Password Security

The job of some people (hackers) is to attempt to find out, or crack, your computer password to access your files and data. Once they obtain your password, they can do malicious things to the information stored in your account. Even worse, they may be able to do harmful things to the accounts of other people on computer networks. So the argument—"I don't need a good password because I don't have any important information in my account—doesn't work. Passwords are usually the weakest security link within an organization's network.

To avoid falling prey to cybercriminals, create a secure password by making use of the techniques listed below:

- Don't use dictionary or foreign words, names, doubled names or first/last names and initials.
- Don't use simple transformations of words (7eleven, seven11, etc.) or any alphabet or keyboard sequence (backwards or forwards).
- Don't use your user ID in any form (as-is, reversed, capitalized, doubled, etc.).
- Don't reuse old passwords. Instead, choose a completely new password every time you change it.
- Don't even consider using short words (less than 8 characters), phone numbers, birth dates, social security numbers or numbers substituted for letters (like a zero instead of the letter O).
- Don't use the word 'password' (statistics have shown that up to 70% of all user passwords are the word 'password').
- Don't tape the password under the keyboard or anywhere else on the computer, the computer's desk or in an unlocked file cabinet. Mischievous people will look for your password in these places like a thief looks for a key under the front door mat.
- Do choose a phrase, and then use the first letters ('A stitch in time saves nine' would be 'asits9').
- Do use a password that has at least two alphabetic characters (a-z, A-Z) and at least one numeric (0-9) or special (punctuation) character. Always use a mixture of upper- and lowercase characters.
- Do use a password that is easy to remember, so you don't have to write it down.
- Do choose a password that you can type quickly. This guards against someone finding your password by watching you type it.
- Do change your password often—at least every three months.
- Do implement a password-protected screen saver in case you must leave your workstation without first logging off. When possible, log off or lock your workstation by using CTRL + ALT + DEL.

Remember, security and crime prevention are everyone's responsibility!

For more information, visit www.AUS.com/Tips