Guidelines for Strong Passwords

It is Information Technology Services (ITS) policy that passwords used to access computing systems at the University at Albany be strong. ITS strongly encourages the use of strong passwords for all other computing systems.

A strong password is one that is more secure by virtue of being difficult for a machine or a human to guess. Password strength can be achieved by incorporating the following characteristics; the more characteristics you incorporate into your password, the stronger it will be.

Characteristics of strong passwords

- At least 12 characters—the more characters, the better.
- For service accounts, we recommend 20 characters.
- A mixture of both uppercase and lowercase letters
- A mixture of letters and numbers
- Inclusion of at least one special character, e.g., ! @ # ? ]

Note: do not use < or > in your password, as both can cause problems in Web browsers

A strong password is hard to guess, but it should be easy for you to remember—a password that has to be written down is not strong, no matter how many of the above characteristics are employed.

While all systems that use the University NetID and password for authentication support a password with the above characteristics, please note that other systems may not support similarly strong passwords. For example, a system may not recognize case, may have a limit on the number of characters, or may not allow special characters. ITS recommends that in these situations users incorporate as many strong password characteristics as the system will allow.

Examples of weak passwords

- Any word that can be found in a dictionary, in any language (e.g., airplane or aeroplano).
- A dictionary word with some letters simply replaced by numbers (e.g., a1rplan3 or aer0plan0).
- A repeated character or a series of characters (e.g., AAAAA or 12345).
- A keyboard series of characters (e.g., qwerty or poiuy).
- Personal information (e.g., birthdays, names of pets or friends, Social Security number, addresses).
- Anything that's written down and stored somewhere near your computer.

Tips for keeping your password secure

- Change it regularly—once every three to six months.
- Change it if you have the slightest suspicion that the password has become known by a human or a machine.
- Never use it for other websites.
- Avoid typing it on computers that you do not trust; for example, in an Internet café.
- Never save it for a web form on a computer that you do not control or that is used by more than one person.
- Never tell it to anyone.
- Never write it down.

Tips for creating a strong password

Think of a word or phrase, and then substitute the letters with numbers and special characters and mix the case. For example:

- Snoopy and Woodstock becomes Sno0py&ws
- In the dog house becomes InTh3dawgHs
- Let’s have dinner at 8:00 p.m. becomes Lhd@800pm

Think of a word and a number, then intermix them and mix the case. For example, your elementary school name (Main Street Elementary) and your pet’s birth month and year (12/96) becomes m1A2/i9m6

Sourced from https://its.lafayette.edu/policies/strongpasswords/

Need more help? Contact the ITS Service Desk.