5 – Exercising care and remaining alert

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

The most 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 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.

5 – Exercise care and remain alert

5 steps for your digital security

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

eBanking but secure! www.ebas.ch

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

When phishing (https://www.ebas.ch/en/phishing/), fraudsters employ e-mails, text messages, chat messages or phone calls to attempt and gain your trust, for instance by pretending to work for your financial institution and providing you with a link to lure you to a website which looks very similar to the one of your actual financial institution. If you fall for this and provide them with your access data, these fraudsters can then clear out your bank account.

Or there are fraudulent support calls (https://www.ebas.ch/en/fraudulent-support-calls/), where a purported Microsoft employee or IT support company contacts you to then try and gain access to your device.

Always remember: A reputable financial institution will never ask you for your e-banking access data in an e-mail or by telephone.

Fraudsters often find the basic knowledge for such attacks in social media and networks (https://www.ebas.ch/en/social-media-and-networks/) . You should exercise caution there, too, and seriously think about (https://www.ebas.ch/en/privacy-and-data-protection-on-the-internet/) the kind of information you disclose there.

Increased risks with mobile devices

Access rights with mobile apps

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.

You should be cautious about passing on your location details as a matter of principle: Avoid localisation services, and don't save any location details in any photos you might upload to social media. Thieves and hackers can leverage that kind of information.

Immediately lock in case of loss

With the help of various apps, lost or stolen mobile devices can be locked remotely. This will ensure your personal data on your device are erased and can no longer be retrieved. But beware: This type of command can also be abused by malicious third parties. You should therefore ensure you only use reputable suppliers here, too. Once you have locked your device, you should also get your provider to lock your SIM card.

Ask for help

If you are not certain, suspect an attack or worse, or have already fallen victim to an attack, don't hesitate to ask for help, for instance:

- In case of uncertainties and ambiguities with regard to your e-banking facility, contact your financial institution (https://www.ebas.ch/en/partners/) .
- For technical problems or in case you suspect a malware infection, contact your IT expert/IT support for help.
- If you have fallen victim to an attack, notify your financial institution (https://www.ebas.ch/en/partners/) and the police (https://polizei.ch) .

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 (https://www.ebas.ch/en/4-protecting-online-access/)

Step 5 – Exercise Care