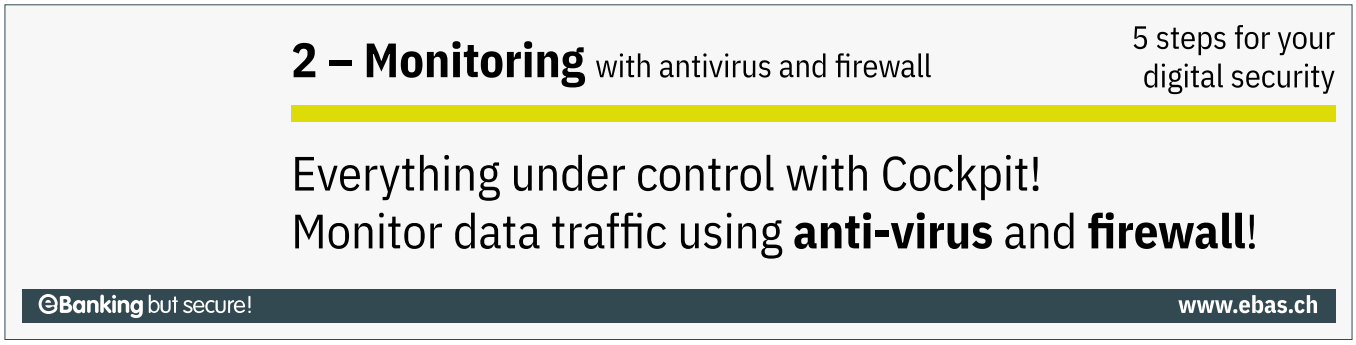
2 – Monitoring with antivirus software and firewall

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.

The most 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.



How to proceed

Use antivirus software and a firewall, which is continuously kept updated with automated updates so that you are always protected against the latest risks.

Windows

Windows 10 and Windows 11 are supplied with a firewall, and their “Windows Defender” antivirus software is activated by default. This ensures you are perfectly protected.

To use additional protective functions, such as a parental control content filter, you can also use any of the following list of products (which is not comprehensive), sometimes even free of charge:

- AVG Free Anti-Virus (https://free.avg.com)
- Avira Free Antivirus (https://www.avira.com)
- Bitdefender (https://www.bitdefender.de)
- F-Secure (https://www.f-secure.com)
- G Data (https://www.gdata.de)
- Malwarebytes (https://www.malwarebytes.com)

- McAfee (https://www.mcafee.com)
- Norton (https://ch.norton.com)
- Panda (https://www.pandasecurity.com)
- Sophos (https://www.sophos.com)
- Trend Micro (https://www.trendmicro.com)

macOS

Under macOS, it is vital to activate the internal firewall, which is deactivated by default. To do so, click on “System Settings…” in the “Apple” menu. Under the “Firewall” tab, you can activate the firewall under “Network”. This will now remain activated even when you restart.

Mac OS also has an integral protective mechanism meant to prevent any malware infections. The “Gatekeeper” software, which is activated by default, will protect you from accidentally installing malware.

Additional protection is provided by specific antivirus software. We would recommend the following software, which sometimes comes free of charge and also recognizes Windows viruses (not a comprehensive list):

- AVG (https://free.avg.com)
- Avira (https://www.avira.com)
- Bitdefender (https://www.bitdefender.de)
- F-Secure (https://www.f-secure.com)
- Norton (https://ch.norton.com)
- Trend Micro (https://www.trendmicro.com)

Smartphone und Tablet

It is not readily possible to install a firewall on a smartphone or tablet. While root privileges are required with Android devices, you will have to use a “Jailbreak” on an iPhone. Both a root and a Jailbreak process can damage your device and will deactivate several of the operating system’s security mechanisms. In addition, this may also void all your warranty claims. We therefore do not recommend such processes.

However, you should make absolutely sure to use antivirus software on Android devices. We recommend the following antivirus software for use with **Android**, some of which is free:

- AhnLab (https://www.ahnlab.com)
- AVG (https://free.avg.com)
- Avira (https://www.avira.com)
- Bitdefender (https://www.bitdefender.de)
- G Data (https://www.gdata.de)
- McAfee (https://www.mcafee.com)
- Norton (https://ch.norton.com)

- Sophos (https://www.sophos.com)
- Trend Micro (https://www.trendmicro.com)

You don't need any antivirus software for **iOS devices** such as iPhone or iPad at the moment. This is due to the closed operating system which is meant to prevent the installation of any questionable apps or other malware, and which severely restricts the permissions of any apps installed.

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

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

Further information for those interested

Malware infection - what now?

Should you suspect your device is infected with malware or if your antivirus software notifies you of such an infection, you can find additional information on what you can do here (https://www.ebas.ch/en/malware-infection/).

Firewall?

When users are surfing the Internet on their computer, tablet or smartphone, invisible “access doors” (ports) are opened on their devices 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.