Choosing Strong Passwords (ISSP-005)

Introduction

Passwords are the first line of defense on any system connected to the network. It is not enough to simply have any password associated with an account. Passwords must be chosen in such ways that the casual hacker would not gain access to the account simply by trying a few easy combinations.

Picking Good Passwords

- It should contain characters from at least 3 of the four groups listed:
  - uppercase letter (A-Z),
  - lowercase letter (a-z),
  - digit (0-9),
  - punctuation character (such as ‘,’ ‘%’ or ‘-‘)
- It should NOT be simply a word or a name in ANY language – hackers use tools with online dictionaries in multiple languages, and names relevant to you or your family can be obtained from publicly available records.
- It should NOT contain any part of your name or login id
- The password should be MORE THAN 6 characters long. Keep in mind that some systems truncate passwords longer than 8 digits.
- It should be easy to remember, so you don't have to write it down.
- You should be able to type the password quickly, without having to look at the keyboard. This makes it harder for someone to steal your password by watching over your shoulder.
- Avoid using the same password for multiple locations. For instance, using 'passwordA' to access your banking information and using the same password to access a recipe web site.

How to do it

Ways to come up with a hard to guess (but easy to remember) password:

- Misspell a word.
- Take two short words, capitalize one or more letters and put them together with punctuation marks or numbers in between.
- Choose a line or two from a song or poem and use the first letter of each word.
- Create words that mimic easily remembered sounds.

Improving Security

- USF IT will NEVER ask for your password, on email or in person. Actually, never disclose your password to anyone.
- You are always responsible for your account. Don't share it with anyone.
- Change your password every 180 days. That way, if someone has guessed your password, they'll lose the ability to use your account.
- Don't write your password down. In particular, don't write it down on anything in your work area, and especially not online in a file. Keeping it in your wallet is acceptable, but don't show it to others.