Enabling two-step verification in your Microsoft® 365 account

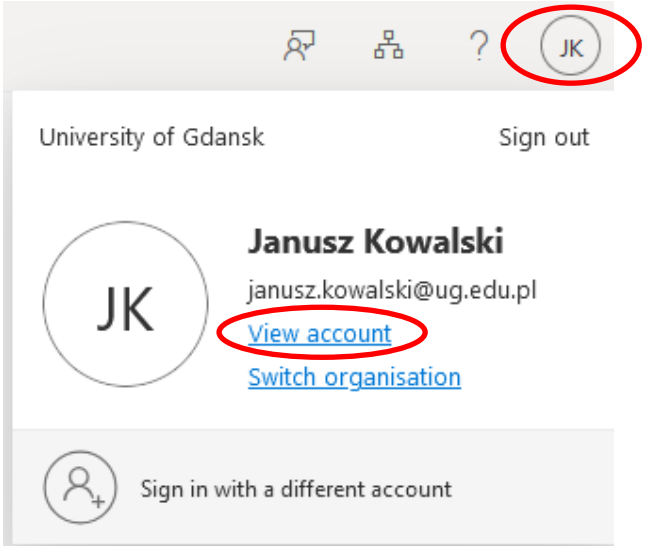
What is two-step verification?

Two-step verification (sometimes called multi-factor authentication) helps protect you by making it harder for others to log into your Microsoft account.
It uses two forms of identity verification: a password and a contact method (also called security information). Even when another person finds your password, they will not be able to log in unless they have access to your other security information. For this reason, it is important to use different passwords for each account.
So to increase your account security, you can set up a two-step login requirement.

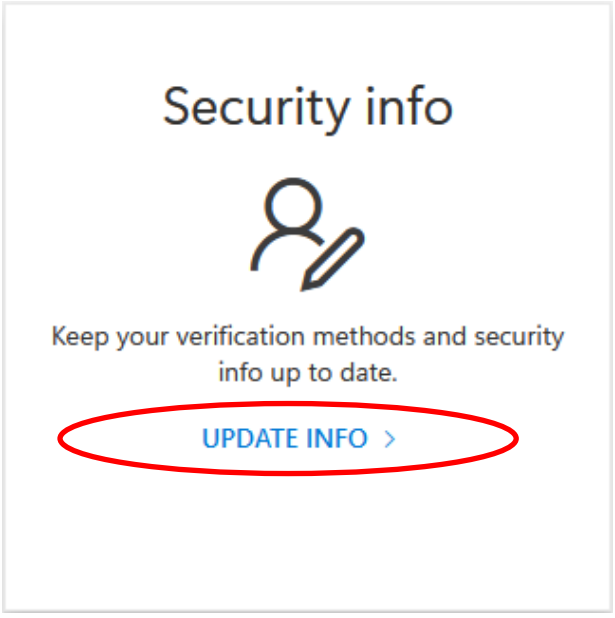
How do I enable two-step verification?

NOTE: During setup, you need two devices: a computer where you launch a browser to log in to your personal account, and a mobile device, e.g., a phone, where you install the Microsoft Authenticator® application, which is needed to scan the QR code from the browser window on your computer.

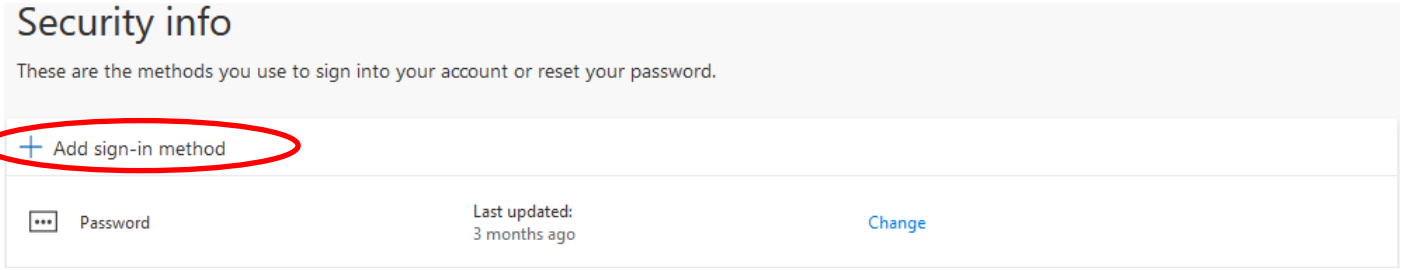
1 Log in to your **Microsoft®** account via any browser (e.g.: Microsoft **Edge®**, **Firefox®**) by going to https://office.com/. Then in the top right corner or bottom left corner of the browser, you need to click on the circle with our initials from our first and last name - then a menu will appear with the option 'View Account'.



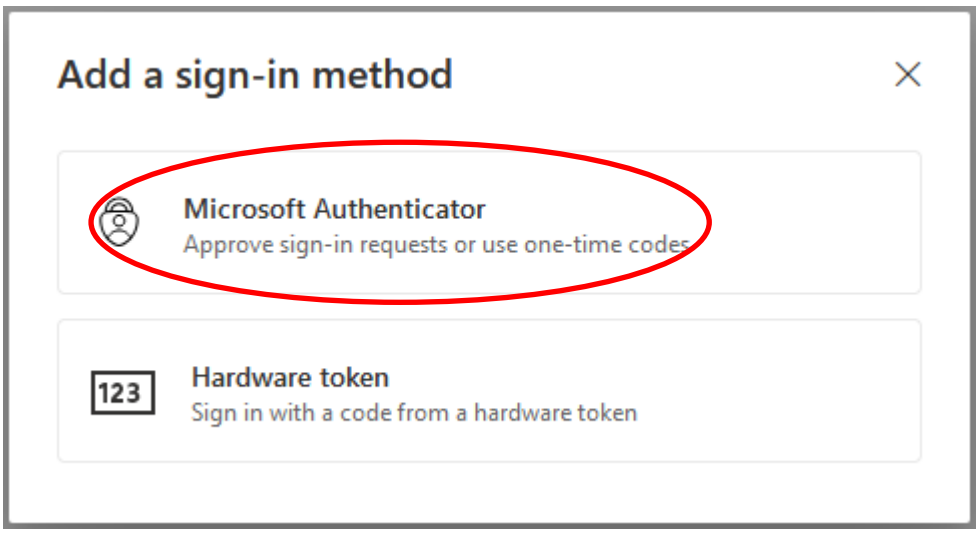
2 We are then redirected to https://myaccount.microsoft.com/?ref=MeControl where we click on the 'Security information' -> 'Update information' window.

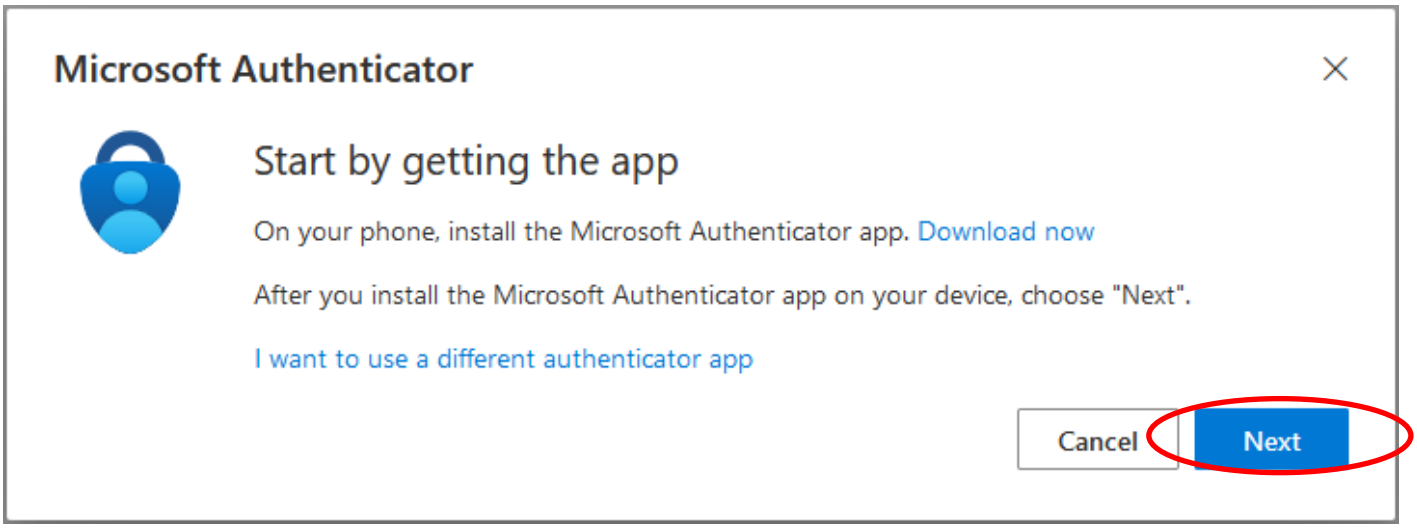


3 A new page will appear (https://mysignins.microsoft.com/security-info) where we have the option of adding a new login method 'Add login method'.



We select the "Microsoft Authenticator" option.



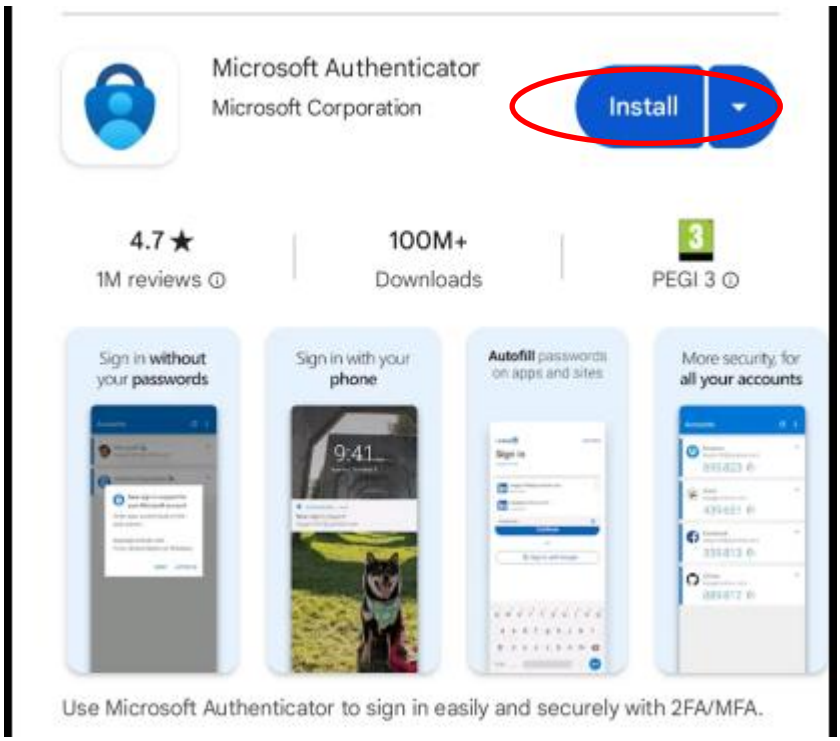


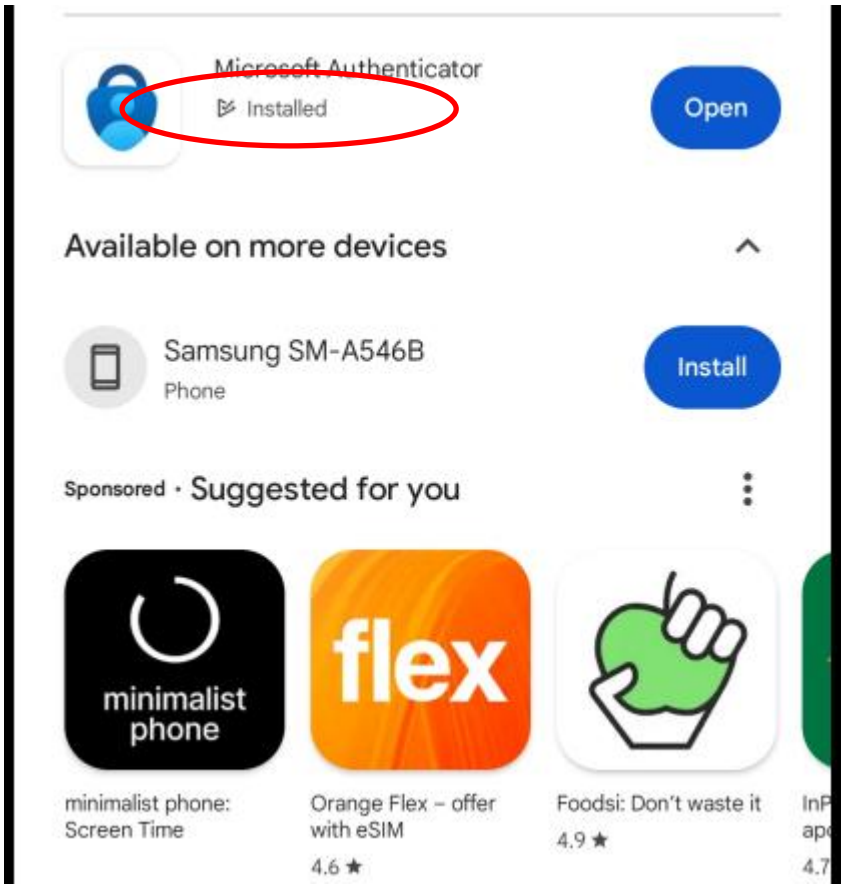
We do not click on the next button yet because now we have a choice, i.e. either we use the Microsoft® recommended application installed on the mobile device '**Microsoft Authenticator®**' for identity verification or we install alternative applications by selecting 'I want to use another authentication application', but for the moment we do not recommend this option.

Apps are available for free for **Android®** on the **Play® Store** or for **IPhone®** on the **App Store®**.

If you already have the **Microsoft Authenticator®** app installed, you can skip step #4 and proceed to the option to add an account (**step #5**).If you need to reinstall the **Microsoft Authenticator®** app, follow the rest of these instructions, but make sure you install 'Microsoft Authenticator' and not another app called Authenticator, as there are many apps that have similar names.

4 To install the **Microsoft Authenticator® app** in **the Play® Store** or **App Store®** we search for the app name 'Microsoft Authenticator', we click 'Install' and wait while the system finishes installing the **Microsoft Authenticator® app**. We can click on 'Open' or temporarily do not run the application but go to the browser window on our computer.

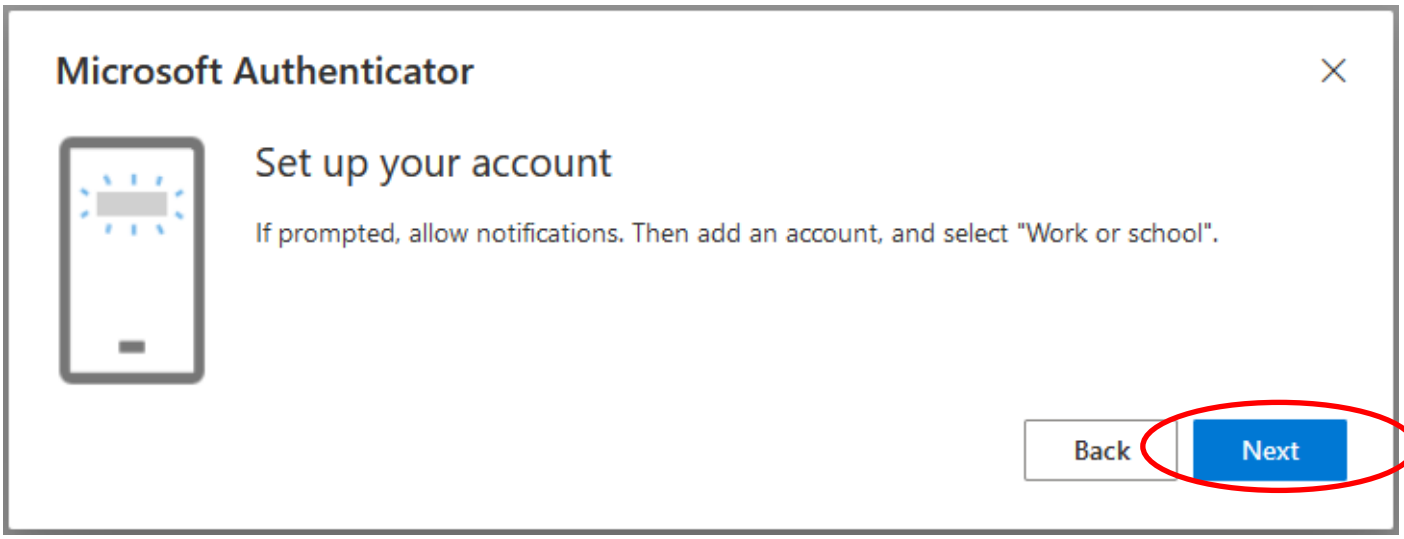




5 The next step is to add our business account to the app on the mobile device.

In step No. 3 - when we were asked to install **Microsoft Authenticator®** on the mobile device. When the installation was successful or we already had the app installed, only then we can click the 'Next' option in the browser.

Another window will appear on the page with an Announcement to set up a business account, click on the 'Next' option.



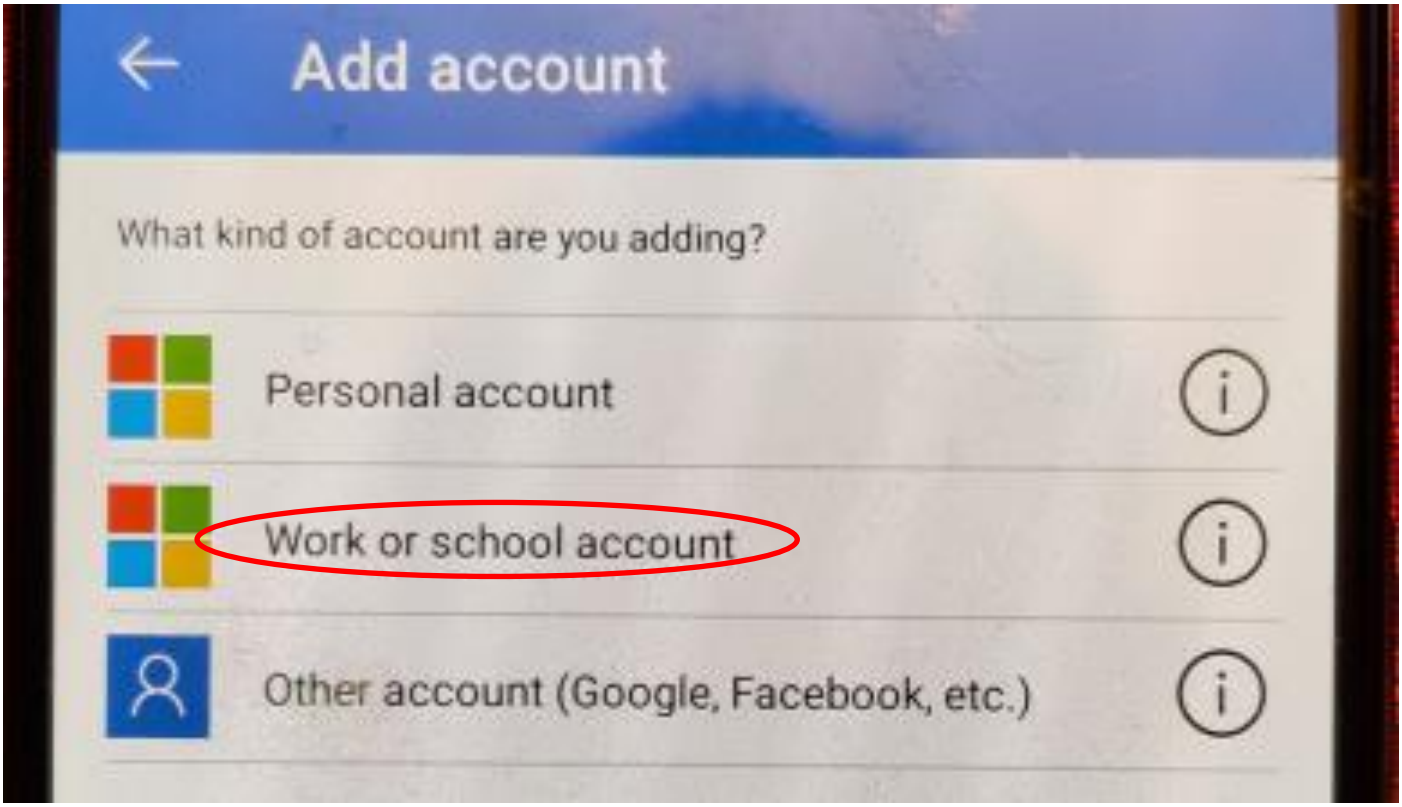
Very important note!!!
In the Microsoft Authenticator® app, do not select the QR code scanning option.
To add an account, select the "+" symbol and select "Work or school account" as the account type.
This is the only correct method and is described in detail below.

Below you will see a sample view of the QR code in your browser (the view of the QR code has been obscured for security reasons).

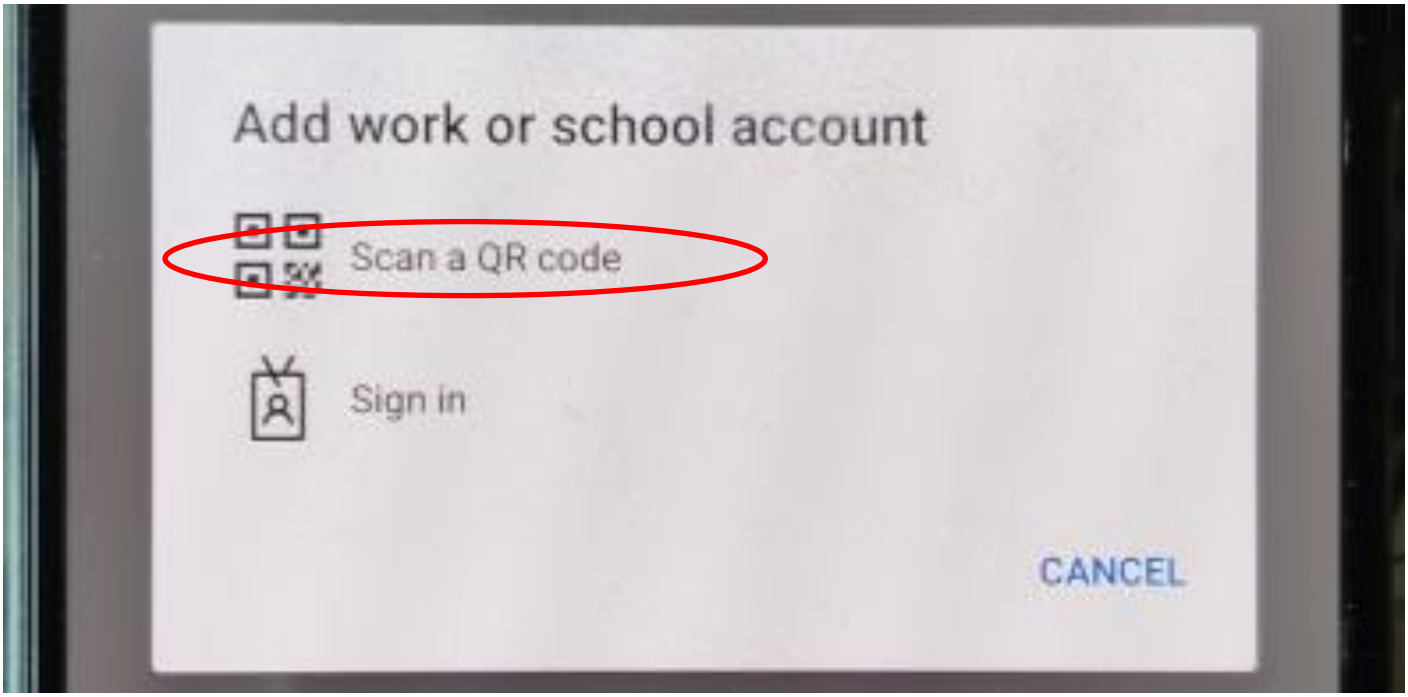
Again, we pause briefly before clicking on the 'Next' option because we need to scan the QR code visible on the screen with our mobile device.

To do this, we launch the **Microsoft Authenticator®** app on the mobile device and click on the plus sign to add our business account.

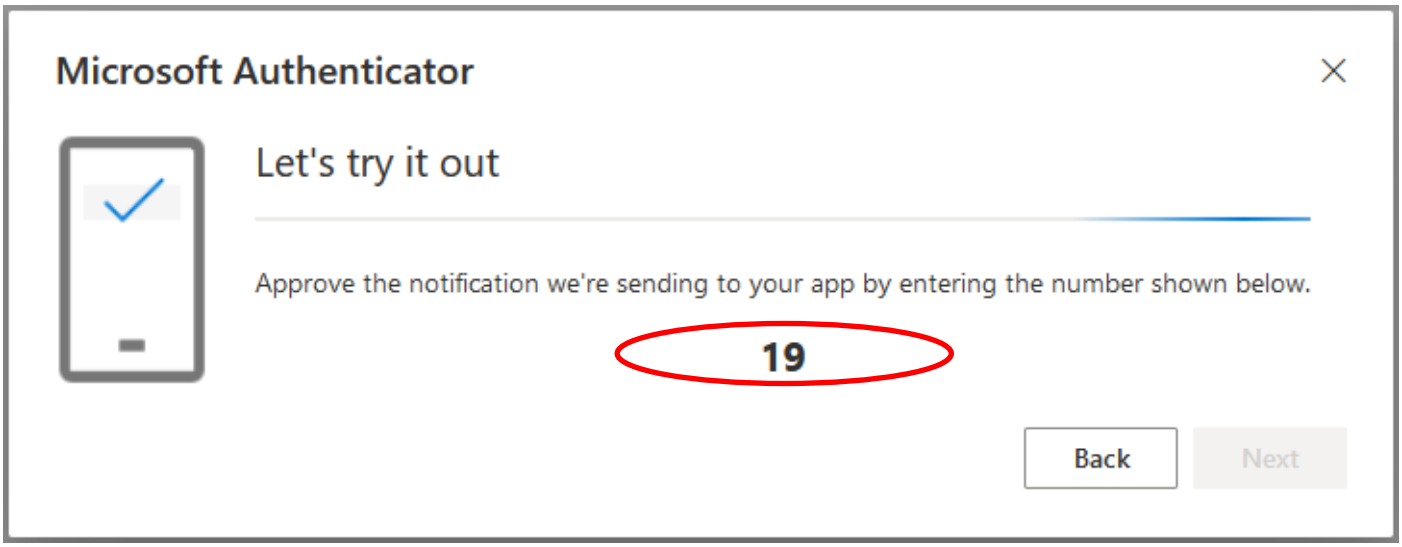
We then select 'Work or school account'.



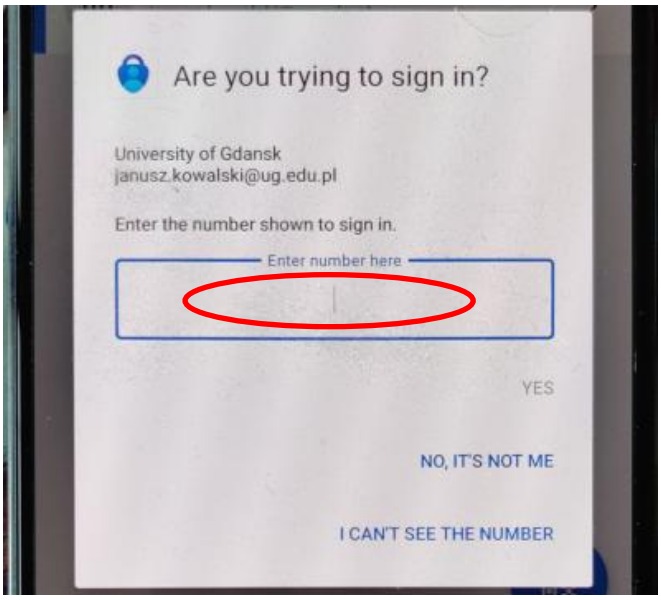
In the next window, we select 'Scan a QR code', in which case the QR code scanner will be activated on the camera-equipped mobile device; simply point the camera at our computer monitor, on which the QR code was previously displayed, and it will be read out automatically.



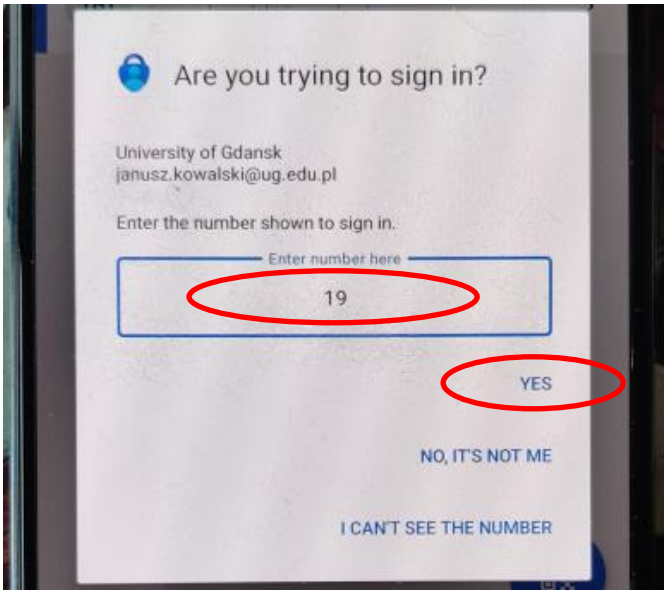
Once the QR code has been scanned correctly, we will be asked to validate on the mobile device a random number displayed in the browser on the computer.



In the **Microsoft Authenticator®** mobile app, you will first be prompted to enter the specified number in the appropriate field,



which, once entered, must be accepted by clicking on the 'Yes' button (as you can see from the example, it is the number 19).

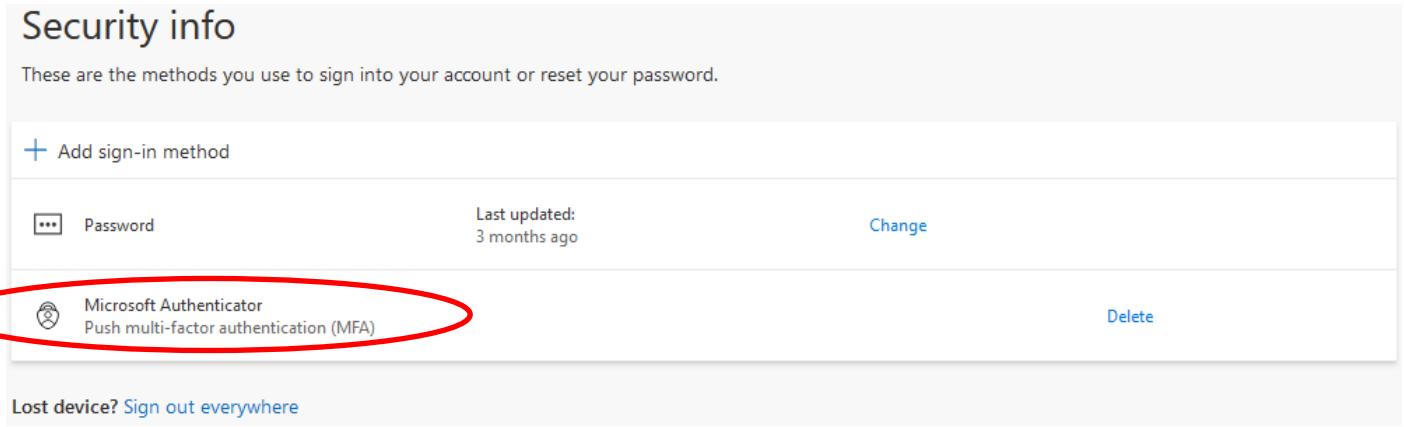


When everything is successful, a notification should appear in the browser that the application on the **Microsoft Authenticator®** mobile device has approved the notification.

We can click on the 'Next' option.

In the browser, we will again see the status of our security methods.

This time we will additionally see a message confirming that we have correctly configured the **Microsoft Authenticator®** application and that multi-factor authentication has thus been activated on our named account.



From now on, if you need to confirm your identity when logging in to **Microsoft®** services, you will be asked to enter a randomly generated number in the mobile app to verify your identity.

When and why do Microsoft Authenticator® app prompts appear?

Microsoft Authenticator app prompts only appear when:

- The Microsoft® service will detect an MFA-protected login attempt.
- On a new device.
- On a device for which a previous memorisation has expired (7 days since the last login using MFA).

In such cases, the app sends a notification that allows you to **confirm or reject the login attempt**.

When should you not confirm the notification?

- **You are not the one attempting to log** in: If you are not attempting to log in at this time, do not confirm your identity.
- **The notification is questionable**: If it seems suspicious or does not relate to your account, reject it.
- **Notifications are frequent and worrying**: If you are getting notifications that are not related to your activities, this could be a sign of an account security problem. If this is the case, report it to your system administrator.

What you should know about using MFA and the MS Authenticator® app

- Two-factor authentication (MFA) is required every time you log in to Microsoft® 365 services from outside the university network. The exception is if you have selected the option to remember a specific device for 7 days when logging in to the Microsoft Authenticator® app.

- Do not uninstall the Microsoft Authenticator® app from your smartphone – it is essential for daily use of your university account. Uninstalling the app (e.g., by mistake) and reinstalling it on the same device requires reconfiguration, meaning reconnecting the app to your Microsoft® 365 account. MFA configuration information is unique to each device and each app installation.

- The Microsoft Authenticator® app can be installed and configured on more than one mobile device (e.g., smartphone and tablet). This is recommended – in the event of a device failure or inaccessibility, it allows you to log in using a second, previously configured device. It also allows you to add a new device (e.g., to replace a damaged one) using two-factor authentication on a backup device.

- In the event of loss of a device with the Microsoft Authenticator® application installed (e.g. failure, loss, theft), it is necessary to contact the Information Center to remove the lost device and force reconfiguration of the login method when subsequently accessing Microsoft® 365 services.

Always contact the Helpdesk Section tel. 58-523-25-88 if you have any concerns.