Password Creation Tips

Canisius College has some basic password requirements. Within these rules, you can create almost limitless combinations of characters that make quite strong passwords:

- At least eight characters long.
- A mixture of alphabetic letters and numbers. The first character must be alphabetic.
- At least one "special character," *after* the first character, but not the *first* character.
  - Allowed special characters are: ! % * + - / : ? and _
  - Disallowed special characters are: # @ $ & " ( ) , < > ` = ; and the space character.
- Cannot contain your name, or the words "password" or "canisius."

Remember, ITS will NEVER send a message with a link to click for password resets. Legitimate password reset email messages will simply give instructions referring you to the portal.

Professor James Moriarty, the evil criminal genius from Arthur Conan Doyle's Sherlock Holmes stories. He probably wants to get into your Canisius accounts, so he likes weak passwords.

OK, those are the rules. But how do I keep thinking up *strong* passwords?

Strong passwords get away from familiar combinations of letters and numbers, by cleverly employing characters in unfamiliar ways.

The *strongest* passwords:

- do not contain your name, your username, "Canisius," "College," your department, office, or unit name,
- do not include simple information about yourself, your job, or your life that could probably be found through web searches (ex. your building name or office number, children's or spouse's names, or date of birth),
- do not contain a complete word or words spelled out with letters only, like "SocketWrench," "OldShoes," "Ice_Cream," "Mikes*laptop," "Sallystablet," "myMacBook," or...(sigh)..."Password,"
- do not consist of simple keyboard patterns, such as QWERTY, or 45678,
- are significantly different from previous passwords,
- contain numbers symbols, uppercase *and* lowercase letters,
- and are longer than simply eight characters.

So, for example, "**SimpleCode-1**" meets the official requirements. But because it contains complete words, it is not as strong as it could be.

Choose words or phrases that have special meaning to you, so you're more likely to remember them. Then, re-spell them using symbols and numbers in place of similar letters.

5!mp!eC0de* is stronger, with letters replaced by numbers and symbols.

The more characters a password has, the more secure it is. Twelve characters is a good minimum.

A longer password may seem difficult to remember, but consider a verse, phrase, or sentence you can jumble with capitalization, numbers, and symbols, or make into an acronym. It's even better if you can include deliberate misspellings. Bear in mind that you cannot use the spacebar.

"**I love my greyhound!**" can be "**1Luvmy_Greyh0und!**"

"**What Hath God Wrought?**" can be (with two Vs for each W, and a zero for "o") "**VVha+ha+hG0DVVr0ugh+?**"

Another possibility is creating acronyms. So "**Your taun-taun will freeze before you reach the first marker!**" can be (with a +s replacing the first two "t"s, and two "v"s for W), "**Y++vvfbyrtFM!**"

In this way, simple phrases, verses, or sentences that have special meaning to you can become *formidable* passwords.

Once I create a good password for my Canisius login, what should I do to keep it secure?

Your Canisius password should be different from any of your other passwords.

The password you use to access your Canisius tools and services should be different than the passwords you use for your private (non-canisius.edu) email accounts, online banking tools, shopping sites, and anywhere else you go on the web. But for your non-Canisius internet activities, the above advice is equally valid!

> **Tip: Security Questions**
>
> Many websites, particularly banks and other places where you perform financial transactions, ask you to answer questions about yourself along with providing a username and password. These questions are straightforward: "What was the name of your elementary school?" or "In what city was your mother born?" For added security, you could supply answers that are nonsensical, but that you will remember. So in response to "What was the name of your of your elementary school?" you might enter "Long Division." For "In what city was your mother born?" you might enter "Mercy Hospital."

Do not share your password with anyone, or store them electronically.

Never share your Canisius password with anyone, whether they be work colleagues, fellow students, friends, or family. Canisius ITS will not ask you for your password in email or over the phone. Do not even hint at your password when explaining how you create them to others. (ex. "I use the make and model of my car, but I replace some letters with similar-looking numbers.")

If you must write your password(s) down, keep these on paper, somewhere very, very secure (such as a locked desk drawer). Do not write your password on desk blotters or post-it notes. Do not store passwords in word processing files, spreadsheets, or note-taking applications on your computer, tablet, or phone.

Do not let your browser (Internet Explorer, Firefox, Chrome, or Safari) remember passwords for you.

Reset your Password