5 steps for your digital security

Your police and Swiss Crime Prevention (SCP) – an intercantonal office of the Conference of Cantonal Ministers of Justice and Police (CCMJP)

5 steps for your digital security

The internet has become an important part of our everyday life: It is on the internet that we read the latest news, consult timetables, pay bills or simply communicate with friends and family.

As well as all these possibilities, however, the internet has also brought new risks. Countless threats are continuously trying to find new ways of compromising our computers, smartphones or tablets, where our personal data such as photos, letters or important documents are stored. If an attack is successful, criminals can cause a great deal of damage to your devices and you personally. Data can be changed, deleted or the information contained within abused, for instance to shop on the internet in your name and at your expense.

You should therefore protect your data and devices with our "5 steps for your digital security":

Step 1 **Back** up your data

Step 2 **Monitor** your devices with antivirus software and a firewall

Step 3 **Prevent** incidents with software updates

Step 4 **Protect** online access

Step 5 **Exercise** care and remain alert

Saved in a crash by your belt!
Saved from data loss by your back-up!

1

Back up your data

How much do you value your data? You should regularly back it up onto at least one second medium, and always check that your data is actually been backed up, too.

Important points to remember:

- Regularly back up your data to an external hard drive, DVD, CD or online to cloud storage.
- Check all your data is included in your back-up and that it can be restored properly.
- You should only connect your external back-up hard drive when you are actually using it. Don't keep your online back-up storage device permanently linked either, but only when you are running a back-up.

These days, large amounts of text documents, emails, photos, videos, music and more are stored on computers, tablets and smartphones in the form of digital data. You cannot completely rule out that this data will be partly or even wholly destroyed or deleted by some kind of misuse (e.g. accidental deletion); due to technical faults (e.g. a defective hard drive); because a device is lost or stolen; or due to malware (viruses, worms, Trojans etc.).

→ Secure your data by backing it up before you suffer data loss!

Further information including detailed instructions and tools can be found here:
www.ebas.ch/step1

The cockpit allows you to have everything under control!
Antivirus software and a firewall allow you to monitor data traffic!

2

Monitor your devices with antivirus software and a firewall

What kinds of "access doors" are open on your device, and which kind of viruses can pass through? Practically none, as long as you have activated a firewall and installed antivirus software.

Important points to remember:

- Use antivirus software and activate its automatic update function.
- You should periodically check your device for virus infections by running a complete system check.
- Activate the firewall that comes with your Windows or macOS before you connect your device to the internet or another network.

Without these specific measures, your computer, tablet or smartphone are entirely at the mercy of threats from the internet and may possibly become infected with malware in no time at all. In that case, any of your stored data can then be viewed, manipulated or even deleted by unauthorised third parties.

→ **Monitor your internet communications with an antivirus software and an activated firewall!**

Further information including detailed instructions and tools can be found here:
www.ebas.ch/step2

Regular services keep your car in top condition!
Updates keep all your programs up to scratch!

3

Prevent incidents with software updates

Who better to look after your programs' security than their manufacturers? Maintain your system, software and apps, and make sure to regularly run the latest updates.

Important points to remember:

- Only ever install software and apps you actually need, and make sure to download these exclusively from the manufacturer's page or an official store.
- Activate the automatic update feature not just for your operating system, but also all programs and apps installed.
- Only ever use the latest browser version to surf the internet.

Outdated software often suffers from vulnerabilities, making it easy for attackers to take control of a device. Software manufacturers will correct any such vulnerabilities and offer patches in the shape of program updates.

Only ever install software and apps you actually need

Only install software and apps you actually need, and ensure that they originate from reputable sources, i.e. directly from manufacturers or an official store (e.g. Apple App Store or Google Play Store).

Keep your devices up-to-date

Ensure that you always use the most up-to-date version of any software. The mainstay is an up-to-date operating system. However, all other software installed (such as browsers like Firefox or Chrome, or Adobe Acrobat Reader) must always be kept up-to-date, too.

→ Prevent incidents by always installing all latest software updates!

Further information including detailed instructions and tools can be found here:
www.ebas.ch/step2

A key protects against car theft!
A password protects against data theft!

4

Protect 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.

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 10 characters long, consisting of numbers, both uppercase and lowercase letters and also special characters).
- Don't always use the same password everywhere but create different passwords for different applications.
- If possible, also activate so-called two-factor authentication.

Handle your passwords carefully

Short, not too complex passwords are not secure, since attackers may for instance be able to guess them. In particular, last names, children's or pets' names, words of any popular language, key sequences (for instance "asdg" or "45678") or birthdays must not be used. **The best protection is offered by a random combination of at least 10 uppercase and lowercase letters plus numbers and special characters.** Don't always use the same password everywhere, but use different passwords for different applications, and don't disclose them to anybody else. Remember your passwords, or keep them in a safe place.

It is not really that hard to draw up a secure password: Take a sentence you can remember easily, and make up your password from the respective first letters, numbers and special characters: "**M**y **d**aughter **T**amara **w**as **b**orn **o**n **19** **J**anuary**!**" This creates a password consisting of a random character string which you can easily remember: "**MdTwbo19J!**"

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

5

Exercise care and remain alert

Do you believe everything they want you to believe? Take responsibility yourself, and always apply a healthy dose of suspicion when surfing.

Important points to remember:

- When surfing the internet, always remain wary and consider carefully where and to whom you provide any personal information.
- Financial institutions, telecommunications and other service providers will never ask you for a password (neither by email nor over the telephone) and will never ask you to change your password in this manner either.
- When using mobile devices (smartphones or tablets), you should take the same precautions as the ones you take on your PC at home.
- In case of uncertainty or suspicion as to whether there has been an attack, always seek support.

Two-factor authentication

In addition to a secure password, so-called two-factor authentication provides additional security. Here, 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.

→ **Protect your devices and online access against access by strangers!**

Further information including detailed instructions and tools can be found here:

www.ebas.ch/step4

Steps 1 to 4 ensure that you have protected your device and online access very well from a technical viewpoint. However, user conduct often poses the greatest risk in itself and makes users targets for attack – you should therefore always apply a dose of common sense.

Protecting against phishing and social engineering

With phishing, fraudsters will try to win your trust, for instance by impersonating your financial institution in emails or on the telephone to try and lure you to a website with the help of a link which looks almost identical to the ones used by your financial institution. If you fall for this and provide them with your access data, these fraudsters can then clear out your bank account.

Increased risks with mobile devices

Many apps grant themselves extensive access rights with no apparent justification. It is for instance not necessary for any old app to access data such as location, address book or telephone status. You should therefore critically check whether an app actually needs these access rights to function, and deactivate any rights not required if possible.

→ **Exercise caution and always remain alert when surfing the internet!**

Further information including detailed instructions and tools can be found here:

www.ebas.ch/step5

This leaflet was created in co-operation with the **University of Lucerne** and **«eBanking – but secure!»**

Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik
FH Zentralschweiz

eBanking but secure!

About «eBanking – but secure!»

«eBanking – but secure!» is an independent platform set up by the University of Lucerne Computer Science department for the purpose of helping you protect your personal data. On our website www.ebas.ch, anyone interested will find practical information on measures and rules of conduct required for the secure use of e-banking applications.

- Main page:
  https://www.ebas.ch
- Facebook page:
  https://www.facebook.com/ebankingabersicher
- YouTube channel:
  https://www.youtube.com/user/ebankingabersicher
- Media section:
  https://www.ebas.ch/mediasection

University of Lucerne Computer Science department

The University of Lucerne Computer Science department offers Bachelor and Master study courses, application-oriented research and development plus a range of professional development courses in the fields of computer science and business informatics on one campus.

- Home page of Computer Science department:
  https://www.hslu.ch/informatik
- Information security & privacy:
  https://www.hslu.ch/forschung-information-security

January 2020

Swiss Crime Prevention (SCP)
Haus der Kantone
Speichergasse 6
CH-3001 Bern

www.skppsc.ch