Univerzita Hradec Králové
Filozofická fakulta

BEZPEČNOST A PŘIPOJOVÁNÍ

Financováno Evropskou unií
NextGenerationEU

Národní plán obnovy

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Tento materiál vznikl v rámci realizace projektu Rozvoj kapacit a adaptace na nové formy učení na UHK, reg. číslo: NPO_UHK_MSMT-16601/2022.

Financováno Evropskou unií
NextGenerationEU

Národní plán obnovy

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Bezpečnost a připojování

Začátek vaší akademické cesty na FF UHK je důležitým krokem. Aby váš přechod do univerzitního, a především digitálního života proběhl hladce, připravili jsme pro vás tohoto krátkého průvodce. Tato brožurka pokrývá základní témata jako přihlášení do našich systémů, přístup k univerzitnímu e-mailu a základy kybernetické bezpečnosti. Prostudujte si tyto sekce, abyste se naučili, jak chránit svůj univerzitní účet a bezpečně se pohybovat v digitálním prostředí.

Obsah

Každý student má svůj unikátní login. Ten obdrží na základě rozhodnutí o přijetí e-mailem společně s automaticky vygenerovaným heslem. Pokud máte problém se svým loginem nebo heslem, obraťte se prosím na Centrum služeb FF (viz sekce Připojení k Wi-Fi a pomoc).

Login

Každý login je zkratka uživatelova příjmení a křestního jména doplněná o číslo. Login slouží pro přihlášení do všech služeb poskytovaných UHK, jakými jsou například počítače v učebnách, univerzitní e-mail, Wi-Fi, online platformy (IS/STAG, Moodle, MS Teams) a další.

Při přihlašování se v některých případech používá samotné přihlašovací jméno, jindy je nutné použít e-mailovou adresu UHK ve stanoveném formátu. Zde jsou nejčastější případy použití s konkrétními příklady:

PC na učebnách	username1
IS/STAG	username1
Moodle	username1
MS Teams	username1@uhk.cz
UHK e-mail	username1@uhk.cz
Wi-Fi	username1@uhk.cz

Bezpečná hesla a jejich změna

Pro všechny UHK systémy budete využívat stejné heslo. Vaše automaticky vygenerované heslo obdržíte se svým loginem.

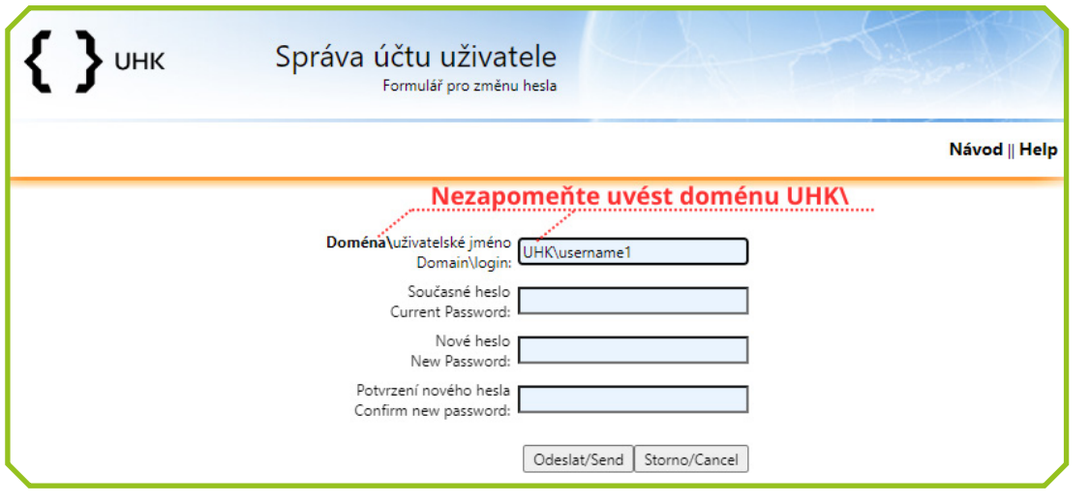
Použijte své původní heslo pouze při prvním přihlášení. Po něm jste povinni heslo ihned změnit!

Přihlašování do systémů UHK

Zde jsou požadavky na tvorbu nového hesla společně s obecnými doporučeními pro bezpečná hesla:

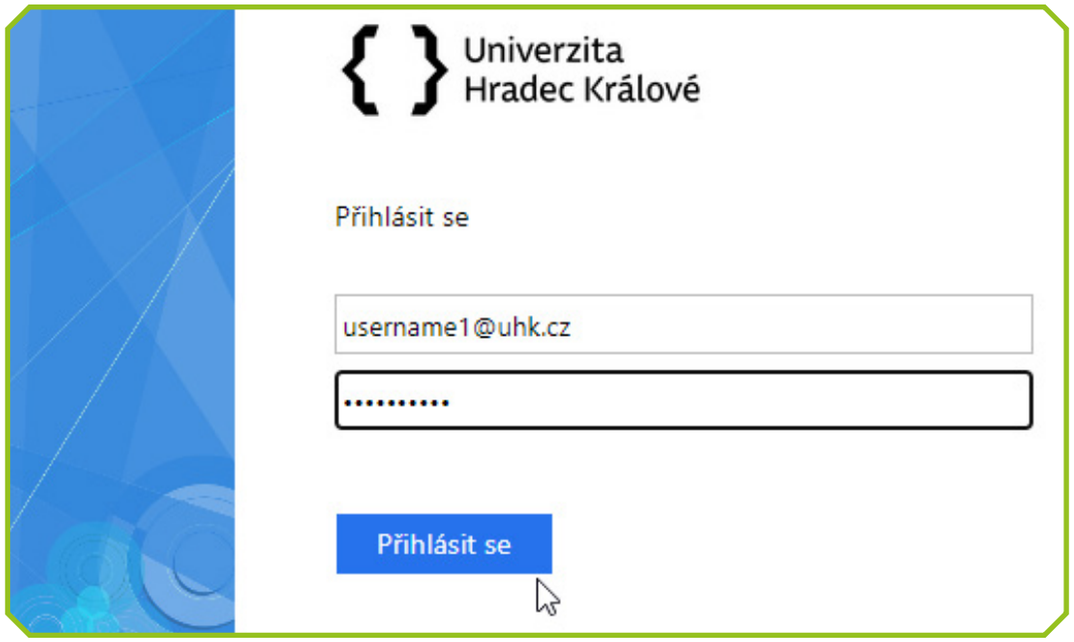
- **Písmena pouze z anglické abecedy** – zabrání problémům s přihlášením do určitých aplikací.
- Heslo musí obsahovat **alespoň 10 znaků.** Čím více, tím lépe.
- Použijte **alespoň jedno velké písmeno**. Nemělo by být na začátku!
- Zahrňte **alespoň jednu číslici**. Neměla by být na konci!
- Pokud chcete extra bezpečné heslo, použijte **speciální symboly** jako @, _ , ! atd.
- **Změňte heslo každých 180 dní**. Systém vás upozorní před vypršením platnosti.

Při změně hesla **vždy používejte pouze oficiální odkaz:**
http://www.uhk.cz/heslo



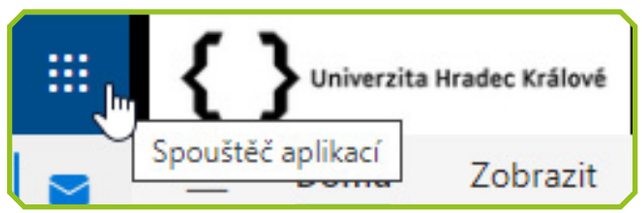
Obr. 1 –Změna hesla

Každý student má zřízen svůj vlastní univerzitní e-mail. Povinností každého studenta je tak tento e-mail pravidelně kontrolovat, protože se jedná o hlavní nástroj pro komunikaci s akademiky a dalšími univerzitními zaměstnanci. Nejčastěji studenti využívají svůj UHK e-mail prostřednictvím webového prohlížeče. Odkaz pro přihlášení naleznete na adrese: **https://outlook.com/uhk.cz**



Obr. 2 – Přihlášení do e-mailu UHK

Jakmile jste ve svém e-mailu otevřeném ve webovém prohlížeči, můžete přistupovat k dalším aplikacím Microsoft Office, jako je Teams, Word, Excel, OneDrive a další. Stačí přejít do nabídky v levém horním rohu viz obr. 3.



Obr. 3 – Spouštěč aplikací v UHK e-mailu

Alternativní metoda přístupu k UHK e-mailu.

Pro přístup k e-mailu můžete také využít aplikaci Outlook, která je dostupná ke stažení na váš počítač, tablet nebo telefon. Pokud již Outlook používáte a chcete přidat svůj UHK e-mail, návod naleznete na oficiální podpoře Microsoft.

Základní pravidlo kybernetické bezpečnosti je **nikdy nesdílet své přihlašovací údaje ani heslo s nikým dalším**. Toto pravidlo platí nejen pro univerzitní systémy, ale také pro další účty, jako jsou bankovní účty, sociální média a podobně. Vaše přihlašovací údaje jsou důvěrné; jejich sdílení může vést k neoprávněnému přístupu a ohrozit vaši bezpečnost a soukromí. Buďte ostražití a chraňte své údaje na všech platformách.

V digitálním prostředí se dříve či později setkáte s řadou kybernetických útoků. V dnešní době jich existuje mnoho typů, ale pro to, abyste zůstali v bezpečí, se obvykle stačí držet pár základních bodů:

1. **Buďte pozorní:** Pečlivě kontrolujte e-mailové adresy a odkazy na webové stránky. Pokud vypadají podezřele nebo obsahují chyby, může se jednat o útok.
2. **Pozor na urgentní výzvy:** Pokud na vás někdo tlačí do rychlé akce, nebo nabízí něco, co se zdá být jako příliš výhodná nabídka, radši udělejte krok zpět. Podvodníci často používají triky, aby vás přiměli jednat bez promýšlení.
3. **Hledejte chyby:** Pokud samotný text e-mailu nebo zprávy obsahuje gramatické či pravopisné chyby, může se jednat o útočníka. Legitimní organizace obvykle píší bez chyb.
4. **Dvojitá kontrola:** Před kliknutím na odkazy nebo stahováním dokumentů se ujistěte, že jsou bezpečné. Můžete také zkusit kontaktovat přímo organizaci přes její oficiální kontakty a zeptat se, co vám zasílá.

Abyste se ujistili, že se nestanete obětí útoku, je důležité se seznámit s tím, jak fungují. Zde je popis nejběžnějších typů útoků a informace, co dělat v případě, že se stanete obětí daného útoku:

Phishing

Co to je: Phishing spočívá v zasílání podvodných e-mailů nebo zpráv, které se tváří, že pochází od důvěryhodných zdrojů, aby vás oklamaly a přiměly sdílet důvěrné informace jakými jsou hesla, čísla platebních karet nebo další osobní údaje.

Co dělat: Ihned nahlaste pokus o phishing příslušné autoritě (např. IT podpoře), neklikejte na podezřelé odkazy a za žádnou cenu nesdělujte své osobní údaje. K nahlášení phishingu nebo spamu obecně přepošlete danou zprávu našim správcům na adresu spam@uhk.cz

Malware

Co to je: Malware, zkrácenina pro škodlivý (malicious) software, zahrnuje různé typy softwaru navržené k infiltrování nebo poškození počítačového systému včetně virů, trojských koní a ransomwaru.

Co dělat: Odpojte se od internetu, spusťte antivirový software k vyhledání a odstranění malwaru a nahlaste incident IT podpoře nebo expertovi na kyberbezpečnost.

Ransomware

Co to je: Ransomware je typ malwaru, který zašifruje vaše soubory, nebo uzamkne uživatelům přístup do jejich systému a následně požaduje platbu (obvykle v kryptoměně) za dešifrovací klíč nebo obnovení přístupu.

Co dělat: Odpojte infikované zařízení od sítě, okamžitě informujte IT podporu a ignorujte výzvy k zaplacení platby. Pokud máte k dispozici zálohu, můžete později obnovit data z ní.

Sociální inženýrství

Co to je: Sociální inženýrství využívá lidskou psychologii k oklamání jedinců za účelem získání důvěrných informací. To zahrnuje vytváření falešných profilů a vydávání se za někoho jiného. Útočník často disponuje základními informacemi o osobě, kterou se snaží napodobit.

Co dělat: Nahlaste incident IT podpoře nebo příslušné autoritě. Zjistěte si více o taktikách sociálního inženýrství, které se neustále vyvíjejí, abyste odhalili budoucí pokusy o útok.

Wi-Fi

Všechny budovy UHK, včetně kolejí a knihovny, jsou vybaveny Wi-Fi sítí Eduroam. Pro připojení stačí zadat své přihlašovací údaje ve formě univerzitní e-mailové adresy (např. username1@uhk.cz) a hesla. Pokud se vám nedaří připojit, ověřte si nastavení Wi-Fi, aby odpovídalo požadovaným parametrům.

Parametry pro manuální nastavení:

- Typ zabezpečení: **WPA2-podnikové**
- Typ šifrování: **AES**
- Metoda ověřování: **PEAP – EAP-MSCHAP v2**

Na přístupových bodech Wi-Fi sítě Eduroam je možné na jedno přihlašovací jméno připojit maximálně 3 zařízení.

Nejčastější problémy s připojením

1. **Špatné heslo –** Ověřte funkčnost svého hesla přihlášením do intranetu na webových stránkách UHK. Pokud se Eduroam po určité době odpojí, může to být způsobeno slabým signálem nebo chybným ovladačem Wi-Fi karty.

2. **Nelze se připojit nebo připojení vypadává –** Některé přístupové body (především ty, které jsou situovány ve studovnách/knihovnách) mohou být ve špičkách přetížené, což může vést ke ztrátě připojení.

3. **Obecné rady – Pokud máte problémy:**
   - Zkuste odebrat síť Eduroam a znovu spustit konfiguraci.

Připojení k Wi-Fi a pomoc

- Pro Windows 10: Klikněte na Start a vyberte Nastavení. Z následujícího menu klikněte na Síť a internet. Poté klikněte na Wi-Fi a „Spravovat známé sítě.“ V zobrazeném menu klikněte na Eduroam a vyberte Odebrat z místního menu. Poté síť znovu nakonfigurujte.
- Vypněte a znovu zapněte Wi-Fi; většina zařízení má pro tento účel ovládací tlačítko.
- Restartujte své zařízení.
- Vytvořte nový profil a zkuste nakonfigurovat připojení v něm.

Centrum služeb FF

Pokud máte technické problémy, kontaktujte Centrum služeb FF. Mohou vám pomoci se změnou hesla nebo odblokováním vašeho účtu UHK. Dále vám mohou pomoci s připojením k Wi-Fi nebo přidáním kreditu na vaši studentskou kartu, kterou můžete použít pro tisk a kopírování.

Kontakty:

E-mail: podpora.ff@uhk.cz
Tel.: +420 493 331 225
Místnost 21030, přízemí, budova B

Tento materiál vznikl v rámci realizace projektu Rozvoj kapacit a adaptace na nové formy učení na UHK, reg. číslo: NPO_UHK_MSMT-16601/2022.

Financováno Evropskou unií NextGenerationEU
Národní plán obnovy
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Univerzita
Hradec Králové
Filozofická
fakulta