

## protect data and devices

PCs, smartphones, or tablets store and have access to valuable data. Security measures should be taken to make sure that this data is not lost, spied on or changed without authorisation.

## use good passwords

Username and password only allow access to authorised users.

A good password should

- consist of lower- and upper-case letters, numbers and special characters
- have a minimum length of 8 characters
- not be in a dictionary
- have no personal reference such as date of birth, parts of names, etc.
- be changed regularly

good password: i1963mfib! (reminder: in **1963**, my father is born!)

poor passwords: 12345 qwertz secret hello boss password...

## firewall

The firewall controls data traffic between computers. It protects computers from unwanted access via the network. Modern operating systems, such as Linux or Windows, have a firewall as software.

## backup

*The computer is broken - where is my data?*

If a hard disk is damaged or a fire breaks out, computer data can be destroyed. Therefore, **backups** (security copies = backup copies) should be made on external data carriers (hard disks, online data storage, etc.) with which data can be restored in the event of an accident.

The backup copies should be stored in a different place so that they are not destroyed in the event of damage!

## malware and antivirus software

Malware is an umbrella term for various types of unwanted programs. If the computer reacts more slowly than usual or no longer works as usual, malware may be the cause.

## basic types of malware

**Computer viruses** are the oldest type of malware. They spread by writing copies of themselves in programs, documents or data carriers.

A **computer worm** is similar to a computer virus, but spreads directly via networks such as the Internet and attempts to invade computers.

A **Trojan Horse** (short Trojan) is a combination of a (sometimes only apparently) useful host program with a hidden malicious part. A Trojan horse does not spread itself, but advertises the usefulness of the host program in order to be installed.

**Spyware** and **adware** (composed of advertisement and software) research the computer and user behaviour and send the data to the manufacturer or other sources either to sell or to place targeted advertisements. This form of malware is often installed unnoticed together with useful software.

## How does a virus get onto my PC?

Infected files can be copied to the PC as e-mail attachments or by downloading them from the Internet. When an infected program is called up, the virus spreads. USB drives can also contain malware!

## How do I protect myself from malware?

- Do not install programs from unsafe sources
- Do not open unknown e-mail attachments
- install antivirus software: For private users, the antivirus program Windows Defender, which is included in Windows 10, is sufficient.
- Antivirus programs update themselves automatically so that the latest viruses are also detected
- The operating system and programs must have the latest security updates installed.

## answer the following questions:

What could a good password look like? Create a password!

A – good password: \_\_\_\_\_

How is the data traffic between computers or in the network controlled?

A: \_\_\_\_\_

What is the umbrella term for unwanted programs?

A: \_\_\_\_\_

How can you also call a security copy?

A: \_\_\_\_\_

What does a spyware do?

A: \_\_\_\_\_

## scan this QR-code, open the link and solve the quiz:



points achieved: \_\_\_\_\_