How to Create a Strong Password You Can Actually Remember

2 Proven Methods for Creating Complex, Memorable Passwords

We all know we need to use strong passwords. Every news story about a data breach or stolen identity is a reminder of this need. But when you look at the most commonly used passwords, it becomes clear that too many of us in reality, we have a lackadaisical attitude towards the security of our passwords. So much so that the 20 most commonly used passwords not only contain highly unsecure passwords like the word “password”, they also account for a whopping 10.3% of all passwords that are being used. That’s an astonishingly high number, considering the near endless combination of possible passwords that can be built with just 4 characters containing upper & lower case letters, numbers, and symbols.

TOP 20 MOST COMMON PASSWORDS

(as a percentage of all passwords)

1.	123456	4.1%	11.	login	0.2%
2.	password	1.3%	12.	welcome	0.2%
3.	12345	0.8%	13.	loveme	0.2%
4.	1234	0.6%	14.	hottie	0.2%
5.	football	0.3%	15.	abc123	0.2%
6.	qwerty	0.3%	16.	121212	0.2%
7.	1234567890	0.3%	17.	123654789	0.2%
8.	1234567	0.3%	18.	flower	0.2%
9.	princess	0.3%	19.	passw0rd	0.2%
10.	solo	0.2%	20.	dragon	0.1%

Looking at the top 20 list of passwords makes one thing clear: even though computing power has continued to grow to the point that a machine with a GPU costing no more than a few thousand dollars can crack most passwords in minutes, you don't need a machine to readily guess most of the passwords listed above. People using any of the above passwords will probably continue to use them until one of their accounts have been compromised, but for the rest of us who are serious about proactively protecting our data, the good news is that there are nearly endless number of hard-to-crack passwords that can be used. The bad news is that most of these are very difficult to remember without some help.

What makes a password strong?

Password strength is directly related to how much computing power is required to crack the password. Security experts recommend that users create long, complex passwords to exponentially increase the time it takes to crack. Here are some concrete steps you can take to improve the security of your passwords:

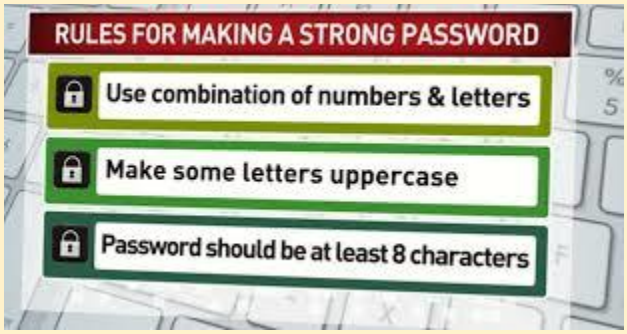
- **The longer the password, the better** – Experts recommend creating passwords that contain a minimum of 8 characters. If your password protects something sensitive, like access to your bank account, then use a minimum of 12 characters.
- **Use everything available on your keyboard** – Numbers, upper and lower case letters, and symbols all help to exponentially increase the strength of your password.
- **Throw away dictionary words** – You should never use common words or names within passwords. This rule can be extended one step further for those passwords protecting highly sensitive data to include compounds of multiple words. "IloveLabraDorReTrievers" is not a secure password if the information it's protecting is of high importance.
- **Avoid commonly used password patterns** – A 2013 study by DARPA, the Defense Department's research agency, found that about half of all passwords used at a Fortune 100 company followed five common patterns, 3 of which are listed below:
    - One uppercase, five lowercase and three digits (Example: Komand123)
    - One uppercase, six lowercase and two digits (Example: Komando12)
    - One uppercase, three lowercase and five digits (Example: Koma12345)
- **Use unique passwords** – Don't cycle through the same set of passwords or recycle one across different services because that

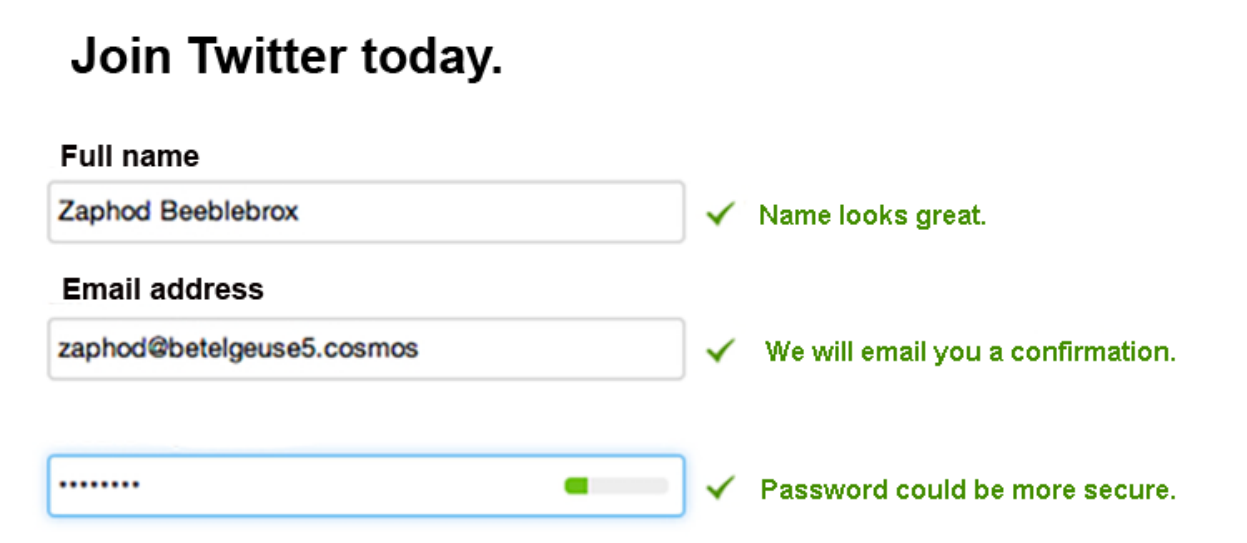
only diminishes the benefit of using a strong password. Research by Joseph Bonneau at the University of Cambridge shows that 31% of users reuse passwords in multiple places. When one of those reused passwords becomes compromised, the impact to the user is amplified.

- **Be careful where you store your passwords** – Do not store your passwords in spreadsheets or upload it to the cloud unless it's within an encrypted file. Data shows that the average company has 143 files on Microsoft's OneDrive that contain the word "password" in the file name. There are reputable platforms available you can use to create strong passwords and store them for safekeeping, such as LastPass.
- **Two-factor authentication is your friend** – This adds an additional layer of protection against hackers logging in with a stolen password. With two-factor authentication, the user must have her cell phone in order to verify her identity in addition to the username and password.

Making strong passwords memorable

The above rules are easy enough to follow. So why aren't more people following them? There are two primary reasons. First, far too many services simply don't require a particularly strong password. Sure, they show your password's strength, but more often than not, they will still allow you to save a weak password.





Second, remembering a truly random 12-character password that utilizes upper and lower case letters, numbers, and symbols and then trying to remember many such passwords is impossible unless you have a photographic memory. That's why far too many people settle for passwords that are weaker and easier to remember than they should. Fortunately, there are a few tricks that can help you create and remember some truly long, random, and highly secure passwords.

Method #1: Create your password from a sentence

People are much better at remembering sentences and song lyrics than they are remembering random letters, numbers, and symbols. One trick to creating a strong password is to take the first letter of every word in a long and memorable sentence and then add upper and lower case letters, numbers and a few symbols to produce your password.

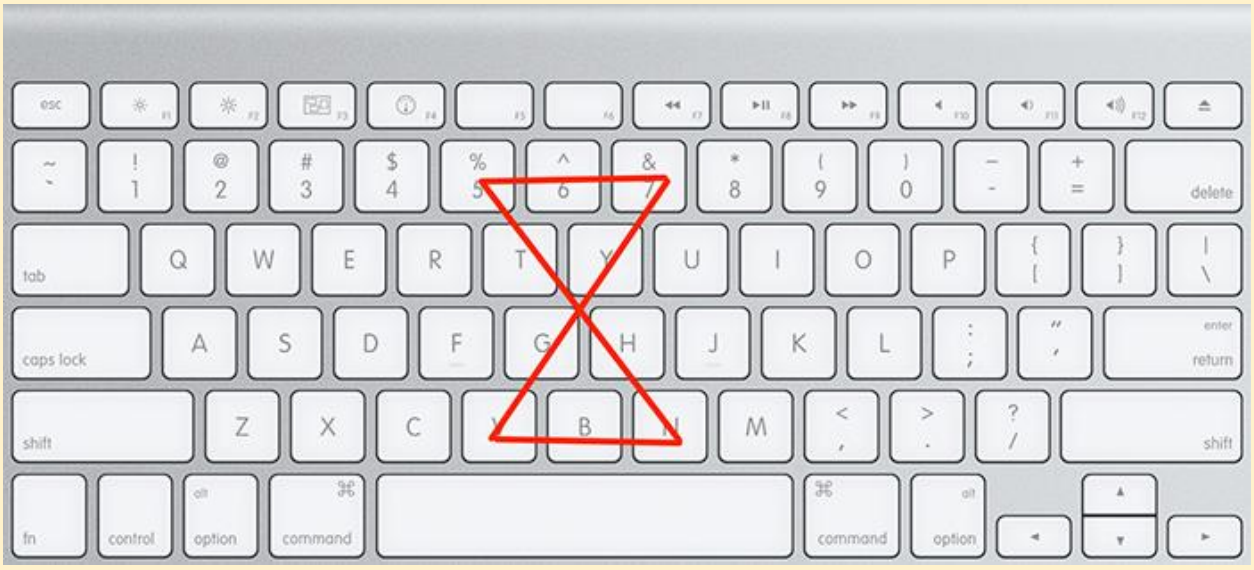
Are you a fan of the Beatles? Then try this: "Yesterday, all my troubles seemed so far away / Now it looks as though they're here to stay /

Oh, I believe in yesterday", which in password form converts to "Y,amtssfa/Nilatt'h2s/O,Ibiy". Simple enough, right?

Another good example of this trick is to use a personal statement such as "Don't forget, your wedding anniversary is on October 3rd!". The password then becomes "Df,ywaioO3rd!". There are endless ways to build highly secure and easy to remember passwords using this trick.

Method #2: Treat your keyboard like a constellation

Your keyboard is a blank canvas, ready to help you create your strongest password yet. Draw patterns meaningful to you across the keyboard, including letter and numbers (using your imagination, not permanent marker). The shapes could be your initials, your first name, or a geometrical shape like your favorite constellation to create your password of choice.



These two methods can generate random and secure passwords that are as easy to remember as your favorite song or constellation. In addition to strong passwords, experts also recommend turning on

multi-factor authentication. A wide variety of websites support multi-factor authentication today, including Dropbox, Gmail and most banking websites.

> While there's no fool-proof way to prevent hackers gaining access to your data or your identity, taking a few easy steps drastically reduces your risk.