Do I need a password?

In order to identify a user on a computer system or a database, a username and password is required to authenticate login.

Guidelines to avoid password abuse

- Do not share your password with anyone
- Never save passwords in a computer file or on sticky notes pinned to a monitor or hidden under the keyboard.
- Do not use easy-to-guess passwords such as common names, cities, landmarks, dates of birth etc.
- Change your passwords at regular intervals

You should avoid using the same username and password combination on multiple accounts. Doing this creates a single point of failure, which means that if an intruder gains access to one account, he or she will have access to all of your accounts.

Password theft and phishing

The University of Bayreuth (e.g. IT-Servicezentrum, Studentenwerk, Verwaltung, etc.) and all other trusted institutions (e.g. banks, etc.) will never send you an email or call you or use any other means requesting for confidential account information such as TANs and passwords.

What are strong passwords?

A secure password should have a minimum length of eight characters combining a sequence of mixed-case letters and numbers, assembled in no apparent order, recognizable pattern or of any obvious meaning (without special characters such as !"§$%&/ß and umlauts such as äüö).

john **MfTsm1feoaD**

unsicher sicher

Link your password with personal experiences or memories. Think of a phrase that only you know. Choose a line or two from your favorite song or poem.

Let your imagination run wild, be creative!

Examples

5 **R**ain**d**rops **k**eep **f**alling **o**n **m**y **H**ead	**5RdkfomH**
My **f**riend **T**om **s**ends **m**e **1** **f**unny **e**mail **o**nce **a** **D**ay	**MfTsm1feoaD**
4th **f**loor **d**own **C**orridor **f**irst **D**oor **r**ight **S**ide	**4fdCfDrS**

These simple password creation hints significantly increase password security and are very effective against brute force password guessing attacks as well.

HTTPS-Encryption

When sending confidential information over the Internet such as usernames, passwords, or credit card numbers etc. only send it securely. Verify the URL in the address bar begins with https:// instead of http:// and a closed padlock icon is visible.

Flyer online: German English

Computer Security & Protection

... Staff ... Students

How can I protect myself?

Questions? Please feel free to contact the Anlaufstelle!

☎ 3003 or www.its.uni-bayreuth.de

UNIVERSITÄT BAYREUTH IT-SERVICEZENTRUM

In 7 Steps...

Enable the Firewall

1 All current operating systems have a built-in firewall, which examines incoming network traffic and automatically blocks all unauthorized attempts to connect to your PC. From a safety point of view, these integrated firewalls are absolutely sufficient. When enabled, the use of an additional commercial firewall is not necessary.

Use Antivirus Software

2 Malicious software is a constant threat to any computer connected to the Internet. Malware (i.e. Viruses & spyware), can infiltrate your computer without you noticing it and create havoc. Especially on Microsoft Windows operating systems, it is very important to ensure Antivirus Software is installed and kept up-to-date. Depending on your vendor, virus definition updates may be released hourly, or daily. Only the newest virus signature files offer up-to-date virus detection and disinfection capabilities. To maintain the highest level of protection, configure your antivirus software to automatically check for updates as often as it will allow.

The University of Bayreuth offers antivirus software to all members. Sophos Antivirus Software is available as a free download. For home use, there are a wide range of free antivirus products available such as Microsoft's Windows Defender - integrated into Windows 8 - or Microsoft Security Essentials for Windows 7 / Vista / XP.

Vigilant browsing behaviour

3 Spyware lurks in many corners of the Internet and browsing can quickly compromise your safety. Phishing websites mimic banking or shopping websites and put your computer and personal information at risk. Certain sites are more prone to be a source of spyware than others. Among such are, adult sites, file sharing sites, and social networking sites, but even untended websites can pose a risk. Danger also lurks in: suspicious ads and pop-ups, links in spam messages, clickable graphics, alleged profit promises or messages like "your computer is too slow/infected, please Click Here." Don't! In regard to Internet clicks, less is more.

If it sounds too good to be true...

Always up-to-date: www.bsi.bund.de

Keep your system up-to-date

4 Keeping your computer up-to-date is very important. Microsoft and other software vendors frequently identify security gaps and stability problems in their distributed software. When this happens, they typically release "updates" and "patches" for the affected operating system or application to fix security issues and other reported bugs. Failing to update insecure software could allow attackers access to your computer through an unpatched security hole. To ensure the latest security and other important updates are installed on your system, we recommend that you switch automatic updating to "on".

Schedule Backups

5 In case of a malware infection, sudden hardware failure, accidental deletion, fire, theft, water damage, and other such catastrophes, scheduled full or incremental backups ensure that your sensitive, confidential, and critical data is protected and accessible with minimal interruption. Before a worst-case scenario occurs, create a backup plan and stick to it. Consider one of our campus storage options, an external hard drive, or NAS (Network Attached Storage) best located in a geographically dispersed area for maximum protection. Flash drives are not a backup media.

Identifying Fraud

6 Detecting online fraud as well as identifying email phishing schemes demands constant awareness. How often have you received emails written with poor grammar and spelling mistakes, which offer you millions in exchange for a small fee. Protect yourself: Be skeptical of unknown senders and do not respond to an unknown source! Don't be fooled by personalized emails! Read the email carefully! Use common sense! Do not click on contained links and never open enclosed attachments! Phishing emails are getting more and more sophisticated. But by rule of thumb: If it looks too good to be true, it probably is!

Behavior if infection is suspected

7 If you suspect your computer is infected with malicious software, disconnect your computer from its direct Ethernet connection (wall plug) or disable your wireless adapter, power down the computer in an orderly manner and immediately contact your IT-Servicezentrum. There, a friendly team of qualified specialist will gladly help you completely disinfect your system.

...to more *safety*.