Creating Strong Passwords

Creating a secure password is an important part of protecting any account. A strong password can assist with:

- Keeping your personal information safe
- Protecting your emails, files, and other content
- Preventing someone from breaking into your account

Step 1: Meet/Exceed password requirements

Make your password with 8 characters or more. It can be any combination of letters, numbers, symbols, but it cannot be your name.

You can't use a password that:

- Is used by many other accounts
- You've used before on your account

Step 2: Suggested tips for a good password

A strong password is nearly impossible for someone else to guess. Follow these tips to learn what makes a good password, then apply them to your own.

Use letters, numbers & symbols

Combine different types of characters

Use a mix of alphanumeric characters (letters and numbers) and symbols:

Uppercase (capital) letters: B, U, Y
Lowercase (small) letters: b, u, y
Numbers: 1, 5, 9
Symbols and special characters: # @ & *

Recommendations & examples

You can replace letters with numbers & symbols: Choose a word or phrase and use numbers and symbols instead of some letters. Examples:

- "He who shall not be named" becomes "H3wh0sh@lln0tb3n@m3d"
- "Live long and prosper" becomes "l1Vel0ng@ndpr0sp3r"

Use long passwords: Long passwords are stronger. Since spaces are allowed, you can use memorable phrases or words from your favorite songs, poetry, or quotes. Example:

- "an 0pen <3 = an 0pen MIND"
- "There's a lady wh0's sure, All that glitters is g0ld"
- "Though this b3 madness, y3t there is method in't."

Avoid personal information & common words

Don't use personal information

Avoid using information that others might know about you or could easily find out. Examples:

- pet's name
- nickname
- street name

Don't use common words

Avoid simple words, phrases, and patterns that are easy to guess. Examples:

- Obvious words and phrases like "password", "letmein", “openseesame”
- Sequences like "abcde" or "12345"
- Keyboard patterns like "qwerty", "qazwsx", “Q!2w#e4”
- Any examples in this article

Don't reuse passwords

Use a different password for each of your accounts, like your work email or bank account.

Reusing passwords is dangerous. If an attacker figures out your password for one account, that person could sign in to your other accounts.

Step 3: Keep passwords secure

After you create a strong password, take steps to keep it safe.

Don't display your passwords

Avoid leaving notes with passwords on your computer or desk. People who walk by can easily steal this information and use it to sign in as you. Also don’t leave your computer unattended and unlocked, keep student data and personal information secure.