Internet risks and how to recognize them

The Internet offers many possibilities – from studying to communicating to working.
But it is also a place where various traps lurk: fraudulent emails, malicious links or viruses. One moment of inattention and your data, passwords or devices could be in danger.

On this page you will find an overview of the most common types of attacks, how to recognize them and how to avoid them. You can find current warnings about attacks, recommendations and an overview of typical frauds in the section Current Threats on the ICT .

Phishing - when someone is "baiting you"

Most often fraudsters pose as a university, bank, transport service or other trustworthy institution. The aim is to lure you out of your login details, card number or other sensitive information.
How do you recognize Phishing?
- The message pushes you to take immediate action (e.g. "renew your account", "click now" or "threat of being blocked").
- The link leads to a suspicious or unknown address - often it is only slightly different (e.g. **cuni-login.net** instead of **cuni.cz**)
- The seemingly official email contains grammatical errors, strange phrases, or logical nonsense.
- The sender wants your password, card number, or other private information.

Most common types
- email
- text message
- social platforms

How to defend yourself?
- Never click on links in suspicious emails.
- Never enter passwords outside of official login pages.
- Never share your password with anyone.
- If unsure, forward the email to faculty support - better safe than sorry.

Malware - viruses, spyware, ransomware

Malware is malicious software that can get into your device in order to damage it or steal data.
Most common types
- **Viruses** - spreads through infected files, flash drives, or email attachments.
- **Spyware** - tracks what you do, collects data, and sends data to attackers.
- **Ransomware** - locks your files and demands a ransom for unlocking them.

How to protect yourself?
- Use an **up-to-date anti-virus program** and have automatic updates turned on.
- Do not install programs from unknown sites.
- Do not open attachments from people you don't know - even if it "looks trustworthy."

Spam - junk mail

Spam is junk email that may contain annoying advertising, links to fraudulent sites or malicious attachments.
How to recognize it?
- Suspicious sender's address or a meaningless domain,
- spelling errors and unusual wording,
- links that point to an address other than the one visible when you hover the mouse over it.

How to deal with it?
- Do not open spam, do not delete it manually - use the "Mark as spam" feature.
- Never react or click on "unsubscribe" links if you are not sure where the email comes from.

- Update junk mail filters - most email services do this automatically.

Fraudulent attachments

Never open attachments from unknown senders, they may contain malicious software. They are used to install malware, ransomware or steal data.
How to recognize them?
- They contain suspicious extensions: .exe, .scr, .rar, .vbs or doubled as .pdf.exe.
- Unexpected message: a document arrived that you did not order/expect.
- Pressure: threat of execution, disconnection of services.

How to proceed on suspicion?
- **Do not open**: do not download an attachment and do not click on anything.
- **Verify**: contact the sender by other means (e.g. by phone)
- **Report/Delete**: Report an email as phishing and delete it.
- **Secure**: if you have opened an attachment, run antivirus protection.

Fake websites

They look like the original, but they steal data.
In fact, they are designed only for you to enter your login credentials, which the attacker then immediately retrieves.
How can you tell?
- Suspicious URL: often differs only in one letter or domain.
- Missing **https//:** and certificates: a key/padlock icon in the address bar indicates encryption.
- Grammar errors: a common character is bad grammar and stylistic errors.
- Missing contacts: a fraudulent website is not interested in communication, no phone number or company headquarters is given.

Fraudulent competitions and investment offers

"You've won a new iPhone!" or "Grow your savings by 500% in a week!" Sounds tempting - but in reality it's almost always a fraud.
How to not get scammed?
- If the offer is "too good to be true" it's usually not true.
- Never send money or personal data to unknown entities.
- Always check with e-shops that they use a secure connection (https://) and have real contact details.

Social engineering - when your attacker is manipulating you

Not all attacks are technical - often the attacker exploits our credulity or efforts to help.
What does it look like?
- Someone calls you claiming to be from IT support - and needs your password.
- Someone impersonates a manager/colleague who "quickly needs" access to a document.
- You get an email with the university logo and a request to "check your account".

How to respond?
- Never provide a password, PIN or other access details - IT support will NEVER ask you for them.
- If you are unsure, check the situation through official channels (by phone, in person or via university email).

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)

I have received an email with the CU logo, but something about it doesn't add up. What should I do?

- Check the sender's address. If it doesn't end with **@cuni.cz** or looks suspicious, don't open the email and report it to IT support.

How do I recognise a fake website?

- Check the address – it should start with https:// and belong to the .cuni.cz domain or other official domain of the institution.

Should I click on the "Account Recovery" link that came in my email?

- No! Never enter your login details via links in emails. Always log in manually via the official CU website.

What should I do if I click on a suspicious link or open an attachment?

- Disconnect your device from the internet immediately, run an anti-virus test and contact IT support.

How can I prevent the receiving of so much spam?

- Use university email and do not post your address publicly on websites or forums.
- Do not fill in forms on unverified sites and use spam filters.

How to defend against online attacks in 5 points
Check where messages come from
Check the sender's address – if it is your colleague by name, but the address does not actually end with cuni.cz, be careful.

Watch out for suspicious links
Never click on links in emails that look suspicious. Always log in via the CU official website.
Don't share your passwords
Even IT staff will never ask you for a password. If someone asks for one, it's a scam.

Update your device
Regular updates protect your computer and mobile from attacks and viruses.
If you're not sure – don't click!
Better check your message with IT support. Caution always pays off.