Password Protection

- The more you have to lose, the longer the password should be.

- Choose a password that is at least six characters long and that should cover you fairly
- well. Keep in mind that not every system will allow you to enter, say, a 12-character password.

- Mix upper- and lowercase characters and symbols like #$%"& to add an additional level of protection.

- To make your password easy to remember but tough to crack, use an acronym or pass phrase. For example, TA5WTLYL is easy to remember if you know that it stands for "There are 50 ways to leave your lover!" For even stronger security, create a pass phrase such as "ShepicksSHEllsbyTheCshore."

- Some people create passwords by picking out a pattern on the keyboard. Hackers know that many people like to use patterns like FRED and QWERTY, so you need to be particularly imaginative and try something like l=q]a'z/g (figure it out).

- Don't give out your password to anyone.

- You shouldn't write your password down, but if you do, don't put it on a Post-it and stick that on your monitor or tape it to your desk.

- Do change your password at least every 90 days. Change it immediately if you suspect that your password has been compromised.

- Don't key in your password while someone watches.

- Don't use the same password for all of the computer systems that you use, whether it's your ATM, commercial online account, desktop, or laptop computer.

- Don't allow an unlimited number of attempts to crack a password. There are password programs that shut someone out after three unsuccessful attempts to enter the correct password.