How to download programs and apps safely

Most people are aware of the advice is to obtain software from trustworthy sources only. But how to establish whether a source is trustworthy?

The most important points to remember:

- Only ever install mobile device apps from the official store (Apple App Store or Google Play Store).
- Programs for standard computers should only be installed if obtained from the official manufacturer website.
- You should be particularly careful with software allowing remote access.
- **Your bank will never ask you to download software from a third-party provider!**

For mobile devices, the official app stores (iTunes Store for iOS and Google Play Store for Android) are considered quite safe sources. This is why you should always download apps from the official app stores only. Remain wary towards apps with a low reputation or with recommendations by persons unknown. If you have never heard of the provider, find out more about them before installing any app. Further information on installing and using apps for mobile devices, in particular mobile banking apps, can be found here (https://www.ebas.ch/en/mobile-banking-app/) .

Even with standard computers, software can be purchased from so-called “stores” nowadays”. It is still common though to download and install them from a variety of different websites. When doing do, it is critical to ensure these are the official software manufacturer ones. If you don’t recognise the website address, it is advisable to have it confirmed via several sources. You could for instance compare relevant search engine results with entries in an online encyclopaedia (for instance Wikipedia) or the details provided in a mobile device app store.

Important: Your bank will never ask you to download software from a third-party provider!

You should also trust your gut instincts, in particular when viewing a website. Dubious-looking sites, for instance because they offer all sorts of software by different manufacturers to download for free, are covered in misleading adverts or hide a download link behind a countdown counter, should best be avoided.

In addition, you should also be particularly cautious with any applications allowing remote access. Such applications can be abused by fraudsters to obtain access to a device, gather sensitive information about its user and even enable scammers to log into your e-banking facility. You should be particularly careful if someone for instance calls you asking to install a program or app allowing remote access. In most cases, this involves fraud attempts.

Generally speaking, you should also ensure to follow our 5 steps for your digital security (https://www.ebas.ch/en/5-steps-for-your-digital-security/) to provide you with basic protection. With regard to downloading programs and apps, steps “2 – Monitoring with antivirus software and firewall (https://www.ebas.ch/en/2-monitoring-with-antivirus-software-and-firewall/) “ and “3 – Preventing with software updates (https://www.ebas.ch/en/3-preventing-with-software-updates/) “ are especially important.

Software is a term used to denote computer programs and applications (such as your operating system, Word or Excel) and also apps, which are necessary to render a device operational, operable and useful for users.