University of
Hradec Králové
Philosophical
Faculty

# FIRST STEPS: ACCESS, E-MAIL, AND SECURITY ESSENTIALS FOR INTERNATIONAL STUDENTS

Funded by
the European Union
NextGenerationEU

CZECH
RECOVERY
PLAN

MINISTRY OF EDUCATION,
YOUTH AND SPORTS

This material was created within the implementation of the project Capacity Development and Adaptation to New Forms of Learning at UHK, Reg. No. NPO_UHK_MSMT-16601/2022.

Funded by the European Union
NextGenerationEU

CZECH RECOVERY PLAN

MŠMT
MINISTRY OF EDUCATION, YOUTH AND SPORTS

# First Steps

Embarking on your academic journey at our institution is an exciting step. To ensure a smooth transition into university life, we‘ve prepared a comprehensive guide to assist you. This brochure covers essential topics such as Login and Password security, UHK Email usage, and Cybersecurity basics. Dive into these sections to learn how to safeguard your university account and navigate the digital landscape securely.

**Welcome aboard, and let‘s embark on this journey together!**

# Table of Contents

Each student has their own unique login, which you should receive together with an automatically generated password from your coordinator before your arrival. In case that you did not receive it, please contact your coordinator.

## Login

Your login is an abbreviation of your last name, first name and a number. You will be using your login to log in to **all of the services provided by the UHK** such as the PCs in the classrooms, university e-mail, Wi-Fi, online platforms (IS/STAG, Moodle, MS Teams) and more.

While login in, in some instances you have to use the login itself, in other cases it must be used in the form of your UHK e-mail. Here are the most common use cases with specific examples:

| | |
|---|---|
| PC in classrooms | username1 |
| IS/STAG | username1 |
| Moodle | username1 |
| MS Teams | username1@uhk.cz |
| UHK e-mail | username1@uhk.cz |
| Wi-Fi | username1@uhk.cz |

## Password

You will use the same password for all the systems provided by the UHK. Your automatically generated password is in the form of: **UHK.birthdatecode** (e.g.: UHK.01511389AE).

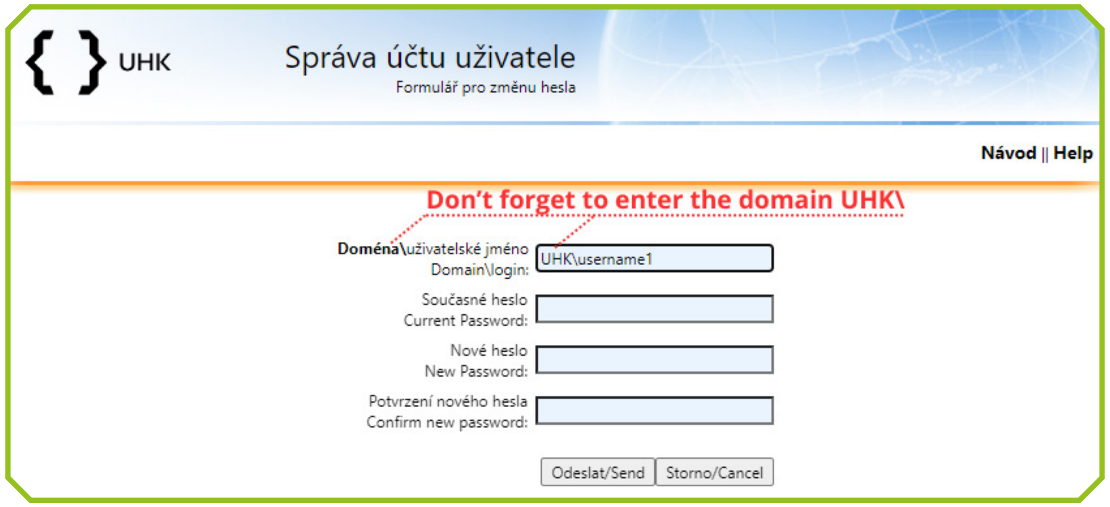
Use the original password only for the first login. **You are required to change your password immediately afterwards!**

**Here are the requirements for the password at UHK together with general recommendations for secure password:**

- **English letters only –** prevents login problems with certain apps.
- Password must contain of **at least 10 letters**. The more the better.
- Use **at least one capital letter**. It should not be at the beginning!
- Include **at least on number**. It should not be at the end!
- If you want your password extra safe, use **special symbol** such as @, _ , ! etc.
- **Change your password every 180 days**. The system will remind you before your password will expire.

When changing your password, **always do so through the official link: http://www.uhk.cz/heslo**.

You can as well access the site through the QR code:



Správa účtu uživatele

Formulář pro změnu hesla

Návod || Help

Don't forget to enter the domain UHK\

**Doména**\uživatelské jméno Domain\login: UHK\username1

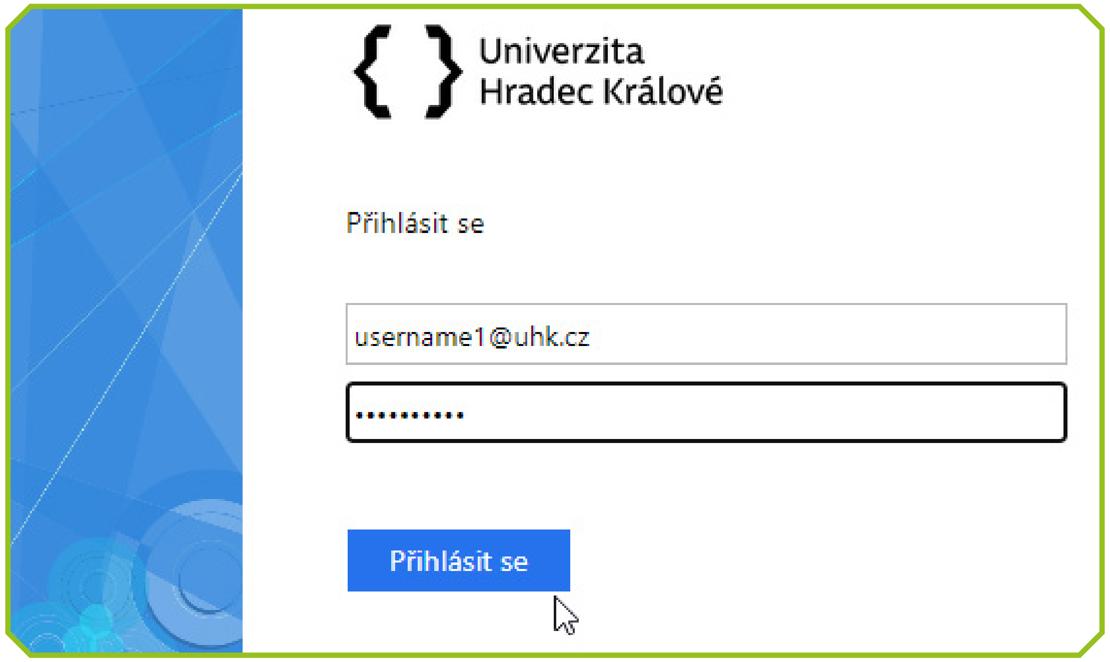
Současné heslo Current Password:

Nové heslo New Password:

Potvrzení nového hesla Confirm new password:

Fig. 1 – Password Change

Each student gets their own UHK email. You must check it regularly as it's the main way to talk to your coordinator, teachers, and university staff. Remember, this is the only email you should use for official university communication. The most common way for students to access their UHK email is through the browser, using Outlook. Access your UHK email here: **https://outlook.com/uhk.cz**.


Univerzita Hradec Králové

Přihlásit se

username1@uhk.cz

••••••••••

Přihlásit se

Fig. 2 – Logging into UHK e-mail

After your first login, your email interface will likely be in Czech. As an international student, your first step may be to change the language setting to your preferred language. To change the language, click on the gear icon on the top right.

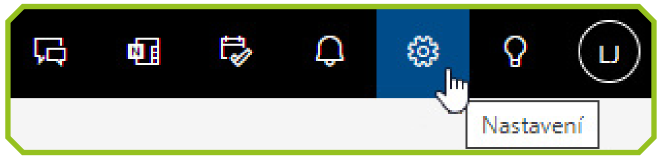


Fig. 3 – Detail of the upper right corner in the e-mail

Then click on the "Obecné" option in the displayed menu.

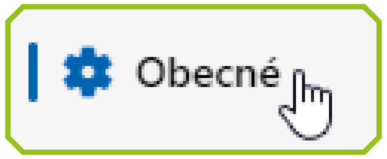
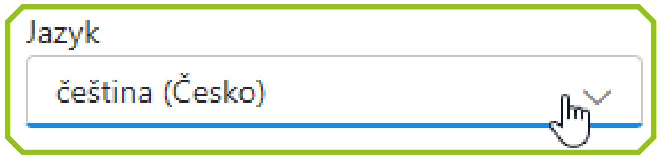


Fig. 4 – Obecné (General)

Subsequently, select any of the offered languages in the "Jazyk" drop-down menu.


Jazyk

čeština (Česko)

Fig. 5 – Language selection

Once you're in your email, you can access other Microsoft Office applications like Teams, Word, Excel, OneDrive, and more. Simply navigate to the menu in the upper left corner for easy access.

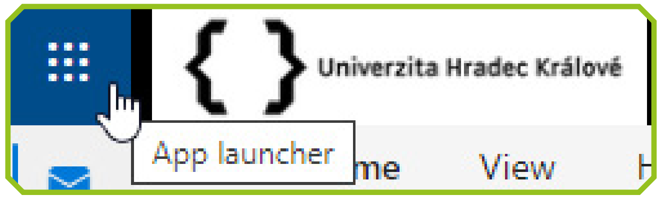


Fig. 6 – App launcher in UHK e-mail

## Alternative Method for UHK Email Access

You can also access your UHK email using the Outlook app, which is available for download on your computer, tablet, or phone. If you're already using the Outlook app and want to add your UHK email account, you can find guidance on how to do so through official Microsoft support.

The first rule of cybersecurity is **never to share your login or password with anyone**. This rule applies to university systems and other accounts like bank accounts, social media, and more. Your login details are confidential; sharing them can lead to unauthorized access and compromise your security and privacy. Stay vigilant and safeguard your credentials across all platforms.

As a user in a digital environment, you'll encounter various cyber-attacks sooner or later. Today, there are many types of attacks, but most of them share a few basic points.

1. **Check Carefully:** Look closely at email addresses and website links. If they look strange or include mistakes, be cautious.
2. **Beware of Urgent Messages:** If someone pressures you to act fast or offers something too good to be true, take a step back. Scammers often use tricks to make you act without thinking.
3. **Watch for Mistakes:** If emails have bad spelling or grammar, they might be scams. Legitimate organizations usually write clearly.
4. **Double-Check:** Before clicking on links or downloading anything, make sure they're safe. You can check with the official organization first.

To make sure you don't become a victim of an attack, it's a good idea to familiarize yourself with how they work. Here is a description of the most common types of attacks:

## Phishing

**What is it:** Phishing involves sending fraudulent emails or messages that appear to be from reputable sources in order to trick individuals into revealing sensitive information such as passwords, credit card numbers, or personal data.

**What to do:** Immediately report the phishing attempt to the appropriate authorities or IT support and avoid clicking on any suspicious links or providing personal information. To report phishing or even general spam, forward the given message to our administrator at the address **spam@uhk.cz**.

## Ransomware

**What is it:** Ransomware is a type of malware that encrypts files or locks users out of their systems, demanding payment (usually in cryptocurrency) for the decryption key or to restore access to the affected files or systems.

**What to do:** Disconnect infected devices from the network, notify IT support immediately, and avoid paying the ransom. Restore data from backups if available.

## Malware

**What is it:** Malware, short for malicious software, encompasses various types of software designed to infiltrate or damage a computer system, including viruses, worms, Trojans, and ransomware.

**What to do:** Disconnect from the internet, run antivirus software to scan and remove the malware, and report the incident to IT support or a cybersecurity expert.

## Social Engineering

**What is it:** Social engineering attacks exploit human psychology to deceive individuals into divulging confidential information or performing actions that compromise security. This can include techniques such as pretexting, baiting, or impersonation.

**What to do:** Report the incident to IT support or the appropriate authorities, and educate yourself and others about social engineering tactics to prevent future incidents.

This material was created within the implementation of the project Capacity Development and Adaptation to New Forms of Learning at UHK, Reg. No. NPO_UHK_MSMT-16601/2022.

Funded by the European Union NextGenerationEU

CZECH RECOVERY PLAN

MINISTRY OF EDUCATION, YOUTH AND SPORTS

University of
Hradec Králové
Philosophical
Faculty