SecurityBestPractices

Information Security - Best Practices

Check suspicious files: doc[x], xls[x], pdf, ...

Files receveived from untrusted sender, could be easily checked for viruses online under:

https://virustotal.com

Virus / Trojaner / Keylogger / ...

Anti virus software:

- Windows: Defender (built in since Windows 8)
- Mac OS X: https://www.avast.com, https://www.bitdefender.de
- Linux: https://help.ubuntu.com/community/Antivirus

Password Security

- **Don't tell your password to other people!** Just don't do it!
- **Never, ever send a password by email!**
- If an email which looks authentic asks you to log in on a website, it may still be fake. Check by asking the IT crew personally.
- If you enter a password, try keeping in mind if someone is watching you.

- A lot of damages can be done with the knowledge of your password. The argument 'I have nothing to hide' is useless if someone charges your bank account against your will.
- When choosing a password, keep a good balance between a password which you can remember easily, but others cannot guess easily: use upper case / lower case / digits / special characters. Approximately 10 characters long.
- **Don't** write your password down.
- If you absolutely must write your password down, keep the note in a secure location where others cannot access it (e.g. your wallet or a safe). Never put the note somewhere visible.
- Use password managment tools (like e.g. KeePassX).

email Security

- **Never ever send a password by email!** Just don't do it!
- Some emails try to make you believe that you should either click on a particular link, visit a certain page, set a new password or reply to the sender.
- If you don't know the sender or didn't expect the Email, be careful! If in doubt, ask your IT crew.
- Never trust an Email just by knowing the sender address.
- Emails can easily be spied on. Emails are more secure if sender and receiver are both I-MATH addresses.
- If an email clearly is spam, don't click on any link and don't reply to the email. Just delete it.

File Exchange Security

- When exchanging files with another person from the institute, use "the box". It is more secure and faster than methods over the internet.
- When sharing files about teaching, use /scratch/share/veranstaltungen .
- When sharing files about administration, use /scratch/share/institut .

Working from remote locations

- If you are working at remote locations (public places), try doing as few sensible tasks as possible. (I.e. don't access critical data or log into accounts if it is not necessary). This is especially true if connecting to an unencrypted (open) wireless spot.
- If you log in somewhere (e.g. your email account or similar), the browser may ask you if you want to save the username and password. Think before you click, and click "No, don't

save!".
- In public internet cafes, everything you type (including your password!) may be protocolled.
- While traveling, take your own laptop or a laptop of I-MATH with you, rather than relying on other hardware.

Browsing Security

- Keep an eye open for fake URL's (phishing sites). Some letters look very similar (e.g. 0/O/o, l/1/I, etc. In particular, the extensions .ch and .cn look very similar)
- Don't click on advertisements. Even very reputable websites (like the homepage of a newspaper or tv-channel) can contain fake advertisements which try to harm your computer if you click on it.
- In particular: don't click on advertisements which tell you that your computer "might be infected/in danger" or similar. These advertisements are mostly infectious itself.
- If your browser warns you that a security certificate doesn't match, be cautious.

General

- Contrary to popular belief, the weakest point in a security context is usually the human.
- Almost always there is a contrast between security and usability. (Typical example: password '1234' written on a sticky note versus a randomly generated password learned by heart)
- When thinking in a context of IT security, it is better to worry than to be sorry.
- Almost by definition there is no perfectly secure system. Therefore, IT security is based on "trust". If doing sensible tasks (like entering your password) you should trust your hardware and your network connection.
- If in doubt, ask your IT crew.

Revision #2
Created 2026-06-30 10:52:21 CEST by admino
Updated 2026-07-01 14:22:02 CEST by Jonas Valentin Rose