How to Create a Strong Password You Can Remember 2020

anetworks.com/how-to-create-a-strong-password-2020/

September 17, 2019

By Bill Minahan | September 17, 2019 |

How to Create a Strong Password in 6 Easy Steps

A strong password is one that is difficult to guess and easy to remember. Today it seems like the requirements for creating a strong password are becoming more and more demanding. But, there's a reason for it.

Hackers are becoming savvier and the increase in data breaches means your password is likely already on the internet somewhere. As a result, reusing a password (even if it's a strong one) can be dangerous. Therefore, all the passwords you create should be strong and unique.

It's easy to create a strong password that you can remember if you follow the right steps. First, we'll go over the characteristics that make a password strong. Then, we'll end with some methods to help you remember your passwords and keep them safe.

1. A long password is a strong password

The first way to make your password strong is to give it length. A long password is a strong password. A strong password must be at least 20 characters. If your password is 8 characters or less it can be cracked in 58 seconds.

2. A strong password has special symbols

A strong password should include unique symbols, numbers, lower-case letters, and upper-case letters for added strength. The inclusion of special symbols and numbers makes your password harder to guess because you create more possible combinations. If your password includes special symbols and unique characters, then you're less likely to be a victim of a brute force login attack. During a brute force attack, hackers try every possible combination of letters to guess your password and break into your account.

3. A strong password doesn't include obvious information

When looking at the above ways to create a strong password, it's easy to go for numbers, letters, or phrases that you identify with. However, if you're using your birthday, zip code, or address, hackers can easily trace them back to you on the internet. You shouldn't use personally-identifying information as a part of your password, however, that doesn't mean your numbers, letters, and phrases have to be random. Random passwords may be strong, but they're also difficult to remember.

4. A strong password is memorable and uses acronyms and codes

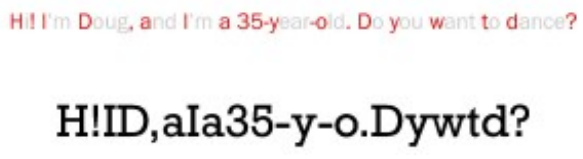
A strong password must be memorable or else it's no good. And no, writing all your passwords on a sticky note by your computer or on your phone doesn't count as remembering them. In fact, it just puts you in more danger. So how do you create a strong password that's easy to remember? Try using codes and acronyms that relate to specific things that you'll be able to memorize. They'll look like a random assortment of letters, numbers, and symbols, to everyone but you.

For example:

TGG_bFSF!HwBo9241896 [**T**he **G**reat **G**atsby_ **b**y **F**. **S**cott **F**itzgerald**! H**e **w**as **B**orn **o**n **9**/**24**/**1896**]

InTlItMbA_rn!4S-mny$ [**I n**eed **T**o **l**og **I**n **t**o **M**y **b**ank **A**ccount_**r**ight **n**ow**! 4 S**ome **– mny$**]

Find more examples of strong passwords here.



5. ## A secure password is backed up by multifactor authentication (MFA)

   Unfortunately, there is no such thing as a password that can't be hacked. Therefore, a second form of authentication is the best way to keep a strong password secure. However, MFA isn't bulletproof and shouldn't be used in place of a strong password. Instead, it should be seen as a way to protect a strong password. MFA is free, easy to set up, and adds an extra layer of security to your account. Learn more about multifactor authentication here.

6. ## Passwords should be stored in password managers

   Password managers are easy, free, and essential today. Password managers keep all your passwords in one place, which eliminates the need to remember 50 different passwords. However, you still need a strong, secure, and memorable password to log in to your password manager. With a password manager, you only have to remember one password, which means creating a strong password is even more essential. As a result, you need to make sure that one password is long, memorable, uses special symbols, and is backed by MFA. Luckily, most password managers offer strong password generation for you. All you need to do is click a button. If you want to get set up with a password manager learn more here.

Your password is your first level of protection against hackers. Therefore, you must learn ways to create a strong password and implement them.

80% of data breaches occur because of a weak or stolen password.

aNetworks offers secure password generation, multifactor authentication, and cyber security awareness training.

SET UP Multifactor Authentication today

If you want to figure out more about your online vulnerabilities, take our free cyber security assessment today.

Finally, if you found these 6 ways to create a strong password useful subscribe to our blog below.