Safe login to CU environment

Login is the gateway to all university systems - from the Study Information System to email.
A little carelessness and someone can gain access to your personal and study data.
Therefore, stick to a few simple rules to protect your account and data.

Always log in safely
Most Charles University services use central CAS authentication to log in.
Log in **only through the official website of the University**. Use links from emails or messages only if you are sure of their origin and always check the address of the page you are logging in to.
In the address bar, check whether the page starts with **https://** and belongs to the **cuni.cz** domain.
Never share your login details with anyone, not even IT staff.
Use a **strong and unique CAS password** and change it regularly.

Use two-factor authentication
For even greater security, you can protect your account with two-factor authentication .
During login, password confirmation is required in a second way – via the mobile application. This prevents account misuse even if someone has obtained your password.
At Charles University, the **mobile app CU Key** is used for this, which is available for free for both Android and iOS.
After activation, the app simply asks you to confirm access when you login - just one click.
For more information and the activation procedure, click here .

Frequently Asked Questions (FAQ)
What is CAS and why do I need to use it?
- CAS (Central Authentication Service) is the CU's single login system.
- Thanks to it, you login to multiple services with one account – SIS, email, Microsoft 365, Intranet etc.

How do I know if I am on a fake login page?
- Check the page address - it must start at **https://**, contain the **cuni.cz** domain and display a key/lock icon.
- If the link looks different (e.g. " cuni-login.net "), close the page immediately.

What if I accidentally entered my password on a suspicious page?
- Change your CAS password immediately and contact the faculty IT administrator or the CU helpdesk.

Do I need to use two-factor authentication?
- It is voluntary for now, but strongly recommended - it protects your account from most common attacks.

Is it safe to log in to university services outside of the university?
- Yes, if you use a secure network and log in through an official website.

Can the university see what's in my personal laptop?
- No. The university only sees access to its services, not your private data.

How do I report a security incident?
- If you suspect a security incident, contact the CU cybersecurity team immediately.