PASSWORD SECURITY

Here is an issue that many people like to ignore, password security. In the last month, we have had a couple of clients who have had an attack on their servers and we even had one ourselves. One of the easiest ways to hamper an attack is to have strong password protocols.

Another reason for this topic is that we have been looking into PCI compliance, since many of our customers accept credit cards and are going through a PCI review. What is PCI compliance? PCI Security Standards (www.pcisecuritystandards.org) are the rules that anyone that accepts credit cards must meet. These standards are strict and encompass not only the software, but your entire computer network. We are working to ensure that Lakeshore meets and exceeds the current standards.

How do the attacks happen?

There are several methods of attacking passwords. The two most common are a Dictionary Attack and a Brute Force attack. Both work to determine a user's access information, though in different ways. A Dictionary Attack, like it's name implies, continually sends words from a compiled word list that the hacker has built against your system. A Brute Force attack continually sends character combinations at your system until it finds one that works.

Another extremely common way that a person gets access to another's password is to find it written down on post-it notes stuck to the monitor or under the keyboard. With this in mind, it is a good idea to never write down your password.

How do you create a more secure password?

How many of you have a user name and password similar to the examples below?

	Ex.1	Ex.2	Ex.3
User Name:	john	john	ashley
Password:	john	smith	ashley123

All of the above are extremely weak security options. They are very prone to be cracked. According to Dave Whitelegg, UK based IT Security Expert, a 6 character password that is randomly generated, contains both lower and upper case letters, and also numbers can be cracked with a brute force attack in just over an hour on a basic home computer system using readily available password cracking software. A 7 character password with the same criteria took several days.

With this information in mind, you need to be able to come up with passwords that are going to be secure, but not too difficult for you to remember. Here are some

recommended guidelines gleaned from numerous sources.

1. Use a mix of upper and lower case letters and numbers, along with special characters such as: !, @, #, $, %, ^, &, *, <, >, ?, etc.
2. The longer your password, the longer it will take to crack. Current PCI requirements are 7 characters. Most sources recommend 8 or more characters.
3. Random characters are best. Do not use any variation of your name, birthday, address, phone number, child's or pet's name. Following this may make it difficult to remember the password, so consider using an interest or hobby that you like and the year you started working with it, for example:
    1. fishing&camping1970
    2. You can make it more secure by: FisHing19&70CamPing
    3. It can be even more secure by using some numbers to replace letters: F1sH1n619&70CamP1n6. Some people use the numbers that correspond with the letters on a telephone, others use the numbers as letters such as the number 1 for the letter I or L.
4. Change your password regularly. PCI compliance requires passwords to be changed at least every 90 days. Do not repeat old passwords.
5. Do not tell anyone your password.
6. Do not leave your password out where anyone else can find it. Always keep it secure under lock and key if you have to have a written copy. Post-it notes with the password stuck to the monitor or under the keyboard are not considered secure.
7. Do not have your web browser save passwords. Anyone who can access your computer will then have access to Lakeshore or any other site for which you have saved the passwords.

Why worry about having a secure password when it is a hassle to remember them? Well, if you accept credit cards, then you have to meet PCI compliance. Also, you do not want any of your data to be stolen and put your company at risk of lawsuits. Another hack that is very common now is to break into a computer and then use that computer as a base to send spam, porn, and other undesirable junk out to the masses.

According to several security experts, the biggest risk to a company is not the outside hackers, but the employees sitting at their desk. If strong password security is not used, then you may as well not use any passwords and hope for the best.