Password Best Practices

What makes a password strong?

- **Length**: Each additional character in a password makes it stronger.
  - A *pass phrase* is one easy way to add length while still keeping a password *easy to remember*.
  - Several random words strung together or a phrase that is unique to yourself make for a good, long password.
- **Different Character Types**: Each time you use a character of a different type it makes your password stronger:
  - Lower Case Letters: a, b, c, d ...
  - Upper Case Letters: A, B, C, D ...
  - Numbers: 0, 1, 2, 3 ...
  - Special Characters: !, @, #, $ ...
- **Uniqueness**: Don't use the same password for multiple systems such as both SPU and your Facebook account.
  - By making your passwords unique, you prevent someone who has hacked one account from hacking all your accounts that use the same password.
- **Randomness**: The more random a password the less likely it is to be "guessed".
  - For example using, "1234567" or "1111111" as part of a password isn't very random.
  - By contrast, "8675309" has the same length and character types, but is a much harder part of a password to "crack".

Keep Passwords Safe

When it comes to protecting online information, good password techniques are cornerstone. A good password is both a function of password strength, and user practice.

- Don't write them down.
- Keep it secret, keep it safe. Don't share it with others.
- Don't use the same password for multiple accounts.

Organizations should never ask for your passwords. There is no "technical" reason to disclose them, so don't! Be *very* suspicious of anyone who asks.

Password Software

Many software products exist today that have proven helpful in managing all the accounts and passwords that are used on a daily basis. They do this by storing the unique credentials, while keeping that information secure and encrypted against unauthorized access. You get the benefit of stronger passwords on your accounts that you don't have to memorize. *As with any software, be sure to research it to ensure it is secure, reputable and has all the features you need.*

Here's one article that talks about several of the popular password managing programs available (LastPass, 1Password, KeePass, Dashlane & RoboForm).

Browsers

Be cautious when allowing browsers to save your credentials. You should only save passwords in your browser when you are the only one with access to the computer and user account that you are logged into. Never save passwords on a public terminal or on a computer with a shared login account.

Password Policies and Guidelines provides more guidance to create and maintain a strong password.