SMT
SICHERHEITSMANAGEMENT-TEAM

GOETHE
UNIVERSITÄT
FRANKFURT AM MAIN

Goethe University recommendations and best practices for using internet services

The following recommendations apply to all members of Goethe University Frankfurt. They regulate the official use of internet services. Goethe University regulations and statutes, in particular IT security regulations, IT security guidelines and the IuK use regulation[1], are not affected by these recommendations.

Life without the internet is unimaginable in our modern world. Today, nearly all important information can be found in the “web”, whose abundant offerings can accessed by “surfing”. It is important to note that the use of the Internet is only permitted in compliance with applicable law, in particular personal rights, data protection, copyright and criminal law regulations.

Goethe University’s Security Management Team (SMT) recommends the following measures to increase security when surfing in the Internet:

1) Protection programmes

   - Make sure the **internal firewall** on your PC is activated.

   - Install and activate anti-virus programme on your PC and update it regularly. The university computing centre (HRZ) provides a free virus scanner that can be downloaded by all Goethe University members (**Sophos** for Windows and Mac OS).

2) Security updates

   - Regularly download and install **system updates** for your devices. Use an up-to-date version of your operating system and the programmes you have installed. Install security updates for your software, in particular your web browser and operating system right away. If possible, use the function for **automatic updates**.

   - In addition, uninstall **programmes that are no longer needed**. The fewer applications you use, the less vulnerable your system is to attacks.

3) Accounts

   - The use of Internet services should only take place with a user account with limited rights, and never with an administrator account!

[1] Allgemeine Nutzungsordnung für die Informationsverarbeitungs- und Kommunikationsinfrastruktur der Goethe-Universität Frankfurt – General use regulations for information processing and communication infrastructure at Goethe University Frankfurt

- Be mindful of how you handle usernames and passwords. Besides online banking services, this includes access data for social networks, online shops and similar websites.

- Use secure **passwords** of at least **10-16 characters** consisting of letters, numbers and symbols. **Never** store passwords, PINs, TANs, or your credit card information on your devices. **Official passwords** may **not** be used for external services. You can find additional information in our **recommendations on „Using Passwords**".

4) Software and programmes

- Only download programmes from **trustworthy sources**. (Preferably from the websites of the software manufacturer).

- When installing programmes and software, be mindful of hidden software components.

5) Surfing the Internet

- The **input of sensitive data** should be carried out only through an encrypted connection (**https**). Always check to make sure "https" is in the address field and a closed lock symbol in the status field of the browser.

- Heed any **warning messages from the web browser** regarding the validity and trustworthiness of the certificate.

- **Digital certificates** attest to the trustworthiness of communication partners in the Internet.

- Use **common sense** when surfing. Do not blindly trust notifications, messages and requests. Do not click on every offer, no matter how enticing it sounds. Nothing in the Internet is for free. Many providers who lure with prices and rewards are only after your data.

6) WIFI

- WIFI connections should not be used indiscriminately, as they do not always provide a secure, encrypted connection. Especially with regard to sensitive data (e.g., online banking, shopping, etc.) an **encrypted connection** is essential.

- **Avoid online banking** in internet cafes or at public terminals or places. As a rule, **do not enter passwords** when using the Internet at such locations. If you conduct banking business using your cell phone, do not have the TAN sent to the same device.

- It is recommended to use a VPN connection. The University Computing Centre (HRZ) provides a free VPN connection for all university members. You can find more information at: https://www.rz.uni-frankfurt.de/vpn

7) **Flash** is an outdated technology that often serves as a gateway for malware. Uninstall your flash player, or at least adjust the settings on your web browser so that trustworthy flash content can only be activated individually per mouse click.

8) **Delete cookies and flash cookies** regularly, preferably after each session. Automatic deletion can often be selected in your browser settings.

9) Be wary of emails with unknown attachments. **Delete suspicious emails immediately** without opening them.

10) Make regular backups of your files and save them on external media such as external hard drives or USB sticks that are used exclusively for this purpose, to guard against data loss or infection.

11) Please contact your IT support or your IT security officer if you have any questions.

Further information:

- Bundesamt für Sicherheit in der Informationstechnik (BSI) - (Federal Office for Information Security)
  https://www.bsi-fuer-buerger.de

- DFN Computer Emergency Response Team (DFN-CERT)
  https://www.dfn-cert.de

- IT-Sicherheitsmanagement-Team (SMT) - Goethe-University IT Security Management Team
  https://www.uni-frankfurt.de/smt

- Goethe University Computer Emergency Response Team (GU-CERT)
  https://www.rz.uni-frankfurt.de/gu-cert

- Hochschulrechenzentrum (HRZ) – Goethe University Computing Centre
  https://www.uni-frankfurt.de/hrz/it-sicherheit