



# How-To-Document Resource: *How to make a strong password/ passphrase*

## Making a strong password/passphrase

The number of characters has increased through the years due to the increased computing power to process and crack passwords faster. Some security experts will recommend at least 16 characters. In past years, I have recommended creating a password with a combination of uppercase letters, lowercase letters, numbers, and special characters. This tactic to create a strong password is still viable. Although, a longer password, regardless of character type, is better than a short, complex password.

Below are some examples of passwords.

An example of a weak password is **chris123**

An example of a medium password is **P@S\$w0rD**

An example of a strong password is **P@S\$w0rD=eSC1!**

An example of a strong password is **tcescCMHloginnow!**

Beyond creating a strong password, it is important to maintain a secure password as well. Compromised passwords that have been previously exposed from a data breach are commonly included in "dictionary attacks" and "credential stuffing" attacks on online accounts. If your account has been compromised in a company's data breach, malicious actors can attempt to compromise your account elsewhere with the hope that you are reusing your password with multiple online companies. To avoid this concern, create a unique password for each account and use MFA.

The following web link is to an online password tester: <https://www.security.org/how-secure-is-my-password/>. I don't recommend using your existing password in any of the online testers. Use a password tester to create and test passwords similar to a password you plan to use. Online password testers will allow you to see the strength levels among passwords and help form a strong password.

The following web link will check if a password has been compromised in a data breach. <https://haveibeenpwned.com/Passwords>

In the example below, the password checked is ***Password123.***

### Pwned Passwords

Pwned Passwords are hundreds of millions of real world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts. They're searchable online below as well as being downloadable for use in other online systems. Read more about how HIBP protects the privacy of searched passwords.

 

Oh no — pwned!

This password has been seen 46,167 times before

This password has previously appeared in a data breach and should never be used. If you've ever used it anywhere before, change it!