Basic rules of safe online behavior

Cybersecurity is not just about technology – our everyday behaviour plays the most important role.
Most security incidents are not due to complex attacks, but to minor inattention - for example, clicking on a fraudulent link or using a weak password.
The good news is that protecting your account and data does not need to be complicated. Adopt a few basic habits that will significantly reduce the risk of misuse and help you use university systems and the internet in general safely.

Use strong and unique passwords
Your password is like an apartment key – don't leave it to a stranger and don't use the same for multiple doors.
Create longer passwords (at least 12 characters) and combine letters, numbers and special characters.
Never share your password with anyone – not IT staff or colleagues.

Update your devices
Updates aren't just about new features – they also fix bugs that attackers can exploit. Turn on automatic updates so your computer and mobile are always protected.

Watch out for suspicious emails
Phishing emails often appear as messages from colleagues, banks or universities. If you find something suspicious - such as an unexpected login request or an attachment from an unknown sender - you should not open the message and report it to local IT support.

Install software only from verified sources
Avoid unknown apps or downloadable links from unofficial websites.
Use software approved or provided by your faculty on university computers.

Work only on secure Wi-Fi networks
When working with university systems, only connect to secure networks – such as Eduroam . Use public Wi-Fi networks (e.g. in a café or railway station) only rarely and never to access sensitive data.

Lock your device when you leave
Whether it's an office computer, a laptop or a mobile phone – always lock it when you leave the desk. This protects not only yourself, but also university data.

These simple steps can significantly reduce the risk of account hacking, data leaking, or device misuse. University security starts with each of us.

Do you need advice or report a security incident?

Detailed procedure can be found in the Security Incident Reporting section , where you will learn how to describe the incident, to whom to send it and how the solution is progressing.

Frequently Asked Questions (FAQ)

How do I know if an email is fake?

- Suspicious sender address, urgent tone "forces you to act immediately", email text contains errors, unknown links or attachments - these are all warning signs.

What should I do if I receive a suspicious email?

- Do not open links or attachments. Send it to faculty IT support or report the security incident.
- Detailed procedure can be found in the Security Incident Reporting section , where you will learn how to describe the incident, to whom to send it and how the solution is progressing.

What to do if I suspect someone has got my password?

- Change your password immediately (in CAS or the relevant system) and inform the faculty IT administrator.

Can I use the same password for a university and personal account?

- Absolutely not. Each environment should have its own password.

Is it safe to operate over public Wi-Fi when I use a VPN?

- VPN reduces but does not remove the risk. If possible, use the Eduroam university network or your own mobile hot spot.

Can I use a university account on personal devices?

- Yes - but the device must be updated and secure.

Important links

More information, current threats , recommendations and documents related to cybersecurity:

- Dangerous emails
- Dangerous websites
- Treacherous passwords
- What to protect the most
- Documents and instructions on cybersecurity
- Useful links for solving security problems