[for Users]

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

12+

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 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 OR LONG PASSPHRASES

a _!
1&

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

2FA

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 PLAINTEXT

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

© Benedikt Grande
@benediktgrande
https://bgrande.de

More details at and based on my blog article
https://bit.ly/3rweZpQ (German)
Source: https://bit.ly/3xPQh4W

Infographic based on canva template
https://bit.ly/3lsMPs4