New installation onto an infected PC Windows 7

Your PC has become infected with malware. You don’t know how to correctly reinstall your system? The following step-by-step instructions will help you to reinstall your PC and at the same time reduce the risk of a new infection.

We have tried to draw up as generally applicable a set of instructions for private users as possible. Of course the steps required may differ in specific cases.

These instructions are based on Windows 7 Professional 32 bit edition, but also apply to 64 bit versions.

To be able to properly reinstall your system in accordance with these instructions, you will need the Windows 7 installation CD plus an external storage medium to back up your data.

Step 1: Disconnect your PC from the network

- If your PC is connected to the network via a cable, simply pull out the network plug.
- If you use a wireless network (WLAN), you should deactivate the network card in Device Manager (Click on *Start* → Right-click *Computer* → Click *Properties*→ Click *Device Manager*).

Step 2: Backing up personal data

- With the «Shift» key pressed and held down, connect an external storage medium, and back up your personal data. Do not use a «normal» back-up medium to do so, but a new, completely blank one if possible.

  PLEASE NOTE: Malware on your PC can lead to your external storage medium and all data stored on it becoming infected too. Malware specifically uses the Autorun function to spread via external storage media (USB stick etc.). It is relatively simple to temporarily deactivate this Autorun function. To do so, press and hold the «Shift» key on your keyboard. Then connect the external storage medium to your computer and only let go of the «Shift» key a short time later. In this case, the «Shift» key prevents Windows from automatically executing programs and files on the external storage medium.

Step 3: Cleaning the Master Boot Record (MBR)

Certain computer viruses will infiltrate the so-called Master Boot Record (MBR) of your PC. For this reason, this should be rewritten and cleaned this way. Use the «bootrec.exe» utility in the Windows restore environment to do so.

- Insert your Windows 7 installation CD into your drive and restart your PC.
- If your PC does not boot from the CD inserted after this restart, set the CD drive as the first device in the PC BIOS (see mainboard manual). Alternatively, press the «F8» function key straight after starting the PC. This will take you to the boot manager where you can select the CD drive.
- Press a key when you are asked to do so.
- Select a language, time, currency, keyboard or method of entry, and then click *Continue*.
- Click on *Computer repair options*.
- Click the operating system and then *Continue*.
- In the dialogue box System Restore Options, click *Command prompt*.

- Enter «`bootrec.exe /fixmbr`» and then press the *Enter* key. This will restore the MBR (thus deactivating the MBR rootkit functionality of any malware).
- Close the Command prompt and use *Shut down* to close your PC down. Leave the Windows 7 installation CD in the drive.

Step 4: Reinstallation of Windows 7

- Restart your PC.
- If your PC does not boot from the CD inserted after this restart, set the CD drive as the first device in the PC BIOS (see mainboard manual). Alternatively, press the «F8» function key straight after starting the PC. This will take you to the boot manager where you can select the CD drive.
- Press a key when you are asked to do so.
- Select language, time, currency, keyboard or method of entry, and then click *Continue*.
- Now you need to click on *Install now*.
- As you progress through the installation, click the drive options. You can delete, newly create and format partitions there.

  WARNING: When you delete or format a partition, all data on the partition will be lost!

  PLEASE NOTE: To make sure there is no malware present on your PC any longer, you must delete the existing partitions and create them once again. Afterwards, the newly created partitions should be formatted. Please also note that there may be a recovery partition created by the manufacturer present. This should not be deleted or formatted.
- Finish installing Windows 7 with the recommended settings.
- Reconnect your PC to the Internet (insert network plug).
- Use Windows Update to update your operating system (click *Start* → *Control panel*→ *Windows Update*).

Step 5: Installing antivirus software

- Install antivirus software from a trustworthy source and update this using the integrated update function.

  PLEASE NOTE: A list of recommended antivirus software can be found under www.ebas.ch/5steps_step2.

Step 6: Installing and updating programs

- Install the required programs. Update all programs, and activate the auto-update function wherever possible.

  PLEASE NOTE: Please make sure to only install programs from trustworthy sources (e. g. manufacturer download sites or software archives such as PCtipp, Heise etc.).

Step 7: Scanning data

- Hold down the «shift» key and connect the external storage medium with the data backed up previously to your PC.

  PLEASE NOTE: In case malware was copied to the external storage medium when backing up your data, your PC can become reinfected! To prevent this, if possible, it is mandatory to hold down the «Shift» key when connecting the external storage medium (see note under step 2).
- Scan the whole system and the external storage medium using the antivirus software installed previously. In case any infected files are found, you should have ask to clean or delete them!

PLEASE NOTE: A better, yet more elaborate alternative to scanning via the newly installed system would be to check your external storage medium via a bootable live CD or from another operating system (e. g. Linux, macOS).

Step 8: Restoring data

- Restore your backed-up data from the external storage medium to the PC.

Step 9: Other vital things to do!

- As malware very frequently captures user names and passwords nowadays, you should make sure to change all passwords on your system itself, but also all passwords to log into any websites (e. g. e-banking, e-mail access, Facebook etc.).
- In addition you should closely check your e-banking and credit card statements.

These instructions were drawn up by «eBanking – but secure!» in co-operation with SWITCH.

eBanking but secure!

On our website **www.ebankingbutsecure.ch**, which is free to use, you will find information on measures required and codes of conduct for the safe use of e-banking applications.

SWITCH

SWITCH provides additional innovative, unique and practice-orientated Internet services for Swiss universities and Internet users.