



אגף טכנולוגיות חדשנות ודיגיטל  
צועדים יחד קדימה

## Securing our corporate e-mail !!! conditional access and multi-factor authentication

Members of the University's faculty.

Multi-factor authentication is an important security layer in protecting our user account.

This is an authentication method that requires to use of more than one identification method (for example: password).

This is to prevent a situation where an attacker who obtained the password for the account could access our e-mail.

Authentication with this method requires two or more credentials to log in to the account.

In our case the identification is based on two factors:

1. Something only we know (for example, our password).
2. Something we have (for example, our personal smartphone).

The following guide will guide us through the different steps that are needed to set up the additional security of our e-mail.

Important to note - The corporate e-mail security mechanism referred to this guide is designed to secure access to our e-mail from out campus. The mechanism will be activated at any connection attempt made outside the campus and from any new computer (from which the first connection is made) that is not in the university network.

On each computer, after establishing the connection once, this connection will be valid for 120 days of our choice.

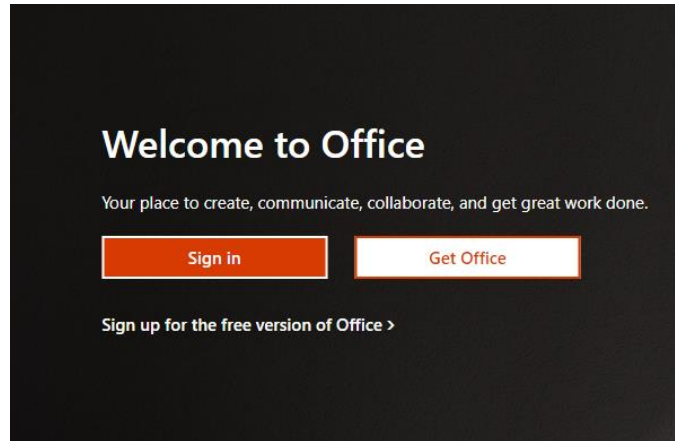
Note: For those who use the iPhone / iPad – at the end of the second stage of the settings below, delete the account setup, reset the device and proceed to the third step.

Guidelines appear in the two files attached to the message.

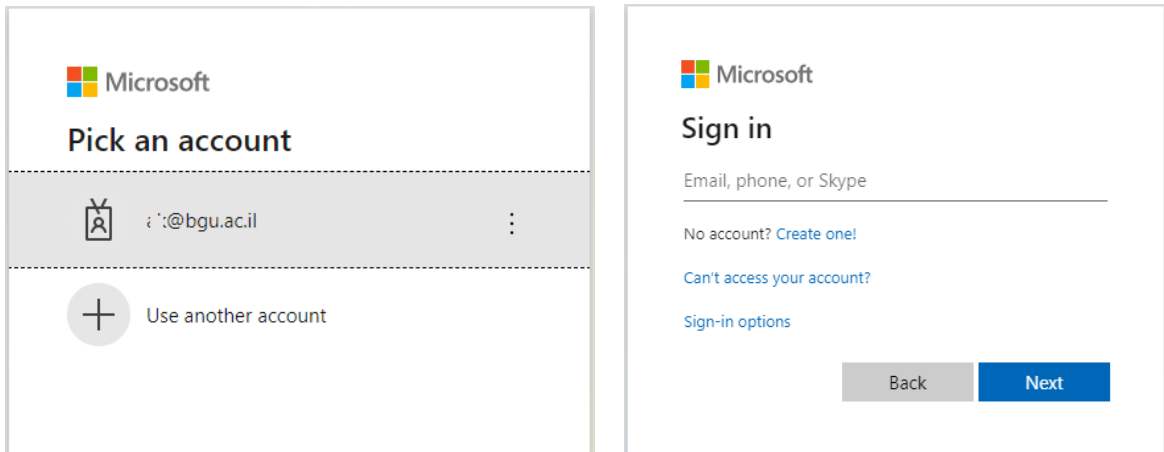
## Step one – one-time activation of the authentication via a computer

In the first step, you must log in to your Office account through a web browser at:  
<https://aka.ms/mfasetup>

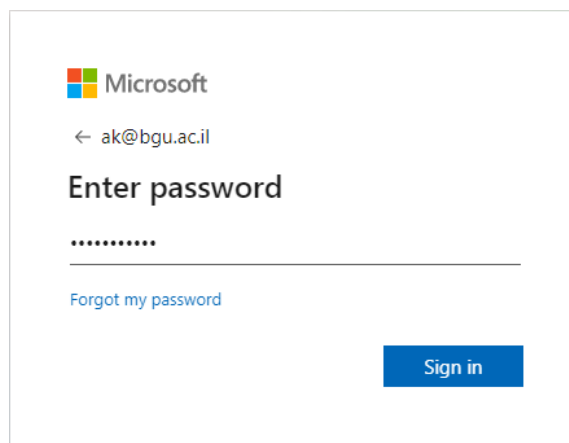
And Click on Sign in



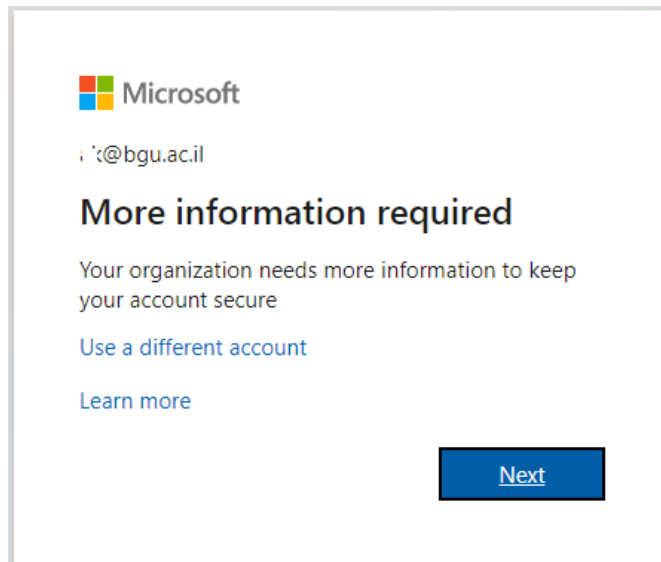
In one of the following windows, type your e-mail address or select the appropriate account.



In the next window type your password and click on Sign in



In the next window that explains that more details are needed, click Next



In the next window (Step 1) we will perform the following actions:

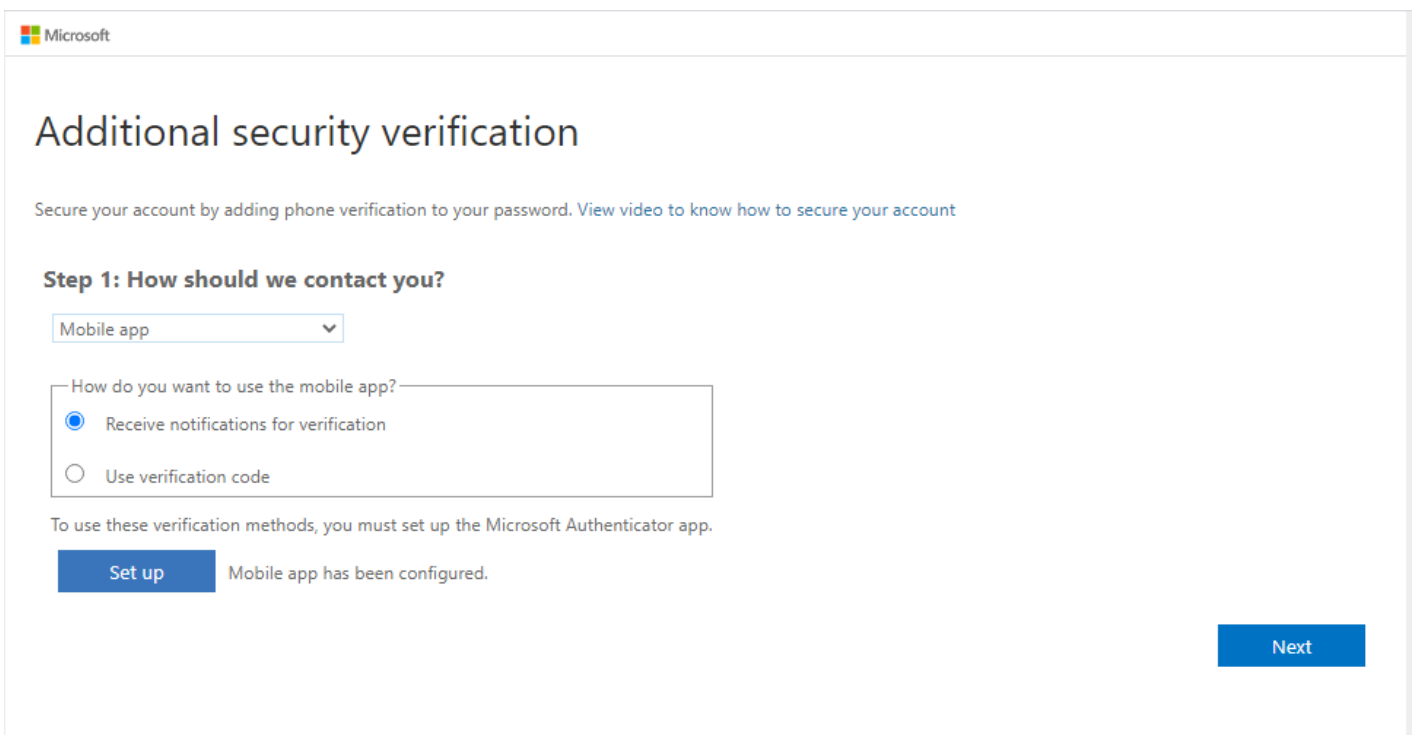
In the top selection box, select the Mobile app option.

check the option: Receive notifications for verification

And click the Set up button

Note: This option is recommended by the Technologies, Innovation and Digital Division.

Another option is to get a numeric code to the phone.



The next window will open in front of us (please do not touch it, in a few minutes we will have to scan the code on the cell phone)

## Configure mobile app

Complete the following steps to configure your mobile app.

1. Install the Microsoft authenticator app for Windows Phone, Android or iOS.
2. In the app, add an account and choose "Work or school account".
3. Scan the image below.



If you are unable to scan the image, enter the following information in your app.

Code: 626 429 255

Url: <https://mobileappcommunicator.auth.microsoft.com/mac/MobileAppCommunicator.svc/466549306>

If the app displays a six-digit code, choose "Next".

Next

cancel

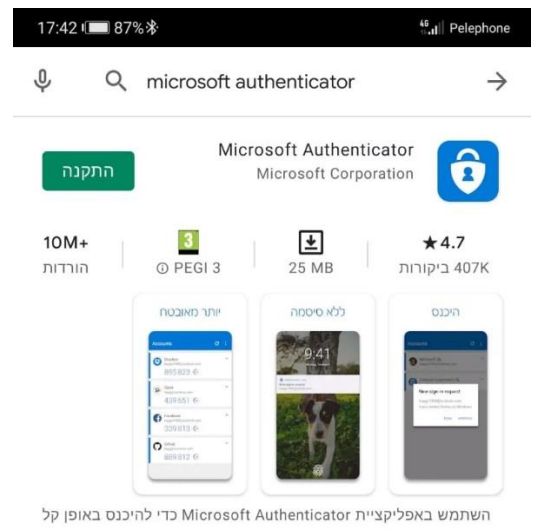
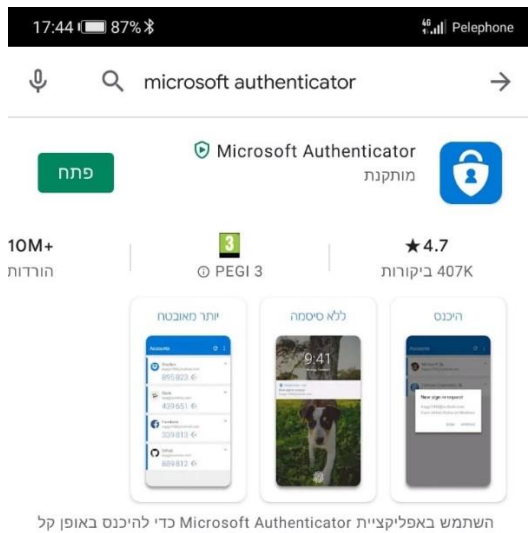
## Step Two - Install the app on your mobile phone

(For owners of iPhones, dedicated guides are attached to the message)

In the App Store / Google Play look for an app called: Microsoft authenticator.

After selecting it, click on "Install."

At the end of the installation, click on the "Open" button.

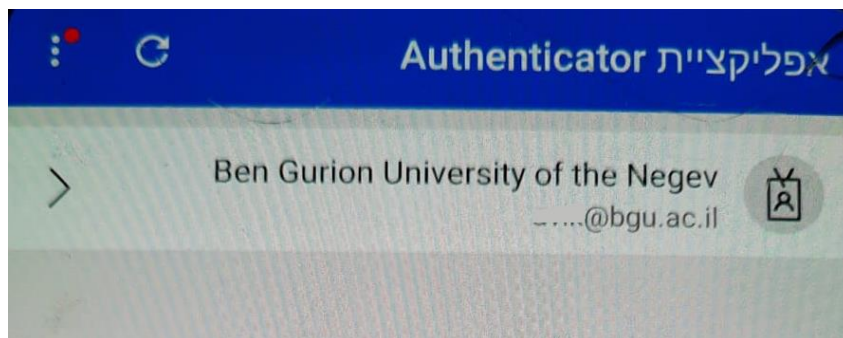


Once the app has opened, confirm the usage agreement screen and click on "Add Account."

Select the option: "Account at work or school".

Next, select: Scan QR code.

scan the code that appears on the computer (in the window we were in until the application was installed). After scanning the code the account will be added to the app.



### Step Three - Finish the process on your computer and phone

now return to the computer, to the window we were in and click Next

#### Configure mobile app

Complete the following steps to configure your mobile app.

1. Install the Microsoft authenticator app for Windows Phone, Android or iOS.
2. In the app, add an account and choose "Work or school account".
3. Scan the image below.



If you are unable to scan the image, enter the following information in your app.

Code: 626 429 255

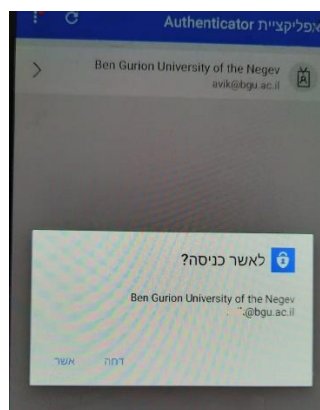
Url: <https://mobileappcommunicator.auth.microsoft.com/mac/MobileAppCommunicator.svc/466549306>

If the app displays a six-digit code, choose "Next".

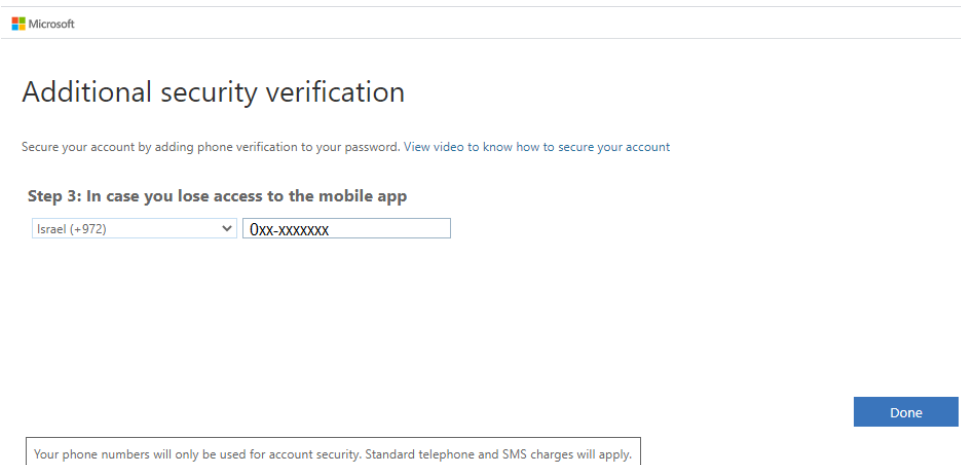
Next cancel

After a few seconds, a message will appear on the phone asking you to confirm the setting.

Click "approve" or "אשר"...



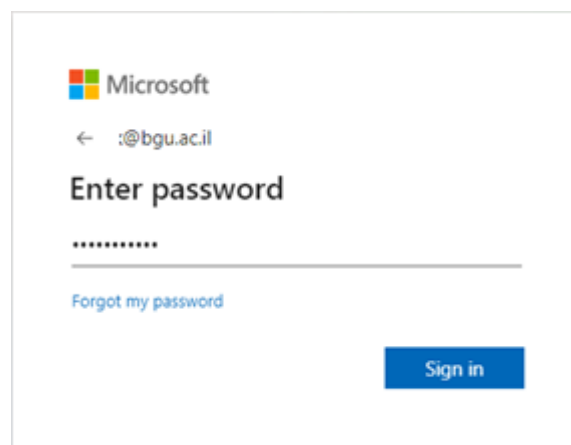
After you confirm the message on the device, select Israel and type in your cell phone number  
And click the Done button.



The screenshot shows the Microsoft account security verification interface. At the top, the Microsoft logo is visible. The main heading is "Additional security verification". Below it, a sub-heading reads "Step 3: In case you lose access to the mobile app". A small link says "View video to know how to secure your account". The form contains a dropdown menu set to "Israel (+972)" and a text input field containing "0xx-xxxxxxx". A blue "Done" button is positioned to the right. At the bottom, a note states: "Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply."

It is important to note that the phone number is only used for security purposes and another option to log in if there is a problem with the app.

To finish the settings type in your password.



The screenshot shows the Microsoft account password entry screen. At the top, the Microsoft logo is visible. Below it, the email address ":@bgu.ac.il" is displayed with a back arrow. The main heading is "Enter password". Below the heading is a password input field with a masked password ".....". A link "Forgot my password" is located below the input field. A blue "Sign in" button is positioned at the bottom right.

## We are ready - from now on - Approve sign in request

When you log in to the account, a window will appear that allows us to decide whether or not to receive confirmation messages to log in to our account For 120 days.

When we log in from a computer that belongs to us, we will mark the ✓ and we will not be required to confirm the login from this computer each time again.

When we log in from a random computer (for example friend's computer or hotel computer), make sure not to mark the ✓ and leave the check next to "Do not ask again for 120 days" blank.

Receiving this message on your computer will always lead to a request for approval or rejection in the app installed on the phone.

