, proper nouns, foreign words
- ✗ Don't use personal information (like your birth date, home number, car registration)
- ✗ Don't use common misspellings

DO:
- ✔ Do include a mix of uppercase and lowercase
- ✔ Do include numbers
- ✔ Do include punctuation/special characters
- ✔ Do remember: the longer the password, the harder it is to crack (8 or more characters is considered good)

How Good is Your Password?

Here's a useful tool from **SecurityStats.com** to check the strength of passwords. Enter them on their website and you'll get feedback on their strength when scored against best practices. Note: They don't recommend checking your actual passwords. Instead, try something **similar**. As their website states,

"Please note that although we will not store the password you enter, it's never a good idea to send your password to someone you don't know. Instead, we recommend testing a password which is *similar* to one you might use."

http://www.securitystats.com/tools/password.php

Plug in the password you want to test in the entry box, click on **submit** and wait for the feedback. The advice on how to improve your choice is very helpful.

How Do You Keep Track of Your Passwords?

As I mentioned before, you could try to remember them all, write them all down, or write the reminder questions to your passwords.

You could also keep your list on your computer.

Wait! Before you scream or groan in disbelief, I agree that keeping your passwords on your PC is a VERY BAD IDEA. Unless, that is, your passwords are protected by an effective **encryption**. This way, even if someone were to steal your computer and prying eyes tried to look at your password list, it should look like gibberish. Only by supplying the proper key (decryption) should your passwords allow themselves to be read.

There are several products out there which allow you to store and maintain your passwords in some kind of encrypted database. The key to your entire list takes the form of a single password. So, you only need to remember the one code. **Just don't forget that one.**

Here Are Two Password Managers You Can Consider:

Roboform was named PC Magazine **Editor's Choice**, and CNET Download.com's **Software of the Year**. It's a Password Manager and a Web Form Filler. This one has gotten a lot of rave reviews. There is a free version and a pro version. The free version is a "try before you buy" type of product and limits the total passwords from 30 to 10 after 10 days. No problem for those who only need to keep track of a few passwords, or upgrade to the pro version as desired. For those with "writer's block", **Roboform** can generate random passwords for you.

(http://www.roboform.com)

Password Safe is an "open-source" password manager. That means it's free! It doesn't have the whiz-bang frills of **Roboform** but neither does it have a time limit nor restricted password-count. If you remember, I have 61 passwords. I use **Password Safe** to keep track of them all. I prefer to invent my own passwords, but like **Roboform**, you can let **Password Safe** generate random passwords for you.

(http://www.schneier.com/passsafe.html)

How Does My Own Password Stack Up?

So. As I surf the net, do my internet or phone banking, all I have to remember is ONE password. With that, I can open up **Password Safe** and get the passwords to all my email accounts, bank accounts, subscription lists, etc. Whenever I have to set up another account and need to remember another password, I simply add that into **Password Safe**. Type and forget. All I have to do is remember the key to the safe: my **main** password. Luckily, these days it's as familiar as my first name.

But how strong is my main password?

Well, first I checked an old one I used for everything before I got wise. I put that into the Password Strength Meter at **SecurityStats.com** and got this:

Ouch! Then I tried (something very similar to) my current main password and this is what I got:

Excellent! By the way, while writing this article I had to add two more to my list. Soon, I'll beat that Microsoft security guru's count of 68 passwords! Not really a good thing, but at least I know I'll "remember" them all!

Allan Naguit is an I.T. Consultant for Funai Pty Ltd, an outfit that provides "I.T. Handyman Services" for small businesses and home offices based in the Sydney Metropolitan Area (Australia). Just like a handyman, but for computers and IT.

For more tips on "how to unblock your computer's pipes", visit our website at www.funai.com.au.