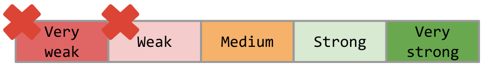
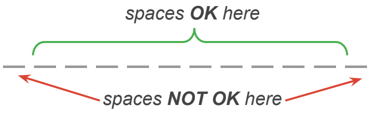
PLU ePass Password Requirements Quick Guide

Password Rules



STRENGTH
Must be Medium or higher when you interactively change your password.



SPACES
No spaces at beginning or end of password.
OK to use spaces anywhere else.

CHARACTERS
Use combinations of uppercase, lowercase, numbers, and symbols.
DO NOT USE these characters: `, ` : ( ) & \`

Reuse after 5 years

REUSE
Passwords cannot be reused within 5 years.

Create a Pass Phrase

Update your password at:
http://epass.plu.edu

May we suggest...

- Make your password **at least 16 characters** long.
- Use pass phrases that **combine random words.**

Example: 21 characters, with random words separated by spaces.

orange_eagle_key_shoe

Very strong, likely to take centuries to crack

REWARD FOR PASSWORD STRENGTH

The stronger your password, the longer you can keep it without it expiring. You'll get interactive feedback as you update your password.

Strategies for Increasing Password Strength

✓ Longer passwords are more secure because it takes hackers longer to crack them when employing a brute force method. Consider using a password phrase with **16 to 24 characters**.

✓ Increase the number of alternatives for each character by using a **mix of uppercase, lowercase, numbers,** and **symbols**.

✓ Computers are great at trying patterns to guess a password. **Avoid using**:

- your **ePass username**, **PLU ID**, **first & last name**, **email**, and **email alias**
- a single dictionary word
- keyboard spatial patterns like: **qwerty**, **asdf**, or **zxcvbn**
- repeating characters like: **aaaaaaa** or **1111111**
- sequences like: **abcdef**, **654321**, **years**, **dates**, or **zip codes**

GET HELP: helpdesk@plu.edu 253-535-7500