

How do I create a secure password?

6 rules for a secure password:

- Use at least 10 characters
- Use numbers, upper- and lowercase letters plus special characters
- Don't use any key sequences, such as «asdfgh» or «45678»
- Don't use any words from a known language, i. e. the password shouldn't make any sense.
- Don't use the same password for all your applications
- Please do not save your password anywhere unless it is encrypted

One example of how to create a secure password:

- **Take a sentence which is easy for you to remember, and create your password from the respective first letters and numbers:**
«My daughter Tamara was born on January 19!»
- **This results in a password consisting of random characters which is easily remembered:**
«MdTwboJ19!»



Passwords

Passwords are still the most common and widely used keys in an electronic environment, protecting access to sensitive and private data. Just observing a few simple rules on how to handle passwords provides you with much improved protection.

You should for instance create a random password from the first letters of a sentence which is meaningful to you, and is therefore easily remembered.

Test your password

Under «<https://review.datenschutz.ch/passwortcheck/check.php>» you can check how secure your password is! Please remember not to test your actual password though, but only an equivalent.

Further information: www.ebas.ch/securepassword

«eBanking – but secure!» is offering helpful security hints for e-banking users

eBanking but secure!

You will find further practical information on measures and approaches required to ensure that e-banking applications are used securely under www.ebankingbutsecure.ch. The use of this website is free.



Hochschule Luzern – Informatik
Campus Zug-Rotkreuz, Suurstoffi 41b
CH-6343 Rotkreuz