

Protect Your Applications with a Strong Password

At Ultra.cc, the security of our users is our top most priority, and we take every precaution to make sure your data is protected. However, the level of our security does not matter if you use a weak password to protect your applications. In this guide, we will show you how to properly create a strong password, and better protect your applications.

How to Create a Strong Password

Length	Numbers only	Lowercase letters only	Mixed case letters	Numbers and mixed case	And symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 second	5 secs
7	Instantly	Instantly	25 seconds	1 minute	6 mins
8	Instantly	5 seconds	22 minutes	1 hour	8 hours
9	Instantly	2 minutes	19 hours	3 days	3 weeks
10	Instantly	58 minutes	1 month	7 months	5 years
11	2 seconds	1 day	5 years	41 years	400 years
12	25 seconds	3 weeks	300 years	2k years	34k years
13	4 minutes	1 year	16k years	100k years	2m years
14	41 minutes	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100tn years	7qd years

One of the most important aspects of creating a strong password is the length of the password. Even though complexity is needed to a certain degree, the length is the deciding factor of how strong a password is. As you can see from the above image, the time it will take to [brute-force crack](#) a password exponentially grows as the length increases.

Below you will find some guidelines for how to create a strong password:

- A password should be 12 characters or more; complexity is needed to a certain degree, but the length of a password is very important.
- A password should include a combination of letters (upper and lower-case), numbers, and symbols.
- A password should never be re-used on other sites or shared with other applications. For example, do not use the same password for SSH and your Radarr, Sonarr, etc.
- A password should not include personal information like username or anything else that can be easily discovered.
- A password should not include your username, email address, application or server name.
- A password should not include any personal information that could be extracted from your social media, e.g. your kids names, pets names, school college names, addresses, etc.

- A password should not have common words, keyboard patterns, and phrases such as `password`, `1234`, `abcd`, `qwerty` etc.
- A password should never be slightly changed for continued use.
- A password should never use a word backwards, such as `321drowssap`. Reversing a word does not improve the security of a password.

By following the above guidelines, you will be able to create a strong password and properly secure your applications.

Below you will find some general suggestions on how you can further secure your presence online.

- Use a password manager:
 - [Bitwarden](#) is an open source password manager that can be self-hosted.
 - [Keepass](#) is a light-weight password manager that is free and open source.
 - [Lesspass](#) is a stateless password manager that is free and open source.
- Use SSH keys - Connect to your Ultra.cc service with an [SSH key](#).
- Adopt the [Diceware passphrase](#) method - Create memorable passphrases instead of hard to remember passwords.
- Passwords should never be shared with another person or saved on a shared device where others might have access.
- Do not store your passwords in a non-secure location, such as post-its, plain-text document, in-built browser password managers, etc.

Revision #9

Created 21 August 2023 07:51:24 by varg

Updated 28 August 2023 09:52:31 by varg