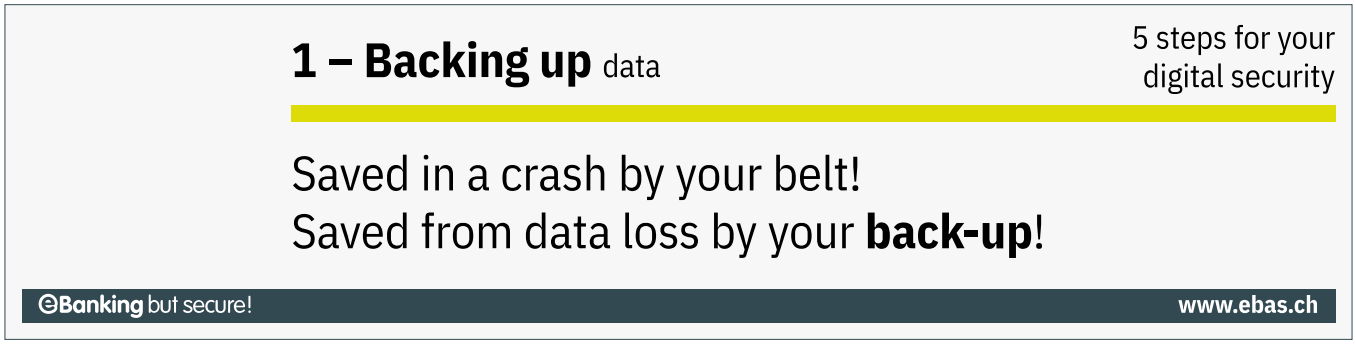
1 – Backing up data

How much do you value 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, too.

The most 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.
- You should only connect your external back-up hard drive when you are actually using it. Don't keep your online storage device for your back-up permanently linked either, but only when you are running a back-up.



These days, large amounts of text documents, e-mails, photos, videos, music and more are stored on computers, tablets and smartphones in the shape of digital data.

You cannot completely rule out that these data are 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 viruses, worms and Trojans.

How to proceed

One simple solution for backing up the data on your computer is to create a copy - a so-called back-up - on an external hard drive. To do so, you copy your files from your own device to an external data carrier, either manually or with the help of special software. Once the back-up has finished, it is vital to disconnect the external hard drive from your device, so your back-up data are protected from viruses, worms and other malware.

For home use, it is usually sufficient to create a back-up every few weeks or so. With smaller data volumes, you can use either writable CDs or DVDs, too. For huge data volumes though, the creation of a back-up copy is quite complex - this is where special back-up software can help.

Keep your data carrier containing your back-up separately from your device and also in a different location, if possible. Please remember that in case of fire or a break-in, back-up data carriers could also get lost or stolen.

Windows

With the “File History” option under Windows 10 or Windows 11, you have convenient back-up features installed as standard available to you: Microsoft instructions (https://support.microsoft.com/en-gb/help/4027408/windows-10-backup-and-restore)

macOS

You can use the “Time Machine” functionality incorporated in Mac OS X to create back-up copies of both your system and data: Apple instructions (https://support.apple.com/en-gb/HT201250)

Smartphone und Tablet

Any smartphone and tablet can be connected to your computer using a USB cable and will then be recognised as a USB data carrier. You will then be able to easily copy data such as photos, music or documents manually to your PC using a file manager (e.g. Explorer under Windows, or Finder under Mac). The type of data you can back up manually depends on the operating system you use. There are other back-up processes too, which differ from one operating system to the next:

- With **iOS devices** (iPhone, iPad etc.), you use iTunes to back up onto a PC/Mac or via the iCloud: Apple instructions (https://support.apple.com/en-gb/HT203977)
- With **Android devices**, you can back-up your most important data onto Google Drive servers: Google instructions (https://support.google.com/nexus/answer/2819582?hl=en)
  Please note: Please remember that potentially sensitive data such as WiFi passwords might be backed up to Google Drive if you store your data there. Theoretically, this would mean Google could also access those.
  Many Android devices have device-specific back-up features, too.

Another good option for storing your data is offered by cloud storage. This means your data are centrally stored on the Internet. Further information on this can be found in our article on “Cloud storage“ (https://www.ebas.ch/en/cloud-storage/) .

In case you no longer need a device or back-up hard drive and you dispose of or sell it, you should make sure to erase all data it contains in a secure manner. Further information on this issue can be found in our article on “Secure deletion” (https://www.ebas.ch/en/secure-deletion/) .

Protect your data and all your devices with the help of our “5 steps for your digital security”:

Step 1 – Back up

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