Passwords

Version 8

Published 9/24/2021 by Jennifer Kim Last updated 2/27/2024 8:48 PM by Giuseppe Aloisi

---

Passwords are often the only defence a website or application has to prevent unauthorized people from reading your private data and impersonating you. Read this page for advice on protecting yourself with strong passwords.

Your Seneca password

You can create or change your Seneca password with MyID at myid.senecapolytechnic.ca. For help with your Seneca password please refer to the Seneca MyID Password Service help page or contact the Service Desk.

Your Seneca password allows you to access many services including the Student Home, email, and other computing services for students, faculty and staff. Systems that access your private information may require additional verification steps, such as personal security questions and a personal identification number (PIN).

General advice about passwords

How to self-create a strong password yourself

A good password is hard to guess but easy to remember.

Passwords that contain a word you'll find in the dictionary, or the name of a family member or celebrity, are very easy to guess. Complex passwords use a variety of characters such as upper case letters, lower case letters, numbers, and special characters (like !@#$).

Here's some advice on making a complex but memorable password. Think of a song you like, and think of your favorite line of lyrics. For example, let's pick It's Like That by Run DMC which says the line "*It's like that, and that's the way it is.*"

1. Let's take the first letter of each word: **iltattwii**
2. The uppercase letter L looks like the number 1 upside down so let's change that character: **i1tattwii**
3. The lowercase letter i looks like an exclamation point upside down so let's change

those characters at the end: **i1tattw!!**

4. Finally, let's change one letter to uppercase: **I1tattw!!**

Don't use this exact example; choose a song or phrase that's meaningful to you and make small changes that you can remember. Now you've got a strong password that's memorable for you but hard to guess for others.

Use different passwords for every website

You don't use the same key for your house, your car, and your business. If you did, and you lost your key, whoever found it could gain access to all your important possessions. Likewise, you shouldn't use the same password on every website.

You can customize your passwords per website, but make it easy on yourself. For example, password add "FB" to the end of your Facebook password, or add "tweet" to the end of your Twitter password. This makes your passwords unique but memorable. For example:

- I1tattw!!**FB**
- I1tattw!!**tweet**
- I1tattw!!**Seneca**

Password Manager

A password manager is an application meant to help you securely manage and store usernames and passwords. Typically, the application will store all your account usernames and passwords in an encrypted format and you have to use a master password to retrieve them. This means that you only have to remember 1 master password instead of multiple ones.

Here is a list of free and commercial password manager applications. Use your best judgment to select one that suits your needs, and please note that Seneca does not endorse any vendor nor provide support for any of the listed applications.

tags : it-security, password, passwords-management, strong-password