Safer Login to Email and Microsoft 365 Services

Microsoft Authenticator Configuration

Take advantage of enhanced security for your account and email inbox by enabling multi-factor authentication (MFA) in Microsoft 365. This is a key tool for improving the security of your data and information.

Main Reasons to Use MFA:

1. **Increased Security**: MFA significantly reduces the risk of data breaches by requiring more than one form of authentication. Even if a password is compromised, an attacker will still not be able to access the account.
2. **Flexibility**: Microsoft 365 MFA currently offers various authentication methods, including text messages, mobile apps, and authentication tokens. This allows users to choose the most convenient method for them.
3. **Easy Implementation**: MFA is easy to set up and does not require any special technical skills. If any issues arise, support staff from the Service Center or IT department are available to assist you.
4. **Compatibility**: MFA is compatible with most devices and platforms, including mobile phones, tablets, and computers.

How to Activate Multi-Factor Authentication

1. Visit the security settings page at https://mysignins.microsoft.com/security-info, where multiple security methods are available. You can select multiple methods under the **"Add a method"** option.
2. **We strongly recommend setting up the Microsoft Authenticator mobile app.**
   - The app is free, easy to set up, and simple to use.
   - It requires a smartphone with Android or iOS.
   - To make setup easier, you can scan the provided QR code from this guide.

Google Play

App Store

!! Before installing, verify that the app is published by Microsoft Corporation, the name matches "Microsoft Authenticator," and the icon is correct.

3. Install the app on your mobile device. The setup steps will be displayed in the app. At the end of the process, you will see a QR code, which you will scan from your device when prompted during setup.
4. Add your work or school account to the Microsoft Authenticator app and scan the QR code from the Microsoft 365 security portal.
5. **Set up an additional backup authentication method** on the webpage mentioned in Step 1, such as SMS verification. You can also install the Microsoft Authenticator app on another device, such as a tablet. Follow the instructions in the Microsoft 365 security portal.
6. **Request activation of multi-factor authentication.**
    - This is a crucial step. MFA will only be activated after this request.
    - Join the **MFA-Activation team** in Microsoft Teams using the code **ivj5agi**.
    - You will receive a confirmation email upon being added to the group. This is for informational purposes only—no further action is required.
7. Your request will be processed, and you will receive a confirmation email along with additional details about multi-factor authentication in Microsoft 365.
8. **Once MFA is activated**, logging into Microsoft 365 services (Outlook, webmail, MS Teams, SharePoint Online, etc.) will require authentication via the Microsoft Authenticator app or an alternative verification method. **E-learning platforms such as Blackboard Learn will also require MFA verification.**

When is Multi-Factor Authentication Required?

MFA will be required based on various security criteria, including:

- The **first time you log in** to an application or web service after MFA activation.
- When **logging in on a new device**.
- When **logging in from an unknown location**.
- When using an **unusual login method** (e.g., a rarely used application).
- **Occasionally**, as a random security check to ensure the device is being used by the legitimate owner.

If you encounter any issues with activation, please contact the IT Department via the helpdesk:
https://helpdesk-it.uhk.cz/