The IT Geek's
"Tip of the Week"

What's in a Strong Password?

Passwords are our first line of defense. In a manner of speaking, we are only as strong as our weakest password. Gaining unauthorized access to a computer on our network establishes a foot hold for the perpetrator to launch attacks against other (and perhaps more critical) systems.

You can help strengthen our defenses by using strong passwords. Microsoft defines strong passwords as those that contain at least three of the following four criteria.

- Uppercase letter (A-Z)
- Lowercase letter (a-z)
- Number (0-9)
- Special symbol (!, @, #, $, %, ^, &, *, (,), -, +, =, etc.)

Let's start by examining an example of a weak password. Even though it may seem strong and easy to remember, b4ucme2 is *not* a strong password because it only meets two of the four criteria (i.e., it only has lowercase letters and numbers). To qualify as a strong password, it would also need an uppercase letter and/or a special character.

b4Ucme2 qualifies as a strong password because it contains uppercase letters, lowercase letters and numbers (meeting three of the four criteria). An even stronger password would be something like I2spend$ (which meets all four of the criteria).

In addition, a password should be at least six characters in length. Some institutions require longer ones as a network policy. Of course, passwords should not contain any part of your name (even if it is spelled backwards).

We are going to implement a strong password policy on the network soon. Begin thinking now of other examples of strong passwords… and start using them! If someone can break into your computer by discovering a weak password, your information is at risk and your computer provides him/her with a foothold to attack the rest of our network.

We'd love to hear from you! Please send questions and comments to HelpDesk@csum.edu. Previous tips are online at: http://www.csum.edu/IT/tipoftheweek.asp