# SECURE PASSWORD RECOMMENDATIONS

Passwords provide the first line of defense against unauthorized access to your computer. The stronger your password, the more protected your computer will be from hackers and malicious software. You should make sure you have strong passwords for all accounts on your computer. If you're using a corporate network, your network administrator might require you to use a strong password.

Passwords are our virtual safeguards in the murky online waters, where hackers lurk like sharks. Passwords have a wide range of applications today. We require them for almost every online transaction, and more than ever because our online time spends have grown considerably. So, it is a must to have a strong password that can be remembered easily.

Hackers on the other hand have become smarter and are armed with latest tools. They spare no effort to breach passwords for stealing vital information. Statistics show that approximately 600,000 hackers logon to Facebook everyday with the intention stealing personal information.

When asking random people about passwords, they tend to agree that having a strong one is very important, but it is also very difficult to remember all of these passwords. As a consequence instead of trying to come up with a good solution, many people simply give up and use this as an excuse for having a weak password.

One problem is that many of us are not even sure what a strong password is. Many people think that a strong password is a complex string of random letters, numbers and special characters. However, when looking at it from a security perspective, rather than a cryptographic perspective, a strong password does not have to be completely random and, therefore, incredibly difficult to remember.

This exercise is intended to simply share some good tips and tricks for how individuals can stop using crappy passwords or using the same password on every single site where authentication is necessary.

## Why do we need a strong password?

Modern password cracking tools can check two billion passwords a second. A five-letter password has ten billion combinations, so it can be cracked in under five seconds, no matter what it is. A six-letter password is much better – it has 1 trillion combinations – but it can still be cracked in under ten minutes. A seven letter password can be cracked by a persistent intruder in about thirteen hours using easily available tools.

Eight letters is the absolute minimum required to be safe – it’ll take about 57 days to break it. If you’ve have ten or more letters in your password, that’s even better.

Longer passwords with 15 or more characters are difficult to crack. A hacker will require approximately a week’s time to crack a 10 character password, whereas it will take him 1.49 million years to crack a 15 character long password.

So, let’s take a look at how we can generate a strong password. First of all, I think that the most important detail to consider when creating a strong password is to make it personal. Most of us would agree that trying to remember a computer-generated password with random letters, numbers and special characters is difficult. But, if it’s a phrase that is personal to you, it will probably be much easier to recall.

### What makes a password strong (or weak)?

A strong password:

- Is at least eight characters long.
- Does not contain your user name, real name, or company name.
- Does not contain a complete word.
- Is significantly different from previous passwords.
- Contains characters from each of the following four categories:

| **Character category** | **Examples** |
|---|---|
| Uppercase letters | A, B, C |
| Lowercase letters | a, b, c |
| Numbers | 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 |
| Symbols found on the keyboard (all keyboard characters not defined as letters or numerals) and spaces | ` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ \| : ; " ' < > , . ? / |

A password might meet all the criteria above and still be a weak password. For example, **Hello2U!** meets all the criteria for a strong password listed above, but is still weak because it contains a complete word. **H3ll0 2 U!** is a stronger alternative because it replaces some of the letters in the complete word with numbers and also includes spaces.

## *Some tips on how to create and remember strong passwords*

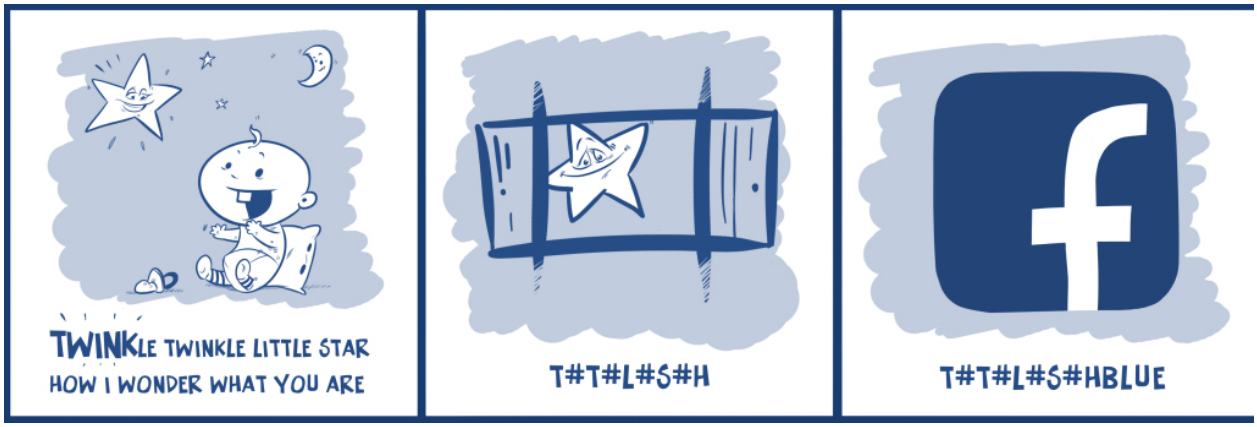
### The Story Algorithm

There are tons of different methods for generating passwords, one of which is often referred to as the “Story Algorithm”. There are many variants in this process, so feel free to come up with your own version that you believe will most help you.

1. Think of a phrase, song lyrics, quotes from a movie or simply a lullaby from when you were a child.
2. Take the first letter from the first five words.
3. Between every letter add a special character.

At this stage you will have created a static string, and from now on you will base all of your unique passwords off of this string. Since it's a static sting, it won't be unique for every site that you need a password for. What you need to do now is use the power of association.

When you think of Facebook, Twitter, eBay, dating sites, online gaming sites or any other site, write down the first word that you associate with that site that you need a password for. For example, if you are creating a password for Facebook, you might associate Facebook with the blue colour in the logo: so, then you can simply append the word "blue," maybe in all caps, at the end of your static string.




For example, let's play with the idea that the phrase I think of is "Twinkle Twinkle Little Star How I Wonder What You Are," and the special character that I want to use is the pound character, '#'. Then my password for Facebook would be something like: **T#T#L#S#Hblue**. It makes no real sense when you look at it, or if someone gave it to you. But, since it's personal, you understand the system used to generate your passwords and you associate the word with the site, it's easy for you to remember. Not to mention, it is quite strong.

There is one password that you should be extra careful about; it may even be good to use a completely different phrase when generating this password. This is the password to your email account. If someone can access your email, they can use the "forgot login" function to not only get access to your email, but also change the passwords for every site you have access to that's connected to that email address.

## Create an acronym from an easy-to-remember piece of information.

1. For example, pick a phrase that is meaningful to you, such as My son's birthday is 12 December, 2004. Using that phrase as your guide, you might use Msbi12/Dec,4 for your password.
2. Substitute numbers, symbols, and misspellings for letters or words in an easy-to-remember phrase. For example, My son's birthday is 12 December, 2004 could become Mi$un's Brthd8iz 12124 (it's OK to use spaces in your password).
3. Relate your password to a favorite hobby or sport. For example, I love to play badminton could become ILuv2PlayB@dm1nt()n.

## Create an acronym from an easy-to-remember piece of information.

Use the words of a song or a line of prose that you can remember easily.

To give an example of a mnemonic phrase password, consider a line from “Hamlet”, by William Shakespeare ***“Alas, poor Yorick! I knew him, Horatio***; would be converted into a password “**A,pY!Ikh,H**”. This password would take at least 200 or more years to crack. These kinds of passwords also provide reasonable resistance from brute force attacks.

Maybe you like the Men At Work song Down Under. You might use the line “**I come from a land down under**” as the base for your password. By applying some basic principles you might finish with something like “**!cf@Ld#U**”

As another example take the phrase “Easy to remember for you and complicated”. This could convert in to a reasonably strong password **“Ez2Rembr4U+compl!8ed”**.

**If you feel you must write down your password in order to remember it, make sure you don't label it as your password, and keep it in a safe place.**

## Three golden rules for passwords

### Rule #1: keep your password private

This sounds obvious, but most breaches of computer security aren’t due to thieves or hackers. They’re most frequently carried out by friends, colleagues, or family who are abusing the trust put in them. Ex-spouses and former employees may have access to all sorts of accounts, particularly if they’re online services like Google or your bank.

Avoid giving your password to *anyone* if at all possible – not even people you trust. If you do have to give your password out – for example if you’re out of the office and a colleague needs access to something – then change it as soon as possible afterwards.

### Rule #2: don’t make it easy for a human to guess

As suggested above, most security breaches are committed by people you know, and they can use that knowledge to figure out what you might have used. Avoid using personal information such as:

- your own name
- your initials
- your nickname
- your business name
- your login
- your star sign
- your date or place of birth
- your pet’s name, child’s name, spouse’s name, or maiden name

- your favorite place, band, movie, or fictional character
- your phone number, social security number or address
- the name of the site or service (when LinkedIn's password list was stolen in 2012, analysts discovered that the most common password was linkedin!)
- your catchphrase

#### Rule #3: the longer, the better

Modern password cracking tools can check two billion passwords a second. A five-letter password has ten billion combinations, so it can be cracked in under five seconds, no matter what it is. A six-letter password is much better – it has 1 trillion combinations – but it can still be cracked in under ten minutes. A seven letter password can be cracked by a persistent intruder in about thirteen hours using easily available tools.

Eight letters is the absolute minimum required to be safe – it'll take about 57 days to break it. If you've have ten or more letters in your password, that's even better.

A password which contains a mix of upper case, lower case, numbers and special characters could take at least 2 years for a hacker to crack, even if it is as short as 9 characters. To give an example of such a password ***"36tADP@!e"***, translated in English it would read 36 Tadpole. But look at the complexity achieved by including special characters and upper and lower case letters. Here 36 would signify the age of a person, making it easy to remember.

## Learn something from the Sarah Palin email hack case

US vice presidential candidate, Sarah Palin's yahoo mail account was hacked in 2008, using the yahoo password recovery system. I guess we should all learn something from the mistakes Sarah Palin made while choosing her password recovery questions. Her account was hacked easily as she had used password recovery questions, answers to which were easy to find online, considering the fact that she is a public figure.

The questions which the hacker encountered were simple and their answers were available on Wikipedia. The hacker did not require any technical expertise in answering questions like her Birthday, her zip code (she comes from Wasilla, which has just 2 zip codes) and last and the relatively difficult one, which was "Where she met her spouse". The hacker probably managed to guess the answer "Wasilla high" within a few minutes.

So choose difficult and unique password recovery questions which are difficult to find anywhere or difficult to guess.

- Never ever share or disclose your password to even close friends or associates.
- Never share passwords over emails.
- Never write password on pieces of paper randomly and leave them lying around.


WORST
PASSWORDS OF 2014
1 123456
2 password
3 12345
4 12345678
5 qwerty
6 123456789
7 1234
8 baseball
9 dragon
10 football
splashdata