

## **PASSWORDS: THE WEAKEST LINK IN YOUR SECURITY CHAIN?**

by Dennis Kennedy ([dennisk@nettechinc.com](mailto:dennisk@nettechinc.com))

We find ourselves awash in the sea of passwords and pin numbers for ATM and credit cards, voice mail, network logins, Internet access and even some Web sites. What are the best ways to stay afloat?

An unwise selection of a password can compromise security of your computer system, your business and your personal life. A poor job of keeping a password secret can compromise the security provided by a well-chosen password.

Even worse, if you make an excellent selection of a password and do an excellent job of keeping it secret but then forget your password, you may find yourself in a hopeless situation.

Passwords pose two key issues: How do you select a good password and how do you manage passwords once you have chosen them?

### **Selecting a Password**

Many of the first computer hackers broke into computer systems by logging on with the user name of "guest" and then trying the password "guest". In many cases, believe it or not, "guest" was the actual password.

These days computer hackers take advantage of readily-available, highly-sophisticated "cracking" programs that try, in rapid succession, most of the common password strategies and variations thereon. These programs use every word in the dictionary and many foreign dictionaries, numerical combinations, and many variations on common password techniques. As computers become more powerful, a hacker can use increasingly sophisticated techniques to become even more successful at cracking your password.

Studies indicate that most passwords fall into several basic categories:

1. Common words like "password", "secret", and other similar words. In fact, one report indicated that at one time the word "password" was the most commonly used password in Germany.
2. Your first name, last name, initials, or a variation on your name or initials.
3. Your spouse's name, the name of a child, the name of a pet or variations thereon.
4. Common numbers based on birth dates, social security numbers, phone number, license plate number and the like.
5. Obscure words.

6. Mythological names, geographical names, common names, characters from TV shows or movies or sports figures.
7. Names of sports teams.
8. Names or words related to your profession or hobby.
9. Simple two word combinations.

Each of these techniques for selecting a password will result in a password that can be broken fairly easily by a cracking program or a sophisticated and persistent person who wants to break into your account and has some knowledge of you and your interests.

A true story: Several years ago, I needed to log on to my old firm's network and found that I was already logged in on my own computer. At the time, I was not allowed multiple logins for my user name and could not use another computer unless I went back to my office and logged myself off of my computer. Not wanting to do this, I went to the nearby office of an attorney who was on vacation and typed in that attorney's initials and spouse's name as a password. I logged right in as that user on my first try. It was that easy.

How do you choose a good password? Here are a few tips:

1. Avoid the common categories of passwords. In particular avoid any use of your name or any variation of your name, your user name, your spouse's name or your children's names.
2. Avoid the use of any word or words that can be found in a dictionary.
3. If you must use words, use nonsense words or intentionally misspelled words.
4. Avoid purely numerical passwords, especially ones based on easily obtainable personal information about yourself such as the license plate number.
5. If you use letters, make some uppercase and some lowercase.
6. A combination of words might be a good choice, but only if you separate them or divide them by using punctuation marks or symbols like "#" or "&".
7. A good password might be based on the first or last letters of the first eight words of a favorite poem, a favorite quote or a favorite provision of the Internal Revenue Code.
8. In many ways the ideal password is a random combination of letters, numbers and punctuation symbols with some uppercase letters and lowercase letters.

Based on the advice from experts, your ideal password would look something like "e#2!B5\$c". And, ideally, you would have a similar password for each of your account which requires a password. In addition, you would change this password once a month or so.

You should be beginning to see the problem. Creating excellent passwords is not nearly as difficult as remembering them.

### **Managing your Passwords.**

Password management takes two forms. First, you must be concerned about keeping your passwords secure. Second, you must have a way to maintain the passwords in a way that you can remember them. These two concerns are often in conflict.

For example, it is common advice that you should never write down a password. If you don't write down a password and you use an "ideal" password of eight randomly selected characters, you will have done an excellent job on security while all but guaranteeing that you will do a poor job of remembering the password.

Your approach to password management will involve your level of comfort and your compromise between security and ease of recall.

### **Security.**

Here are a few basic tips on password security.

1. Avoid writing down passwords and keeping them in a place where they can be readily found. Taping your passwords to the side of your computer monitor is not a smart idea no matter how convenient it may be. Neither is writing a password on a piece of paper kept in your desk drawer, your laptop computer's carrying case or a file folder marked "my passwords."
2. Don't tell anyone your password. If you must do so, change your password after that person is done using it.
3. Be careful when entering your password so that someone can't observe it easily. Avoid passwords based on easily-observable keyboard patterns such as "aaaaaaa" or "12345678".
4. Don't use the same password for all of your accounts. If someone figures out that password, they have the keys to your kingdom.
5. Don't give your password to anyone who asks for it, no matter how official sounding they may seem. A common scam is for someone to send you an official looking e-mail asking you to give them your password for security or maintenance reasons. Don't do it.

6. Change your passwords on a regular basis. Some organizations now require users to change passwords on a monthly basis.
7. If you have any concern that your password security has been compromised, change your password. Often the simple act of changing your password will deny the unauthorized user further access to your account or system.
8. Enforce these rules for every user on your network.

### **Remembering Passwords.**

Let's assume that you have created an ideal password, taken every security precaution, and then one day the password simply disappears from your mind. What do you do? Unfortunately, in some cases you are out of luck. In other cases, your network administrator or a computer consultant might be able to bail you out.

A better approach is to devise a system to help you remember passwords. You have a number of choices, but the two most common are mnemonic and software techniques. If you use a mnemonic technique, you will use a password selected in a way that will help you remember it. A good example is a password chosen by using the first letters of a phrase that you will remember. A second approach would be to create a phrase out of the password that you have chosen which will help you remember the password. For example, many people were taught the name "Roy G. Biv" to help them remember the colors of the rainbow (red, orange, yellow, green, blue, indigo and violet).

Software techniques would include a passworded or encrypted file or a password management program to store and protect your passwords. One example of a software program would be Whisper 32 (<http://www.ivory.org/whisper.html>). I'm also experimenting with a program for the PalmPilot called Mobile Account Manager (<http://www.mobilegeneration.com>). These types of programs allow you to store and manage your passwords and then to encrypt the file that contains them. As a result, all you will need to remember is the password to the password management program.

### **Looking to the Future.**

Fortunately, new methods are being developed to help reduce the threat of your password being hacked. For example, some networks have intruder alerts if multiple unsuccessful attempts are made to access an account. Other systems allow a user to make only a limited number of incorrect attempts before prohibiting access to anyone using that user name.

The word to remember in computer security, however, is "biometrics." In the future, we can expect to see security based on seemingly science fiction techniques such as retinal scans, fingerprinting, voice recognition, face recognition and even DNA-based systems. The key is the massive increase in power and speed of computer chips which will make such options possible. Until then, today might be a great day to change your passwords.