Fundamentals of cyber-security

DO	DO NOT
Do use a strongpassword and change it if you think it may have been compromised	Don’t give your password to anyone
Do report any loss or suspected loss of data	Don’t reuse your University password for any other account
Do be on your guard for fake emails or phone calls requesting confidential information - report anything suspicious to the DD&T service desk at abuse@cuni.cz	Don’t open suspicious documents or links
Do keep software up to date and use antivirus on all possible devices	Don’t undermine the security of University systems
Do be mindful of risks using public Wi-Fi or computers	Don’t provide access to University information or systems
Do ensure University data is stored on University systems	Don’t copy confidential University information without permission
Do password protect and encrypt your personally owned devices	Don’t leave your computers or phones unlocked

Login data

Although data security on network and cloud storage is at a high level, the weakest link is usually the end user or the method of authentication: If you use a weak password/a password shared with other services, etc. for access, and the password is the only element of authentication, then disclosing the password to an unauthorized person will compromise the security of all data and services to which you have access.

You should never enter access information to work data into other people’s computers (in a café, at a friend’s house, etc.) for which you have no knowledge or guarantee of their security. Use your own laptops, phones, etc.

To be able to use strong passwords unique to each service, it could be helpful to use a quality password manager.

Private computers used for work

Home computers or other devices used to access work data should be subject to the same security requirements as work computers. Few people have a camera system or a gatehouse with 24/7 surveillance at home, so **pay extra attention to physical security during your absence** (e.g. when you are at work).

Don’t forget about your children, who may not only forget to lock up when they leave the house, but will often use the home computer together with you – strict **separation of user accounts on the computer for work and personal purposes** and inaccessibility of administrator privileges for children on a shared computer should be a matter of course. You should also install quality **antivirus and antimalware software and firewalls**.

Avoid installing games and suspicious software on the computer you use for work. Only **install trusted software** that you have authenticated. Think about software configuration (for example, antivirus programs often automatically send files they think suspicious to their manufacturer – in such a way, data could be sent from your computer without your knowledge that should not fall into the hands of a third party).

Remember: you do not have to protect any data that are not on your home computer – leave your work data on network and cloud storage, and download only **the minimum amount of data to your home computer for as short a period as possible**. If possible, always encrypt protected data.

Obligation to report the loss of work devices

Based on the instruction of the data protection officer, **you are required to report to the officer any loss or theft of any device or data medium that may allow access to personal or sensitive data for which CU is responsible**. This instruction applies to any device from which data can be retrieved, for example, by breaking the protection (password) or removing the disk and retrieving the data itself or passwords for accessing the university’s systems. Typically, this is a laptop, tablet, computer from the office, or even a mobile phone with access data. The loss should be reported as soon as possible by the employee who discovered it or by their superior to the e-mail address gdpr@cuni.cz .

Reporting security incidents

Coordination for **resolving security incidents in the university networks** has been handled since 2015 by a **security team for the Charles University computer network** CSIRT-CUNI . You should send security incident reports according to the instructions by e-mail to abuse@cuni.cz .