



מאבטחים את הדואר האלקטרוני הארגוני שלנו!!!

גישה מותנית ואימות רב שלבי

Conditional access and multi-factor authentication

לחברי וחברות סגל האוניברסיטה,

אימות רב שלבי מהווה שכבת אבטחה חשובה בהגנה על חשבון המשתמש שלנו. מדובר בשיטת אימות שמחייבת שימוש ביותר משיטת אימות אחת (לדוגמה: סיסמה). זאת על מנת למנוע מצב שבו תוקף שהשיג את הסיסמה לחשבון יוכל להיכנס לחשבון הדוא"ל שלנו.

אימות בשיטה זו דורש שני סוגי הזדהות או יותר לכניסה לחשבון.

במקרה שלנו ההזדהות מבוססת על שני גורמים:

- ① משהו שרק אנחנו יודעים (לדוגמה - הסיסמה שלנו)
- ② משהו שיש לנו (לדוגמה - טלפון חכם הנמצא אצלנו)

המדריך הבא ילווה אותנו בשלבים השונים של ההגדרות הדרושות לאבטחה נוספת של הדואר האלקטרוני שלנו.

חשוב לציין – מנגנון אבטחת הדואר האלקטרוני הארגוני לגביו מתייחס מדריך זה, נועד לאבטח את הגישה שלנו לתיבת הדואר האלקטרוני כאשר אנו נמצאים מחוץ לקמפוס. המנגנון יופעל בכל ניסיון חיבור שנבצע מחוץ לקמפוס ומכל מחשב חדש (ממנו מבוצע החיבור לראשונה) שאינו ברשת האוניברסיטה.

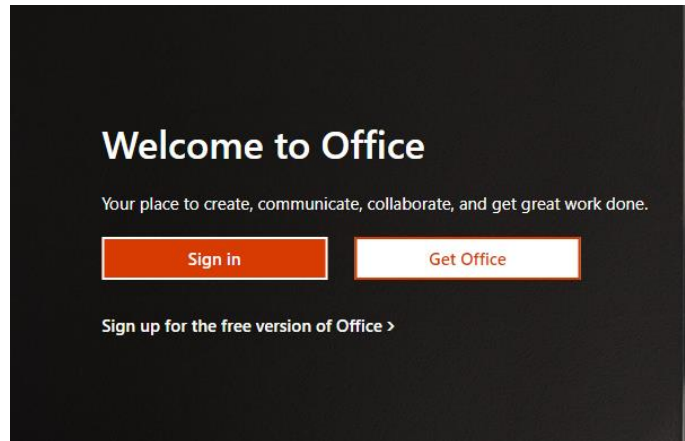
בכל מחשב ממנו ביצענו את החיבור פעם אחת, חיבור זה יהיה תקף ל-120 ימים (לפי בחירתנו).

שלב ראשון – הפעלה חד-פעמית של האימות הרב שלבי דרך מחשב שאינו ברשת האוניברסיטה

בשלב הראשון יש להיכנס לחשבון Office דרך דפדפן אינטרנט (גישה מחוץ לרשת האוניברסיטה)

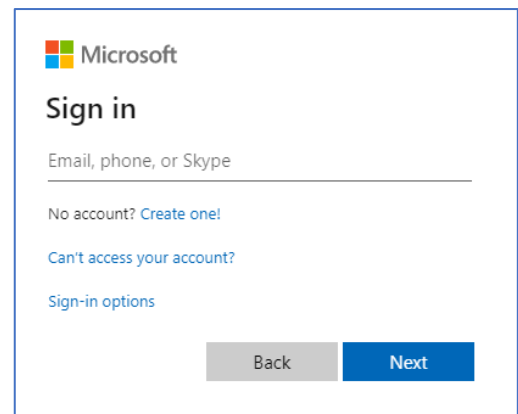
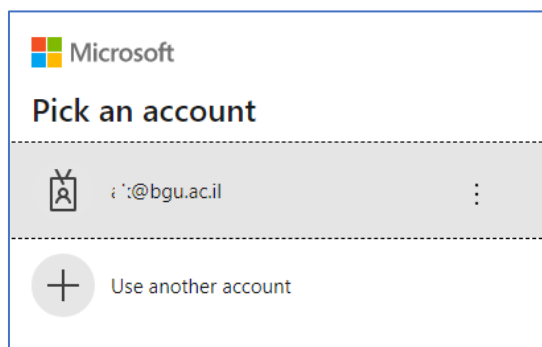
בכתובת: <https://www.office.com>

נלחץ על [Sign in](#):

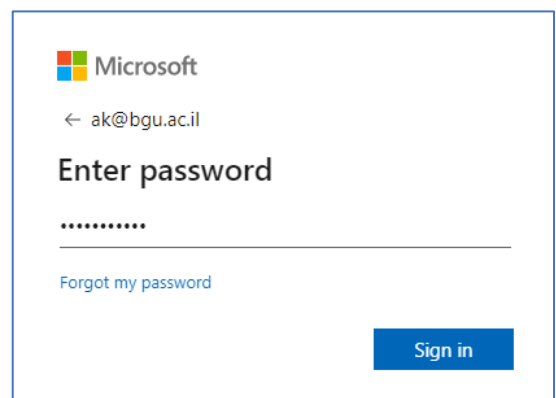


באחד מהחלונות הבאים נקליד את כתובת הדואר האלקטרוני שלנו או נבחר בחשבון המתאים

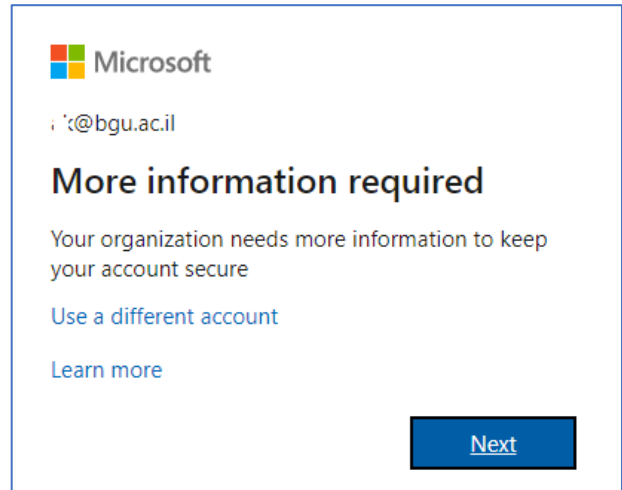
[yourname@bgu.ac.il](#)



בחלון הבא נקליד את הסיסמה שלנו ונלחץ על [Sign in](#):



בחלון הבא המסביר שדרושים פרטים נוספים, נלחץ על [Next](#):



Microsoft

i.k@bgu.ac.il

More information required

Your organization needs more information to keep your account secure

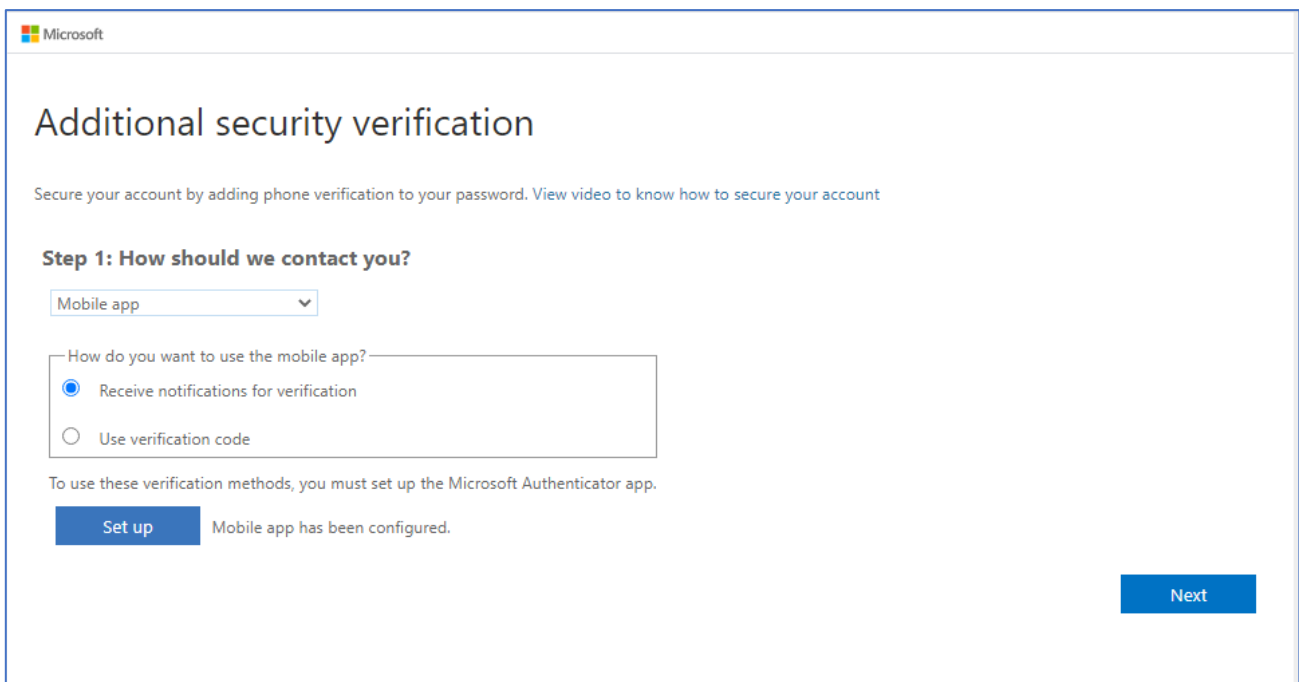
[Use a different account](#)

[Learn more](#)

[Next](#)

בחלון הבא (Step 1) נבצע את הפעולות הבאות:

בתיבת הבחירה העליונה נבחר באפשרות: [Mobile app](#)
נסמן את האפשרות: [Receive notifications for verification](#)
ונלחץ על לחצן [Set up](#)



Microsoft

Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

Step 1: How should we contact you?

Mobile app

How do you want to use the mobile app?

Receive notifications for verification

Use verification code

To use these verification methods, you must set up the Microsoft Authenticator app.

[Set up](#) Mobile app has been configured.


[Next](#)

יפתח החלון הבא. (נא לא לגעת בו, בעוד מס' דקות נצטרך לסרוק את הקוד בטלפון הסלולרי)

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.



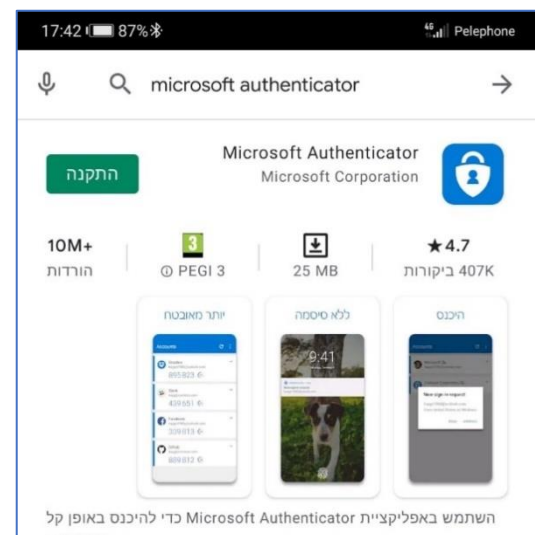
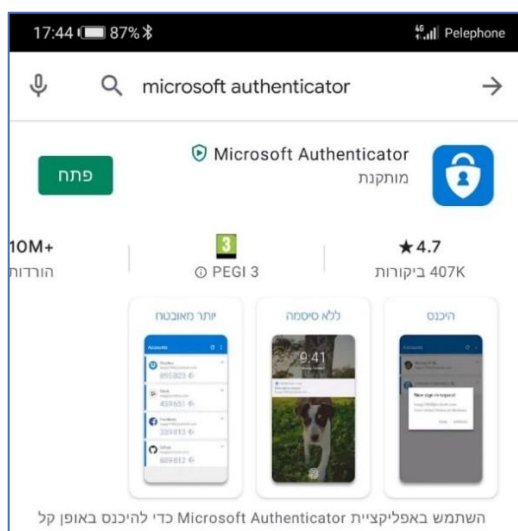
If you are unable to scan the image, enter the following information in your app.
Code: 626 429 255
Url: <https://mobileappcommunicator.auth.microsoft.com/mac/MobileAppCommunicator.svc/466549306>

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

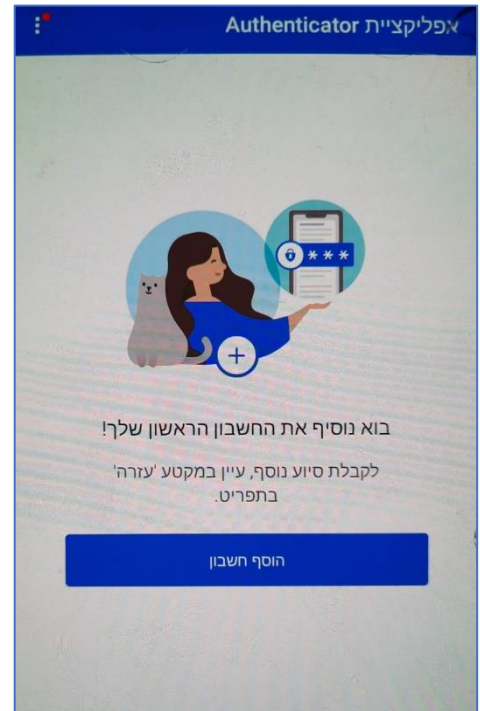
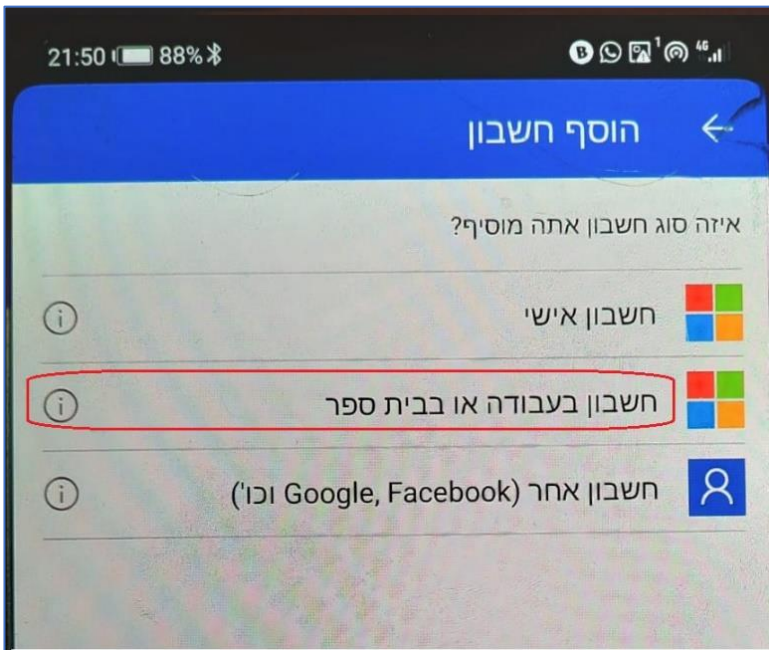
[Next](#) [cancel](#)

שלב 2 – התקנה של האפליקציה במכשיר הטלפון הסלולרי

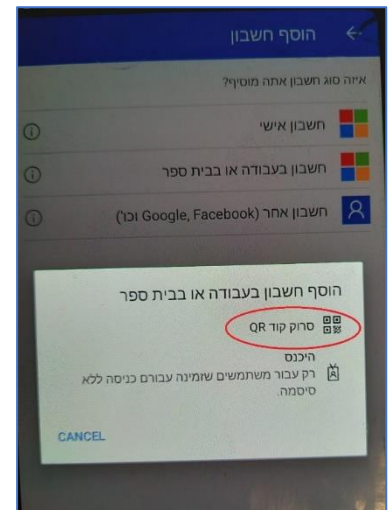
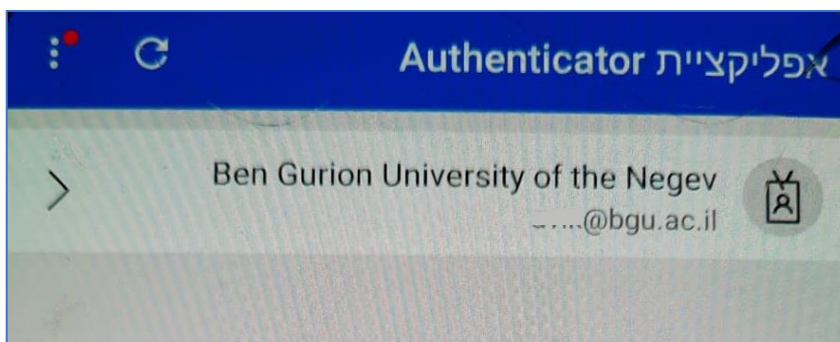
בחנות האפליקציות (App Store/Google Play) נחפש אפליקציה בשם: **Microsoft Authenticator**
לאחר שנבחר בה נלחץ על "**התקנה**". בסיום ההתקנה נלחץ על לחצן "**פתח**".



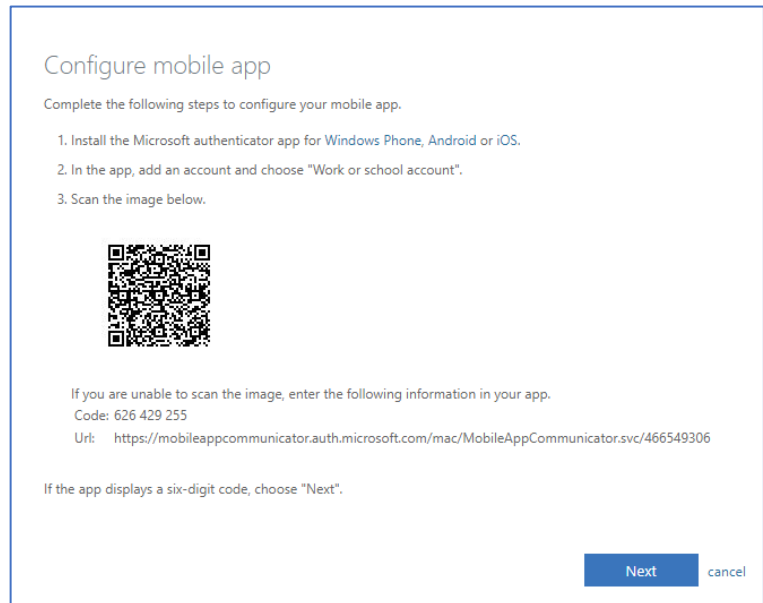
לאחר שהאפליקציה נפתחה, נאשר את מסך הסכמ השימוש ונלחץ על "הוסף חשבון".
נבחר באפשרות: "חשבון בעבודה או בבית ספר":



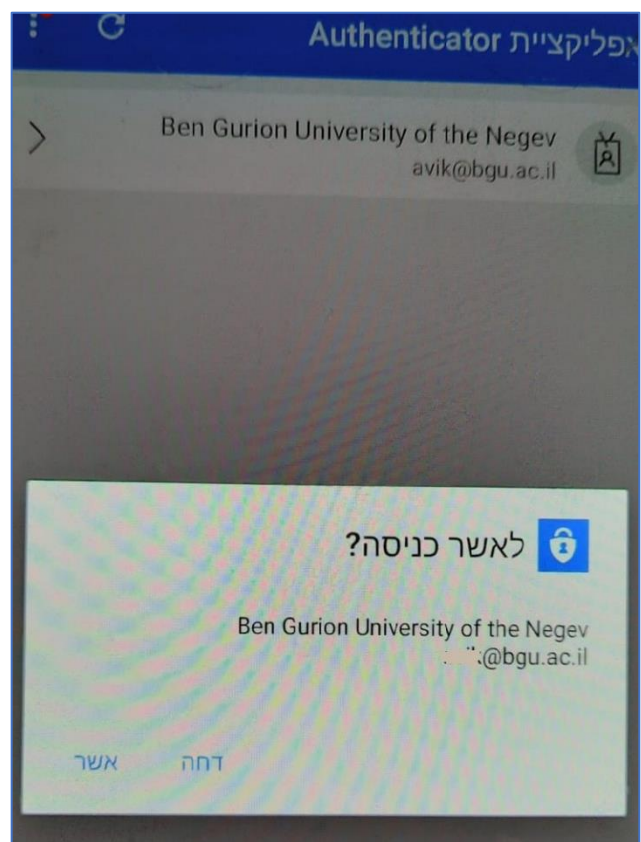
בהמשך נבחר באפשרות: **סרוק קוד QR**
נסרוק את הקוד המופיע שמחכה לנו במסך המחשב (בחלון שהיינו בו עד התקנת האפליקציה)
לאחר סריקת הקוד החשבון יתווסף לאפליקציה.



בעת נחזור למחשב, לחלון שבו היינו, ונלחץ על Next:



לאחר מספר שניות תופיע במכשיר הטלפון הודעה שבה נתבקש לאשר את ההגדרה. נלחץ על "אשר":



לאחר שאישרנו את ההודעה במכשיר, נבחר בישראל ונקליד את מספר הטלפון הסלולרי שלנו במסך המחשב ונלחץ על לחצן Done.

The screenshot shows a Microsoft account security verification page. At the top, it says "Additional security verification" and "Secure your account by adding phone verification to your password. View video to know how to secure your account". Below that, it says "Step 3: In case you lose access to the mobile app". There are two input fields: one for the country code (set to "Israel (+972)") and one for the phone number (set to "0xx-xxxxxxx"). A "Done" button is located at the bottom right. At the bottom of the page, there is a small disclaimer: "Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply."

הערה:

חשוב לציין כי מספר הטלפון משמש רק לצורכי אבטחה ואפשרות נוספת לכניסה אם תהיה בעיה באפליקציה. לסיום ההגדרות נקליד את הסיסמה שלנו.

The screenshot shows a Microsoft account password entry page. At the top, it says "Microsoft" and "← :@bgu.ac.il". Below that, it says "Enter password" and there is a password input field with a masked password ".....". There is a "Forgot my password" link below the input field. At the bottom right, there is a "Sign in" button.

אנחנו מוכנים – מכאן והלאה - Approve sign in request

The screenshot shows a Microsoft account "Approve sign in request" page. At the top, it says "Microsoft" and "...@bgu.ac.il". Below that, it says "Approve sign in request". There is a lock icon and the text "We've sent a notification to your mobile device. Please open the Microsoft Authenticator app to respond." Below that, there is a checked checkbox and the text "Don't ask again for 120 days". At the bottom, there are two links: "Having trouble? Sign in another way" and "More information".

בכניסה לחשבון, יופיע חלון המאפשר לנו להחליט האם לקבל או לא לקבל הודעות אישור כניסה לחשבון שלנו למשך 120 ימים. כאשר אנו מבצעים כניסה ממחשב השייך לנו נסמן את ה-√ ובכך לא נידרש לאשר את הכניסה ממחשב זה בכל פעם מחדש.

כאשר ניכנס ממחשב אקראי (מחשב של חברים או מחשב בבית מלון לדוגמה) נקפיד לא לסמן את ה-√. כלומר, נשאיר את הסימון לצד Don't ask again for 120 days ריק.

קבלת הודעה זו במחשב תוביל תמיד לבקשת אישור או דחייה באפליקציה שהותקנה בטלפון.