Device protection

Your devices - computer, laptop, tablet or phone - are the gateway to university systems. One click on a fraudulent link or not updated program and the attacker can gain access to your data and account.

Workplace computer and laptop security is usually provided centrally by the IT workplace of the faculty or unit. Therefore, the instructions below apply primarily to your **private computers, tablets and phones**, regardless of whether you use them for study or work purposes.
Fortunately, most threats are easily fended off with a few simple steps.

Updates = basis of safety
Updates aren't just about "new features" - they often prevent attacks and fix security bugs that attackers exploit.
Turn on **automatic system updates** (Windows, macOS, Android, iOS).
Update apps regularly – especially your **browser, Adobe Reader, Microsoft Office, Zoom** or other programs in use.
Don't leave the "install later" message long-displayed - this is when the computer is most vulnerable.

Antivirus protection and firewall
Basic protection is provided by anti-virus programs and firewall.
For the average user, **Windows Defender**, which is part of Windows and is updated automatically, is quite sufficient.
On work (university) devices, anti-virus protection is set centrally by the IT workplace of the faculty or unit. Some faculties also offer their employees the option of installing faculty-managed antivirus software on their private laptops – however, the availability of this service varies, so it is always advisable to contact your faculty's IT support.
Always keep your firewall on – it prevents unwanted communication between your computer and extraneous servers.
Tip: Run a "Quick Check" once in a while with an antivirus, especially after connecting an unknown USB drive.

Strong and unique password for the device
Even the best antivirus won't help if the device has a weak password.
Use a password of at least 12 characters in length (combinations of letters, numbers and symbols).
Avoid passwords like "pass123", "student" or "123456".
Never use the same password for a work account and for a private personal account.
Consider using a **password manager** that will store strong passwords securely for you.

Mobile and laptop security
Mobile devices are often overlooked, yet include access to all accounts, emails and files.
Set up a **PIN, gesture, password or biometric authentication** (fingerprint, face).
Activate **automatic locking** after 30-60 seconds of inactivity.
Never leave a device unattended, especially in public places.
Consider **encrypting a laptop drive** – if someone steals it, they won't be able to access the data stored on it.

Safe connection
Be careful on public Wi-Fi networks (cafes, airports, trains). Ideally, connect to university services via VPN .
Don't use a public USB socket for charging and instead use a public 220V socket and your own USB charger.
If this is not possible, pay attention to any warnings that the connection is not trusted.
Do not log in to CAS or email while you are on an unsecured network.
Wi-Fi Eduroam is safer for users – it will not allow anyone to eavesdrop on your communications.

When a device is lost or stolen
Immediately change your password to CAS and any services that have been logged on in the device.
If Find My Device or **Find My iPhone** is turned on, try to locate or remotely delete the device.
Inform faculty IT support – they will help you secure your accounts and report an incident.

Frequently Asked Questions (FAQ)

Is it necessary to have an antivirus when I have a Mac or iPhone?

- Yes – although the risk is lower than with Windows, there is malware for both macOS and iOS. It is recommended to at least update your system regularly and not to install apps outside the App Store.

Do I need an antivirus, or do I need a firewall?

- Both. An antivirus protects against malicious files, while a firewall blocks unwanted connections from the internet.

Can I use public Wi-Fi in cafes?

- Yes, but with caution. Do not log on to internet banking or university systems. If you need to work, use a VPN .

I lost my mobile, where my university e-mail is – what should I do?

- Change your password to CAS immediately, report the event to faculty IT support, and if possible, activate remote device deletion.

How to protect your device in 5 points
If your device is lost, change your passwords immediately and report the incident.

Update your system and apps.
Use the antivirus and firewall turned on.

Lock your device when you leave.
Connect only to trusted networks.