Malware infection

Anti-virus software and automatic updates of your operating system are crucial to be able to surf the Internet safely. Still it can happen that a computer becomes infected with malware. You must recognise this and react correctly!

How do I recognise a malware infection?
Potential signs:

- Your anti-virus software notifies you of an infection.
- There are error messages when starting or shutting down your computer.
- The computer no longer runs in a stable manner - it frequently crashes.
- Your system is slower, your working memory and/or processor are continuously in use, or your hard drive is continuously active.
- The anti-virus software is deactivated (even after you have explicitly activated it).
- You can no longer reach the web pages of one or several anti- virus manufacturers.

You can read up on how to protect yourself against malware infections under "Step 2 - Monitoring" (https://www.ebas.ch/en/2-monitoring-with-antivirus-software-and-firewall/) of our "5 steps for your digital security" (https://www.ebas.ch/en/5-steps-for-your-digital-securtity/) . There you can also find a list of anti-virus software, some of it free of charge. If there is still a strong suspicion that your machine is infected, you have to react correctly.

The most important steps to take after a malware infection:

1. Keep calm, disconnect from the Internet and check your last data back-up. (#step1)
2. Decide whether you will need a specialist. (#step2)
3. Identify and remove malware. (#step3)
4. The last resort: A fresh installation. (#step4)

The term malware is made up of the terms "malicious" and "software". Malware is the generic term for software which executes malicious functions on a device (such as viruses, worms, Trojans, ransomware).

Further information for all those interested
Malware infection - what now?

Step 1: Keep calm, disconnect from the Internet and check your last data back-up

The first thing to do is to disconnect from the Internet (remove your LAN plug or switch the Wi-Fi off). Then you should establish how old your last data back-up is. It is recommended to create an additional, new back-up onto a different storage media from your normal back-up.

Please note: It is possible that you also back up malware when you create such a back-up, but that is irrelevant for the time being.

Step 2: Decide whether you will need a specialist

You should now consider whether you can remove the malware yourself, or whether you want to consult a specialist. There are various anti-virus software manufacturers who offer a special service to remove malware. This often involves a telephone helpline or "remote malware removal". However, such services are chargeable. As an alternative, there are also various computer specialist stores which offer repair services (especially for malware infections).

Step 3: Identify and remove malware

Certain types of malware can be removed by the anti-virus software installed, but not all of them. If your anti-virus software is unable to remove the malware, it is recommended to use a so-called "second opinion virus scanner", for instance

- Malwarebytes (https://www.malwarebytes.com)
- HitMan Pro (https://www.hitmanpro.com)

If this doesn't help either, the malware will need to be precisely identified. It is best to use the malware name (as displayed by your anti-virus software) and then research on the Internet (from another non-infected device) for instructions on how to remove this. Most antivirus software manufacturers provide malware data bases including instructions for removal. If your antivirus software manufacturer provides a boot CD, you should try to start your computer from this CD and remove the malware this way.

Malware data bases

- Avira (https://www.avira.com/en/support-virus-lab)
- Kaspersky (https://www.viruslist.com/)
- McAfee (https://www.mcafee.com/us/threat-center.aspx)
- Microsoft (https://www.microsoft.com/security/portal/)
- Norton-Symantec (https://www.symantec.com/en/en/norton/security_response/threatexplorer/index.jsp)
- Trend Micro (https://www.trendmicro.com/vinfo/us/threat-encyclopedia/)

Removal tools

- F-Secure (https://www.f-secure.com/en_EMEA/security/security-lab/tools-and-services/removal-tools/index.html)
- Kaspersky (https://support.kaspersky.com/viruses)
- McAfee (https://de.mcafee.com/virusInfo/default.asp?id=vrt)

- Microsoft (https://support.microsoft.com/en-us/help/890830/remove-specific-prevalent-malware-with-windows-malicious-software-remo)
- Norton-Symantec (https://www.symantec.com/en/en/norton/security_response/removaltools.jsp)

For very common malware, antivirus software manufacturers offer some so-called removal tools free-of-charge. These will check your computer for a certain type of malware and automatically remove it. When downloading a removal tool, you must make absolutely sure that this originates from a reputable website (for instance that of the antivirus software manufacturer) - there are antivirus software and removal tools created by cyber-criminals which contain malware themselves.

Step 4: The last resort - a fresh installation
If all these measures do not provide the desired result, you will have to completely re-install your computer (or jump back to step 2 and get some advice from an expert).

You can read up on how to reinstall your system, and reduce the risk of becoming reinfected at the same time, in our instructions (for Windows 10) (https://www.ebas.ch/en/new-installation-windows-10/) .