

# Tips to Create Strong and Secure Passwords

Dilpreet Singh Bajwa



Password usage is part of our daily walk of life; we are using passwords daily to unlock our computer system or mobile phone. We use passwords for our email accounts, banking accounts, social networking sites accounts (like facebook), professional networking sites accounts (like linkedin) and other different logins on different sites for various purposes.

But you must be aware of the fact that passwords are the most vulnerable part in any security mechanism, if not properly chosen, created or dealt with. It can be guessed or cracked through various available techniques/tools and provides complete unauthorized access to attackers or hackers of all your confidential information. There are various tools available easily online for password cracking and it is almost matter of some seconds or minutes to crack a poorly configured password.

Here we are sharing some tips to create a strong and secure password. We are also discussing various points that you must keep in mind while dealing with the passwords. Hope the guidelines will be helpful and also helps you in creating a strong password.

## The points you must be keep in mind while dealing with passwords:

- Password must not be made up of any personal information like Date of Birth, Name, Phone number, Date of Marriage Anniversary, Car Number, Car Model, House No. etc.
- Password must not be made up of anything you like or dislike for e.g: Favorite movie/song, Favorite restaurant or place etc.
- Password must not be made up of any information related to your family members like Father's Name, Daughter/Son Name, DOB of any family member, phone number of any family member etc.
- Passwords must not be made up of any information you have shared online or on social media sites like Date of your Marriage Anniversary, Places you often visit, Date or month of your first salary or appointment etc.
- Avoid using any Dictionary word or different Dictionary word combinations for passwords.
- **Password must not rely on obvious substitutions for example "H0ney" is not a strong password just because you have place "0" instead of "o" in the password, That's just obvious for hackers or for password cracking tools.**
- Don't ever use easily guessable, default or common passwords like: "password", "admin", "password123", "12345", "qwerty", "iloveyou" etc.
- Don't use keyboard sequences (like-asdfg, qwerty etc.) or sequential numbers (987654321, 34567 etc.) in your passwords.
- Don't save your password in email or phone, share or not even write down your password anywhere.
- Don't use the password for long time, change it regularly.
- Always use different passwords for different logins.
- Don't Store passwords in your browser.

## How to create a strong and secure password:

- Length of password must be at least 12 characters or more.
- Password must be made up of Alphanumeric, lower case, upper case and special characters (Aa, Bb, Cc, Dd....Zz, 0,1,2....9, #, @,\$,: ...).

Some methods are given below to create strong and memorable passwords:

- Use a sentence to form a password by abbreviating and combine it in unique way. Here are some simple examples given for demonstration:

Sentence1: “Ohh! I am lazy, you are not obviously” = Password: “O!ImL,yoarNObsly”

Sentence2: “After reading “Dracula,” she became afraid of her own shadow” = Password: “ArDrac,shhbAfrdhroSh\_do2”

- Your sentence must be large enough to create a long password.
- It must be memorable.
- Do not use any sentence from online available text or other commonly available text like Bible verses or any other book.
- Always make your own sentence.

- Use a pass phrase to form a password by abbreviating and combine it in unique way. Here are some simple examples given for demonstration:

Pass Phrase1: “80 An Apple a Day, Keeps the Doctor Away 98” = Password: “0AAaD,KdD@way72”

Pass Phrase2: “To be or not to be, that is the question” Password: “2BorNot2B\_ThatIsThe?”

- Don't use already existing pass phrases.
- Your pass phrase must be large enough to create a long password.
- It must be memorable.
- Do not use any phrase from existing literature.
- Create your own pass phrase or show some creativity and modify the existing one.

- Use **Person-Action-Object Method** suggested by Carnegie Mellon University Computer scientists. The PAO method has advantages like it can be memorize easily as human brain remember and recognize image, action, shared cues and unusual scenarios better.

**The idea goes like this:**

Select an image of some Interesting Place (Like Andaman and Nicobar). Select a photo of a famous or familiar person (Like Sharukh Khan). Now imagine some random action (Like Driving) along with a random Object (Like BMW Bike). So at last the resultant sentence can be “**Shahrukh Khan driving a BMW bike at Andaman and Nicobar Islands**” and the corresponding password can be: “**SKd@BMWaAANI**”. Also add some special character and numbers to make it more perfect: “**SKd@#BMW#aAANI1928**”

Once you memorize and create several PAO tails, you can use these tails independently or in combination to generate passwords.

For example:

1. P-A-O= “Sharukh Khan”-“Driving” -“BMW Bike at Andaman and Nicobar Islands”

Sharukh Khan Driving a BMW Bike at Andaman and Nicobar Islands.

2. P-A-O= “Amitabh”-“Weeping”-“Films”

Amitabh Weeping in Films

3. P-A-O= “APJ Abdul Kalam” – “sails”- “Ship”

APJ Abdul Kalam Sails the Ship

Now combine them all to generate a new password. For example, you can take first four letters from 1<sup>st</sup> story’s first two words that is “Sharukh Khan” and “Driving” to create “ShahDriv”, Do the same for other two stories to make “AmitWeep” and “APJASail”. Now combine them all to make “**ShahDrivAmitWeepAPJASail**” 24 character password which is completely random and still familiar to you. Above are just examples, you can make them more complex and strong by including numbers and special characters.

- Use your computer keyboard to create passwords as a keyboard generates more than 90 different characters. So it provides numerous potential to craft new passwords. You can consider a keyboard as a canvas, where you have to draw some shape specifically an alphabet or number.

For example: “1qazdrfvgy7” is very hard to remember unless you know that it’s a character “W” on your keyboard as shown below in image:



Source: <https://www.webroot.com/us/en/resources/tips-articles/how-do-i-create-a-strong-password>

Similarly you can draw different letter, shaper or symbols in different way on keyboard by treating it as a canvas.

- Another option may be that you can use online random password generators but the problem with such passwords is that they are difficult to remember. Second there are also sites available which can calculate strength of your passwords and tell how much your password is strong but I personally not recommend these options for two reasons: first such random generated passwords are difficult to memorize, second who knows such sites at back end stores your password in any database and can be misused or if their own database get compromised due to some attack then there are chances that your password can also leak.

For similar such contents specially related to information security you may visit following link:  
<https://www.facebook.com/BajwaTechAcademy/>

-----x-----x---Happy Passwording---x-----x-----

.....