

# Informace o počítačové síti v Karlíně

O síť a počítačové služby v Karlíně se starají tito IT správci:

Jméno	Kontakt (kancelář, telefon, e-mail)	Hlavní oblast
Jaroslav Richter	K381, 95155 3206, <a href="mailto:richter@karlin.mff.cuni.cz">richter@karlin.mff.cuni.cz</a>	Podpora uživatelů, zakládání účtů, registrace počítačů
Martin Trčka	K381, 95155 3237, <a href="mailto:trcka@karlin.mff.cuni.cz">trcka@karlin.mff.cuni.cz</a>	Počítačové učebny a lab K10
Oldřich Ulrych	K387, 95155 3216, <a href="mailto:ulrych@karlin.mff.cuni.cz">ulrych@karlin.mff.cuni.cz</a>	Síť a servery

(Pokud si nejste jisti, koho kontaktovat, obraťte se na libovolnou výše uvedenou osobu.)

## Služby pro učitele, zaměstnance, doktorandy, hosty

- počítačové učebny (K11, K4, K10A, K10B) – pro přístup do místností, pro zřízení učitelského uživatelského účtu (doména LABK) nebo pro instalaci softwaru -> Martin Trčka
- připojení k internetu přes Wi-Fi síť eduroam (přihlašovací údaje si každý musí nastavit sám v systému CAS: *Další účty* -> *Nastavit heslo pro eduroam realm cuni.cz*)
- připojení vašeho počítače do drátové sítě (registrace počítače) -> Jaroslav Richter
- karlínský uživatelský účet (doména MSEKCE, viz <https://www.mff.cuni.cz/cs/math/vnitri-zalezitosti/pocitace-a-technika/msekce>) -> Jaroslav Richter, účet nabízí:
  - možnost přihlásit se do stolních počítačů v karlínské budově (např. počítače v učebnách K1–K9 s výjimkou počítačové učebny K4)
  - e-mailovou schránku s adresou `jmeno@karlin.mff.cuni.cz` (IMAP/SMTP, nebo <https://webmail.karlin.mff.cuni.cz>)
  - možnost vlastních webových stránek
  - zálohovaný datový prostor
- dále na vyžádání (-> Jaroslav Richter) nabízíme:
  - vzdálený přístup na terminálový (Windows) nebo SSH (Linux) server
  - VPN (vzdálený přístup do místní sítě např. z domova)
- výpočetní cluster (a Git) – informace a založení účtu viz <https://cluster.karlin.mff.cuni.cz/>

Podrobnosti o těchto službách naleznete na: <https://www.mff.cuni.cz/cs/math> -> *Vnitřní záležitosti*.

## Poznámka týkající se bezpečnosti (phishing)

Žádný z karlínských IT správců nepotřebuje znát **heslo** k vašemu účtu a už vůbec o něj nebude žádat přes e-mail. Pokud vám tedy e-mailem přijde zpráva, abyste sdělili nebo na nějaké (pochybné) webové stránce zadali své přihlašovací údaje (protože jinak dojde do 24 hodin k zablokování nebo smazání všech vašich dat), půjde s největší pravděpodobností o podvod, tzv. phishing.

Jedinou výjimkou je univerzitní systém CAS, který jednou ročně připomene uživatelům, že za 14 dní dojde k expiraci jeho hesla a že si ho má na stránce <https://ldapuser.cuni.cz/account/password/nomenu/1> změnit. Ale u správce J. Richtera nebo O. Ulrycha si můžete i expirované heslo změnit (nebo alespoň platnost hesla prodloužit).

Pokud jste na pochybách, zda je nějaká e-mailová zpráva pravá, nebo zda jde o podvod, raději se s dotazem obraťte na libovolného z IT správců.

# Pravidla počítačové sítě UK a MFF (neoficiální shrnutí)

Shrnutí pravidel v jedné větě:

Připojete se do akademické počítačové sítě – chovejte se v ní slušně.

Uživatel je povinen:

1. Seznámit se s **pravidly** sítě, do které se připojuje; respektovat tato pravidla a pokyny příslušného správce.
2. Poskytnout součinnost při vytváření **uživatelského účtu** i při jeho případných úpravách; prokázat svou totožnost na výzvu správce; chránit svůj uživatelský účet před zneužitím.
3. Své **zařízení** (stolní počítač, notebook, mobilní telefon apod.) připojovat do sítě jen na vyhrazených místech a jen prostředky k tomu určenými (v některých případech je třeba zařízení před připojením registrovat u správce); za své zařízení uživatel plně odpovídá.
4. Pokud uživatel zjistí narušení **bezpečnosti** svého účtu nebo nějakého prvku sítě nebo počítačového systému UK, je povinen to nahlásit správci (dané sítě nebo systému), nebo univerzitnímu bezpečnostnímu týmu (abuse@cuni.cz).
5. Zaměstnanci jsou povinni pro pracovní záležitosti (včetně komunikace se studenty) používat výhradně **pracovní e-mailové účty** pod doménou "cuni.cz".

Uživatel při práci v síti nesmí:

6. Používat síť v rozporu s **posláním** UK (zakázána je reklama, politická a náboženská agitace a vše, co poškozuje dobré jméno UK).
7. Porušovat **zákony** (např. autorský zákon).
8. **Škodit** (zatěžovat neúměrně síť nebo servery, omezovat nebo obtěžovat jiné uživatele, poškozovat technické vybavení).
9. **Hackovat** (pokoušet se získat cizí práva, pracovat pod cizí identitou, měnit neoprávněně programy nebo nastavení, vytvářet škodlivé programy).
10. Připojovat k síti **jiné osoby** nebo nepovolené síťové prvky (např. switche nebo celé jiné sítě).

Uživatel bere na vědomí, že:

11. Správce **negarantuje** 100% funkčnost a nenesou právní odpovědnost za výpadky ani případnou ztrátu dat – ochrana (např. zálohování) je tedy plně v odpovědnosti uživatelů.
  - V Karlíně nicméně standardně všechny serverové (síťové) disky až na opodstatněné výjimky (např. pracovní adresář pro výpočetní cluster) zálohujeme.
12. Provoz sítě je v nutné míře **monitorován** za účelem řádného fungování sítě a předcházení bezpečnostním incidentům.

Podrobnosti (cca 23 normostran textu):

- [Opatření rektora č. 34/2017 \(Pravidla počítačové sítě Univerzity Karlovy\)](#)
- [Směrnice děkana č. 4/2018 \(Zásady pro provozování a používání výpočetní techniky zapojené do sítě MFF UK\)](#)
- Pokyny pověřence pro ochranu osobních údajů: [Pokyn č. 3 - Používání soukromých e-mailových adres](#)