

## Managing Effective Passwords Successfully

### Secure Access Practices

If you are reading this online you probably have a password and most likely many of them, and your challenge is to remember them successfully. And if you work in ICT, then the challenge is much larger; the number of sites and applications requiring passwords has grown to an outrageous number. And, it isn't just passwords: there are security questions, used, for instance, in online banking. Managing this collection of passwords and challenge questions is arduous, if not unreliable. This article will address the question of successfully managing effective passwords and the security around them.

### Password Security - Common Perceptions

Clifford Stole (scientist and author of *The Cuckoo's Egg*) suggests that you should treat your password like your toothbrush: don't share it and change it every six months. There are those who suggest, and in some cases require, that password selection be formula-based. Here is a typical formula:

Secure\_Password =

- 6 or more characters in length +
- Must contain lower and upper case letters +
- Must have at least one number +
- Must include a non-alphanumeric character such as @.!#\$%^&\*(){}|":?[]/

First let's look at the typical user, someone who isn't involved in ICT, but requires frequent access to multiple passwords in their work.

Unfortunately, while an often rotated and complex password will deter a casual passerby with ill intent it does nothing against a determined intruder with physical access to the system. Once in possession of a system's hard drive someone can simply connect it to another computer and transfer the files away. To counter the determined hacker with physical access, I recommend encrypting all files which require being secured.

As well, users generally can't remember complex, often rotated passwords. Mandated complex passwords end up on written on a Post-it note hidden under the keyboard, or worse, stuck to the monitor. The casual passerby, someone not willing to acquire hacker skills, is suddenly able to act with ill or foolish intent.

And when the Post-it note is lost, your typical user will call your helpdesk staff, driving up the cost of support.

### Practical Password Security

Typical users will have access to systems with varying levels of security requirements.

One way to approach having to navigate varying security levels is to assign a password per level rather than per access. This means that the number of passwords required to remember is reduced. When moving to an access which demands a higher level of security a more complex password is used. It's harder to guess, even if someone has obtained your lower level password. For example, the password to access a website where there are no financial transactions such as with [www.linkedin.com](http://www.linkedin.com) is not required to be as complex as a site which has the company's intellectual property. Low risk sites often have weaker security positions than sites with higher associated risks. By using password security levels, you inherently safeguard the data that has a higher associated risk potential.

For areas requiring high levels of security consider using a passphrase, or sentence, instead of just a pass word.

### Generating Random Passwords

There are a number of ways to build a randomly-generated password. A simple method, though not terribly comfortable, is to open a text editor and roll your forehead around on the keyboard. This will provide you with a set of somewhat random characters not based on anything found in a dictionary. More typically, you can have a computer generate a pseudo-random list of character strings and select a password from there. Both of these methods for acquiring passwords typically lead to the Post-it-note problem.

### Crafting Passwords

Crafting your passwords is an exercise in pattern recognition. This method relies on the things you already know well, such as friend's names, favourite colours, or your favourite sport. One trick is to use character replacement in such a name—"cat" becomes 'c@t' or 'c@7'. This can be applied easily to create different levels of security. The password 'c@t' can be used for low level access, while 'bl@ckc@t' is more secure and the pass phrase 'Mybl@ckc@7sn@m3dfr3D' can be used for even more secure sites or areas.

I suggest that when you are crafting your passwords based on things familiar keep one idea in mind – lie. In the examples above, there's an implication that I own a black cat named Fred. I do not in fact own any pets, just orchids.

### How to remember your rotated passwords

Occasionally you may wish to change to password or a system you are using forces a password change. This should not cause you any

concern. Continuing with our example above, one effortless method is to make a simple change. There are two easy options here, change the animal or change the name. The change in password would result in the following – d0g, b1@ckd0g and Myb1@ckd0gsn@m3dfr3D. The advantage here is that it is easier to recall the previous password when you come across an access which still has the previous password. You can reduce the possibility of confusion by maintaining a list of places where you have set a password and when you feel the need to change, go through the list and update it.

### **ICT Password Security**

The ICT staff member is far from the typical password user. ICT staff are charged with protecting a company's IP. They have access to and need to protect the edge and end-points which protect the company's IP. They have a far greater number of access points which require passwords. ICT staff end up maintaining a password list—a list of access points and passwords they are in control of. There are too many to reasonably or reliably remember, and typically, the company owner will require access to this list as well for business purposes. Some passwords may be used only every few months; for instance, back-end server and data-base passwords are rarely used after deployment.

The practice of stepping up password complexity to match security level works here as well. Internal network devices which aren't reachable from the public Internet can have weaker passwords than edge routers should. For areas which require the utmost security, consider moving beyond a single password to a passphrase.

### **Managing passwords**

Password management typically means maintaining a list of access points and the associated credentials required for authorized admittance. Some operating systems and applications provide built-in password management tools. Additionally there are third party applications or password vaults which can be used to store passwords. However, all such storage facilities can be dangerous if you don't have exclusive access to your workstation or storage location. Others with equal or greater access levels than you will still have access to your stored passwords.

Using levels of crafted passwords helps to avoid the need for a password storage system.

### **Conclusion**

It should be understood that passwords alone are not enough. A lot of the security onus remains with the system owners. Systems which allow infinite tries are weak—eventually the password will be compromised. Physical access bypasses passwords and so encryption should be considered around the data, or when data leaves the organization's control.

Passwords are the first line of defence in protecting data or access to data on an Internet connected network. So crafting and storing levels of passwords is vital. Craft your passwords to be hard to guess but easy for you to remember.

Through practical password management you can increase security, reduce support costs and avoid the password on a Post-it-note problem.

Originally published May, 2010

### **About the Author**

Richard Danielli is the founder and President of eSubnet Enterprises. He has broad expertise in the fields of networking and data security. Based in Toronto, eSubnet provides superior customized solutions for networking and data security. Additional articles are available at <http://www.esubnet.com/fragment.html>.

### **Reprints**

1. Commercial use: Commercial newspapers, magazines and websites that wish to reprint an article should contact eSubnet for permission.
2. Non-Commercial use: Any reproduction of content (excerpt or full text) by nonprofit organizations or companies wishing to share information with their members or clients requires that you notify us, whether for print or online usage.

Regarding reprints, contact Mr. Danielli at [rdanielli\(at\)esubnet.com](mailto:rdanielli@esubnet.com) or at (416) 203-1223.