

Strong Password



- What is a Strong Password?
- Breaking down how a Strong Password is made
 - Length of password
 - Randomness (hard to guess)
 - Easy for you to remember
- How do I make a Strong Password with these qualities?
- Ok, I got it. So how do I update my Suffolk Password?
- Reminders
- Need Additional Assistance

What is a Strong Password?

Using a strong password is the first step in protecting your information. Strong password advice has been around the block more than a couple of times. Strong passwords really come down to 3 things:

- a. Length of password
- b. Randomness (hard to guess)
- c. Easy for you to remember

These qualities create password entropy, which is how unpredictable a password is and the difficulty for someone/computer to figure it out (crack).

Breaking down how a Strong Password is made

Length of password

Passwords should be as long as you can make them and still remember. The longer the better. Why? Simply put, adding length increases the computational difficulty to crack a password. Passwords should always be greater than 8 characters.

Randomness (hard to guess)

Password should be random and include at least one each of the following: uppercase, lowercase, symbol, and numeric. Why? The more random a password increases the computational difficulty to crack a password. Adding uppercase, lowercase, symbol, and numeric help ensure that a password is random.

Easy for you to remember

Passwords should be easy for you to remember so you can use it.

How do I make a Strong Password with these qualities?

One way to make a Strong Password with these qualities that is *Easy for you to remember* and very *Random (hard to guess)* is selecting an easy-to-remember piece of information such as a phrase, lyric, or favorite saying and change it into a strong password. Or put a few random words and numbers together.

For example, pick a phrase that is meaningful to you, such as *"I was born in a car on July 4 1901"* Using that phrase as your guide for a password, and include the (3) three qualities.

Good Example " iWbiacoJul4,01"

Why? Good because it is random (includes at least one each of uppercase, lowercase, symbol, and numeric), easy to remember and length is greater than 8.

Another example, Using a few random words, and include the (3) three qualities.

Good Example "CAT 50! staple PIG"

Why? Good because it is random (includes at least one each of uppercase, lowercase, symbol, and numeric), easy to remember and length is greater than 8.

Bad Example "iwbj4/1"

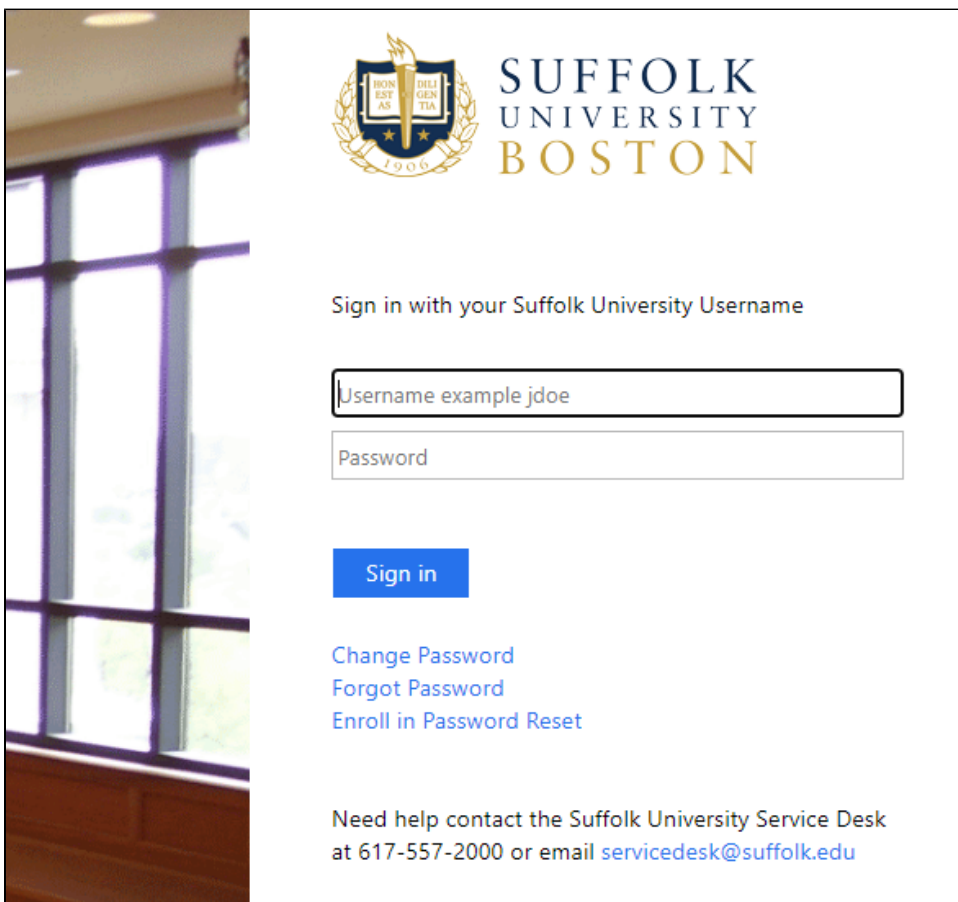
Why? Bad because, although it is very random and easy to remember, the length is too short. Password should never be less than 8 characters and the standard is moving towards 12 characters as computing power increases.

Bad Example "Tr0mBon3!"

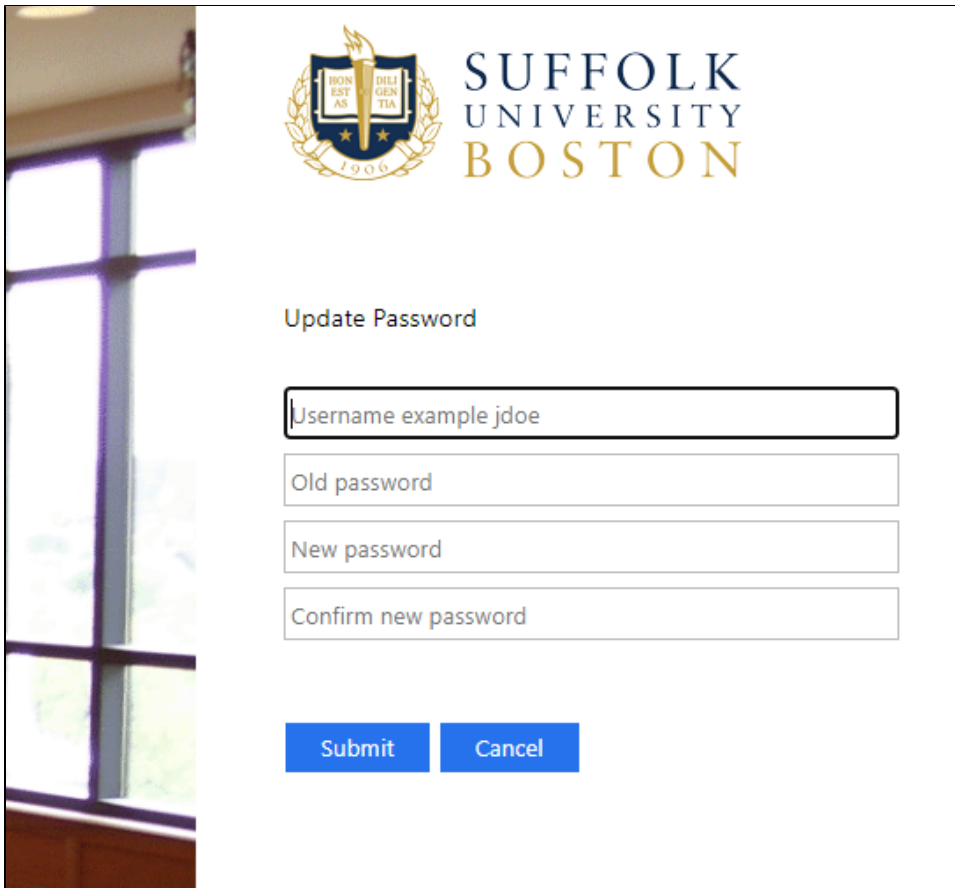
Why? Bad because, although it seems random and easy to remember, the common substitution of numbers and symbols for a single word is not difficult to crack. A password should never use common substitutions made from a single word. In this example swapping upper and lower case with the same letters (letter "T" for "t" and "B" for "b"), using a zero (0) for the letter "o" and the number three (3) for the letter "e" are common substitutions. Also, adding a symbol such as an exclamation mark (!) or numbers to the end of a common word does not increase the randomness.


Ok, I got it. So how do I update my Suffolk Password?

1. Go to Suffolk standard login page and click Change Password (image below)



2. On the Change Password Screen enter your network/email User name, Current old password, and your New Strong Password. Then click Submit. (image below)



 **SUFFOLK
UNIVERSITY
BOSTON**

Update Password

3. Your new password will be effective immediately. You will need to update all devices that use this password. This would include your University desktops, Suffolk WiFi access, and devices such as your smart device, tablets, laptops.

Reminders

- Never share your passwords with anyone
- Suffolk University, Information Technology Services (ITS) and ITS third-party service providers will NEVER ask for your account passwords
- If in doubt about a web link don't click, instead type it in the web address yourself and make sure it is a valid web address / URL that you are browsing to.

You should never circumvent password entry with auto login, application remembering, embedded scripts, or hard-coded passwords in client software, except for University email, which is password secured by the overlaying operating system on University User workstations or smart devices.

Computing devices must not be left unattended without enabling a password-protected screensaver or logging off of the device. Smart devices such as smartphones should be set to auto-lock and require a password or pin to unlock. Laptops and personal smart devices should always be under your control and should be secured when not being used.

If you suspect or have reason to know that the security of a password may be compromised, the password must be changed immediately. Under such circumstances, you should immediately report the discovery to the Suffolk University ITS Service Desk (617) 557-2000.

Need Additional Assistance

Please contact the Service Desk
Email us at
servicedesk@suffolk.edu

or call 617-557-2000
(2000 on campus)

For information about Walk-in Support, <https://www.suffolk.edu/about/directory/information-technology-services/support>

