4 – Protecting online access

Do you lock your door when you leave your home? You should also protect your devices and online access against access by strangers the same way.

The most important points to remember:

- Protect your computer and mobile devices (smartphones, tablets, etc.) against unauthorised access, and lock your screen if you are not actively using your device.
- Use secure passwords (at least 12 characters long, consisting of numbers, both upper and lower case letters and also special characters).
- Don't always use the same password everywhere, but create different passwords for different options.
- If possible, also activate so-called two-factor authentification.

4 – Protecting online access

5 steps for your digital security

No car theft with keys!
No data theft with **passwords**!

eBanking but secure! www.ebas.ch

Securing devices against unauthorised access

Protect all your devices via access protection. With notebooks, tablets and smartphones in particular, the risk of loss or theft is considerably greater than with your home PC.

Especially on your mobile devices, you should therefore ensure that the automatic screen lock via code, password, fingerprint or face recognition is activated.

In addition, you should encrypt your data on any mobile device. This particularly applies to auxiliary storage media, such as external hard drives or USB sticks. This makes it impossible for unauthorised persons to access your data and apps via external systems.

iPhone/iPad

Access lock up to iPhone 9: Under **Settings/Touch ID & Code**, you can protect your device via a number code or password and can also deposit your fingerprints.

Access lock from iPhone 10 onwards: Under **Settings/Face ID & Code**, you can configure your device for face

recognition.

With iPhones and iPads, data are automatically encrypted.

Android

Depending on your device, you can activate the access lock under **Settings/Security and Privacy**.

You can activate encryption under **Settings/Security and Privacy/More security and privacy/Encryption and credentials** – for add-on memory, too, if required.

Secure 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.

6 rules for a secure password...

- Use at least 12 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 word in a known language – i.e. your password should not make any sense and should not be found in any dictionary
- Use a different password for all your applications
- Please do not save your password anywhere unless it is encrypted

It is not really that difficult to create a secure password! Below we have explained how to create and subsequently also remember a secure password in a simple manner:

- Take a sentence which is easy for you to remember, and create your password from the respective first letters and numbers:
  «**M**y **d**aughter **T**amara **M**eier **w**as **b**orn **o**n **J**anuary **19!**»

- This results in a password consisting of random characters which is easily remembered:
  «**MdTMwboJ19!**»

Password manager

A password manager serves to save all your passwords in encrypted form - so you only ever have to remember a single password.

Windows

We recommend the following password managers for use with Windows, some of which are free:

- KeePass (https://www.keepass.info)
- Password Safe (https://www.passwordsafe.de)
- SecureSafe (https://www.securesafe.com)
- eWallet (https://www.iliumsoft.com)

macOS

We recommend the following password managers for use with Mac, some of which are free:

- KeePassXC (https://keepassxc.org)
- SecureSafe (https://www.securesafe.com)
- eWallet (https://www.iliumsoft.com)

Smartphone und Tablet

We recommend the following password managers for use with smartphones and tablets, some of which are free:

- KeePass (https://www.keepass.info)
- Password Safe (https://www.passwordsafe.de)
- SecureSafe (https://www.securesafe.com)
- eWallet (https://www.iliumsoft.com)

https://www.ebas.ch/wp-content/uploads/2023/04/SKP_NCSC_Passwortmanager_de.mp4

Further information and a detailed comparison of common password managers can be found in the "Fact Sheet Password Manager" (https://docs.datenschutz.ch/u/d/publikationen/factsheets-engl/factsheet_password_managers.pdf) of the Zurich canton data protection officer.

Two-factor authentification

In addition to a secure password, so-called two-factor authentification provides additional security. In the process, a second, independent security component is requested in addition to the first one (generally a password). This might be a code sent to your mobile phone or generated directly on your device.

https://www.ebas.ch/wp-content/uploads/2023/04/SKP_NCSC_2FA_de.mp4

Nowadays, it is not just financial institutions, but also many online service providers (such as Google, Facebook) who offer two-factor authentification. You should avail yourself of this increased level of security. A description of all the different methods used by financial institutions can be found here (https://www.ebas.ch/category/23) .

Was my online access hacked?

Check whether your password for any of your online accounts has been hacked:

Have I been Pwned (https://www.ebas.ch/en/have-i-been-pwned/)

Here you can find out whether your log-in details for any online accounts have been compromised or were published due to a data breach. This page uses the familiar https://haveibeenpwned.com (https://haveibeenpwned.com) platform to check its database and then prepares your results in German, French, Italian or English for you. To do so, enter your respective user name or e-mail address, but never the password to be checked!

Protect your data and all your devices with the help of our "5 steps for your digital security":

Step 1 – Back up (https://www.ebas.ch/en/1-backing-up-data/)

Step 2 – Monitor (https://www.ebas.ch/en/2-monitoring-with-antivirus-software-and-firewall/)

Step 3 – Prevent (https://www.ebas.ch/en/3-preventing-with-software-updates/)

Step 4 – Protect

Step 5 – Exercise Care (https://www.ebas.ch/en/5-exercising-care-and-remaining-alert/)