5 steps
for your digital security

Your Police and the Swiss Crime Prevention – an office of the ministries of justice and police of the Cantons.

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.

Next to all these possibilities though, 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 like 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 **Protect** with antivirus software

Step 3 **Monitor** with a firewall

Step 4 **Prevent** by updating your software

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 valuable are your data? You should regularly back them up onto at least one second medium and always check that your data have actually been backed up.

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 are included in your back-up, and that they can be restored properly.
- To ensure your back-up data are protected against malware infections in the best possible way, you should only connect your external back-up hard drive when you are actually using it. Don't keep your online storage for your back-up permanently connected either, but only when you are running a back-up.

These days, large amounts of data such as text documents, e-mails, photos, videos, music and more are stored on computers, tablets and smartphones. You cannot rule out that these data are partially or even completely destroyed due to incorrect operations (e. g. accidental deletion), a technical defect (e. g. due to a defective hard drive) or because of viruses, worms or Trojans.

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

www.ebas.ch/step1

Protected by your windscreen!
Protected from digital vermin by your antivirus!

2

Protect with antivirus software

What kind of viruses will end up on your computer, your tablet or your smartphone? Practically none, as long as you have installed antivirus software.

Important points to remember

- Do use up-to-date antivirus software.
- Configure your software such that it is regularly and automatically updated so it is equipped to deal with the latest threats.
- Regularly check your computer or your mobile device for malware infections. Have your antivirus software scan your whole system by running a complete system check to this end.

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 (viruses, worms, Trojans) 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.

→ **Protect your devices with antivirus software!**

www.ebas.ch/step2

Your garage door stops car thieves!
Your firewall stops data thieves!

3

Monitor with a firewall

Have you securely closed the "doors" of your computer or mobile device? You can do so reliably by activating your firewall to monitor Internet traffic towards your device.

Important points to remember

- Make absolutely sure to activate the firewall that comes with your operating system before you connect your device to the Internet or another network.
- Certain online software, such as online games, require certain "access doors" (socalled ports) to be open. Please make sure that you only ever open any ports actually required, and that you don't completely deactivate your firewall.

When users are surfing the Internet on your computer, tablet or smartphone, invisible "access doors" (ports) are opened on your device to communicate. These offer a target for attackers from the Internet. A firewall installed will close these doors as much as possible and will monitor all data traffic between your devices and the Internet. Your firewall will alert you if it discovers any "suspicious" network traffic.

→ Monitor your Internet communications by activating your firewall!

www.ebas.ch/step3

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

4

Prevent by updating your software

Who better to look after your software's security than the software manufacturers themselves? Maintain your software and apps, and make sure to regularly run the latest updates. This way, you will always be on the safe side.

Important points to remember

- Activate the automatic update function for all software and apps installed – in particular operating system, antivirus software, firewall, browser incl. plug-ins and document viewing software.
- Only ever download software, apps and their updates from the manufacturer's web page, never from third party providers.
- 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.

→ Prevent by always installing all latest software updates!

www.ebas.ch/step4

Use your head when on the road!
Use your brain when on the Internet!

5

Exercise care and remain alert

How do you act responsibly? Don't believe just anything you read on the Internet, and always apply a healthy dose of suspicion when surfing. You should also protect your computer and your mobile devices with a secure password.

As often as not, users themselves are the greatest risk factor – apply a dose of common sense. Just one example: With phishing, fraudsters for instance send you an e-mail or ring you up pretending to work for your financial institution and try to coax you into clicking on a certain link, to lure you to a website which looks almost identical to that of your financial institution. If you fall for this and provide them with your access data, these fraudsters can then clear out your bank account. **Always remember: A reputable financial institution will never ask you for your e-banking access data in an e-mail.** You should therefore apply a healthy dose of suspicion.

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 e-mail nor on the telephone) and will not ever ask you to change your password in this manner either.
- When using mobile devices (smartphones, tablets), you should take the same precautions as you do on your PC at home.

- Use long passwords consisting of at least 10 characters, made up of random uppercase and lowercase letters plus numbers and some special characters, too.
- Never tell anyone your passwords, and always keep them in a safe place, possibly in encrypted form.
- Don't save any passwords to access protected websites in your browser. Browsers generally don't manage these passwords securely enough.

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 choices, and don't tell 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!**

→ Exercise caution and always remain alert when surfing the Internet!

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 of the University of Lucerne – Computer Science meant to assist you in retaining your personal information security. On our website www.ebankingbutsecure.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.ebankingbutsecure.ch
  https://www.ebas.ch
- YouTube channel:
  https://www.youtube.com/user/ebankingabersicher
- Media Section:
  https://www.ebas.ch/mediasection

University of Lucerne – Computer Science

The University of Lucerne – Computer Science 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 at one campus.

- Main page Computer Science department:
  https://www.hslu.ch/informatik
- Information Security & Privacy:
  https://www.hslu.ch/forschung-information-security

SKPPSC

Swiss Crime Prevention (SCP)
House of Cantons
Speichergasse 6
CH-3001 Bern

www.skppsc.ch