# HOW TO SECURELY MANAGE PASSWORDS

# USE A PASSWORD (MANAGER/GENERATOR

Most people can't remember more than a few passwords. And most people need more than one. So: Remember a master Passphrase and generate/save all others.

### USE AT LEAST 12 CHARS

 Right now the threshold for a relatively safe password is around 8+. To be future proof aim for at least 12! The more random and longer the better.

### DIFFERENT PASS V WORD EACH SERVICE

Using a different password for each service increases your security. One account hacked -> all others still safe!

# MAKE SURE THE SITE USES TLS/SSL

Transport Encryption is a must!

Make sure the page you want to login/register uses that!

# DIFFERENT CHARS (1&) OR LONG PASSPHRASES

Get entropy through length and/or complexity by random special chars, space uppercase/lowercase usage. This includes not using easy to guess words or successive numbers as password (i.e. from password top10)

### DO NOT SHARE YOUR PASSWORDS

The less people know a password the safer!

# USE TWO FACTOR AUTHENTICATION

If the service provides a 2FA/mFA, use it! • Can be via email, SMS, FIDO or App.



### USE LONG MASTERPASSPHRASE

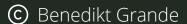
The Masterpassphrase you use i.e. for a Password Manager should be especially save.

Make it long and as random as possible!

## NEVER SAVE AS

Do not store the password as plaintext anywhere.
Not on paper and definitely not on your computer!
Use an encrypted vault or Password Manager.





📝 @benediktgrande

https://bgrande.de

More details at and based on my blog article <a href="https://bit.ly/3rweZpQ">https://bit.ly/3rweZpQ</a> (German) Source: <a href="https://bit.ly/3xPQh4W">https://bit.ly/3xPQh4W</a>

Infographic based on canva template <a href="https://bit.ly/3lsMPs4">https://bit.ly/3lsMPs4</a>