Topic 2: Good Password Sense

A good password is a strong, secure password. Passwords are constructed from at least three of the following characteristics and will be at least 8 characters long:

- **Numeric character** (1, 2, 3, 4, 5, 6, 7, 8, 9, 0)
- **Special character** (/, [ , , - , = , + , ! , # , $ , etc.)
- **Uppercase character** (A, B, C, D, E, F, G, etc.)

A good password is more than strong construction. A good password is a secure password; **one that is not shared with anyone**. When users share their passwords with others, they put all the information that is protected by that password at great risk. Sharing passwords can cause unwanted break-ins from unknown individuals and, sometimes, by known individuals. For example, an ex-boyfriend who decides to use your password to your e-mail account, pretending to be you and breaks up with your current boyfriend!

A **secure password is one that is not posted, written down, or shared**. Experienced hackers know to look for exposed passwords that are taped on monitors, hidden under keyboards, or even in a desk drawer.

The following methods are very useful when creating a new password:

- Choose a password that is easy to remember. Mnemonics provide the ability to associate meaningful data with a password. For example, "one fish two fish red fish blue fish" becomes ()F2f|Fbf. Books and movies provide great passwords, as do phrases such as "I-40 was slow as molasses this morning" which becomes I4()W$aMtM.
- Try to avoid converting letters to numbers, like changing "e" to 3 or "o" to 0. Instead use special characters that resemble the letter, such as changing "o" to (), and "r" to |2. **The password should not contain your username, or any part of your full name.**
- Do not base the password on personal information (spouse's name, favorite sports team, etc).

If you need to change your TU TigerWeb or MyTU email password, please visit Kenney Hall 70-214. Please bring your ID. You may call x8040 for direction to this location.