Identity & personal data protection

Your university identity is the key to all Charles University services – from email and SIS access to Wi-Fi and cloud tools. If someone gets their hands on it illegally, they can use it to steal data, send fraudulent messages on your behalf, or access internal systems.

Therefore, protect your digital identity as carefully as your ID card or bank card.
In the online environment, caution is not mistrust, but a healthy habit.

Be careful when publishing information on the internet.
Consider what you are publicly posting about yourself on the Internet.
Never publish
- birth date, ID number or personal documents,
- scanned contracts, confirmation of study, etc.,
- login details or passwords in text files/emails.

What to NEVER share
Not even with a colleague. Not even "just for a minute". Not even if someone writes to you that they are from IT support.
Never share
- your CAS password (or part of it),
- login details to the email address,
- authentication codes or SMS,
- access to your laptop or mobile phone,
- internal university documents that contain personal data.

Safe identity handling
Log in **only via official university websites and apps**.
Recommended procedures
- Do not use a university account on unknown or untrusted network.
- Always log out and lock your device when you have finished work.

Beware of fake login pages
Attackers often mimic the login page to: **CAS, Microsoft 365/Teams** or university **email**.
How to recognize them
- Always verify that the address begins with **https://** and contains a **cuni.cz** domain or other official domain before entering your password.
- If the page looks unusual or missing key elements, do not fill anything.
- If the page redirects you to an unknown address or looks different than usual, log out immediately and contact IT support.

What to do if you suspect your account is being misused?

Immediately change your CAS password .
Contact your faculty IT support.
Report an incident on the Security Incident Reporting page.
Frequently Asked Questions (FAQ)

Can I also use university email for personal purposes?

- We recommend not to do this. University email is intended solely for work and study communication.

How do I know if someone has logged into my email account?

- You find messages in Ougoing emails that you have not sent
- All emails from Sent folder have mysteriously disappeared.
- You have not received any email for a long time and you find a rule in your email settings that deletes all incoming emails or forwards them to an unknown address and you are sure that you have not set such a rule yourself.

I have received an email to verify my CAS login. What should I do?

- Ignore the message and do not click on any links. University does not normally send verification emails – login always takes place directly at ldap.cuni.cz

What if I have given away the password or discovered that someone has logged into my account?

- Immediately Change your password . Inform IT support and ask for an account check. Changing your password alone may not cut off the attacker from your account.

How to protect your identity in 5 points
Log in only through the official CU websites.

Be careful about what you share publicly.
Do not write or share passwords.

Do not use a university account on unknown network.
If you suspect something, act now – change your password and report the incident.