

Free Tech Report
Executive IT Info Series

*"Virtual CTO" Tim Gillen reports on
current business technology issues*

6 Tips for Using Passwords to Protect Against Identity and Business Theft

Ah, those pesky passwords. If you work in the corporate world or in an office, you have one for your PC/Network and, unless there is a password synchronization application that combines them, you probably have more than one for other applications. Add those to the ones that you have for your home Internet, your banking and other websites that require passwords, and before you know it you have a nightmare on your hands in trying to manage them.

Part of the frustration has to do with the different requirements for password formatting. Some systems only require four characters, some require eight. Some need a combination of alpha and numeric characters and others do the same with the addition of a few capital letters thrown in for extra security. It can be positively maddening.

The worst thing you can do with your passwords is to place them in a text document which can be accessed on the hard drive of your computer. Your files are vulnerable - even if you think they are not. If someone is intent on finding them, they can. Even if you place them into a password protected document, those can be cracked, too.

Writing them down has its own vulnerabilities, too, and there are varying opinions on this practice. If you do write them down on a piece of paper, put the document in a locked location whether it is in your home or at work.

Here are 6 tips on how to handle your passwords:

1. Make them complex. People who use easy to remember or short passwords are inviting disaster. Use a little imagination and pick a password that is very difficult to attach to your life. Stay away from birth dates, phone numbers, house numbers, or any other number that is associated with your life.
2. Keep passwords unique. When you change your passwords, make them unique from each other. Do not use the same password on all of your sites. If you do, then you are open to having every site that you have a password to being vulnerable to hackers to log on and steal your identity, money or destroy your reputation.
3. Be obscure. Use a combination of letters, numbers, capital letters and special characters if possible. The more you do this, the more secure your passwords will become. Create an alphanumeric version of a term you can remember. Using this technique the word "Spaceship" becomes "Sp@ce5h!p".
4. Change regularly. This is the singular tip that can save you if you do not heed any of the other tips. How often should you change your password? How secure do you want to be? The frequency with which you change your password will determine how secure you are

from becoming a victim. The more often you change it, the better you are. The longer you leave it the same, the more vulnerable you become. Three months is a good cycle for a password, but certainly if you fear for the security of your identity, then a monthly change is not out of the question.

5. Password-protect your PC. Be sure to give your PC a password on power-up. This will help protect your files unrestricted access to your PC.

6. Password-protect your wireless home network. If you have a wireless home network, be sure to password protect it as well. Use the same principles above in order to secure your wireless network. This will prevent others from accessing your connection and using it maliciously to hack the personal or business PCs and laptops you and your family use at home. And do not use WEP – this is a very old standard that is very easy to hack. Use at a minimum a variant of WPA.

Finally, there are password programs that can help with this important task, but the best advice is to start with the tips above right away. Password software can be useful as an organizational tool, but it is no match for using sound methods to manage and make your passwords difficult to crack. One of our favorites is the open source (free) software package called "KeePass".

Timothy Gillen CNE | MCP

CEO & President
"Virtual" CTO

AskTim@terrapiIT.com