

שלום רב,

בימים אלו לאור הצורך הרב בפגישות ווירטואליות מרחוק חלה עלייה בניסיונות חבלה בפגישות בכלל ובאפליקציית ZOOM בפרט, התופעה ידועה בשם "Zoom Bombing".

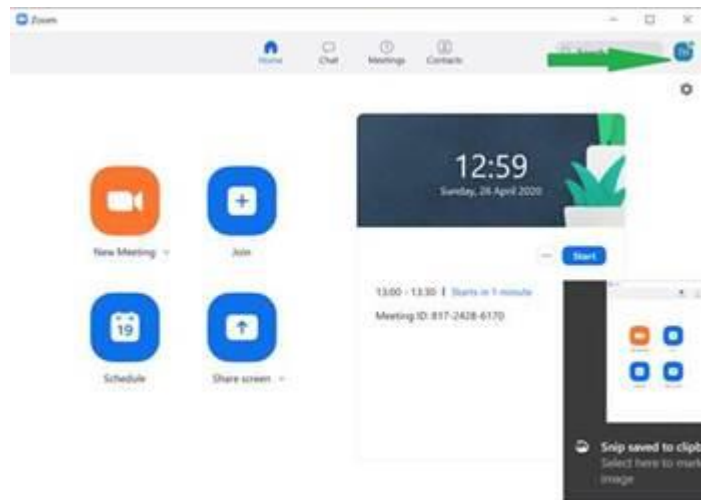
Zoom Bombing - בשל הפופולריות הרבה של שירותי שיחות ועידה בימים אלה, החלו האקרים רבים לנצל זאת, ולפרוץ לשיחות ומפגשים. התוקפים מנצלים את הקלות היחסית ב"ניחוש מספרי פגישה" ובעזרת תוכנות אוטומטיות מוצאים פגישות פעילות בזום ומתפרצים פנימה.

ההאקרים עלולים לגרום, במקרה הטוב – לשיבוש המפגש ולקריסה של השיחות, ובמקרה הפחות טוב – לגניבת מידע והשתלטות על המחשב.

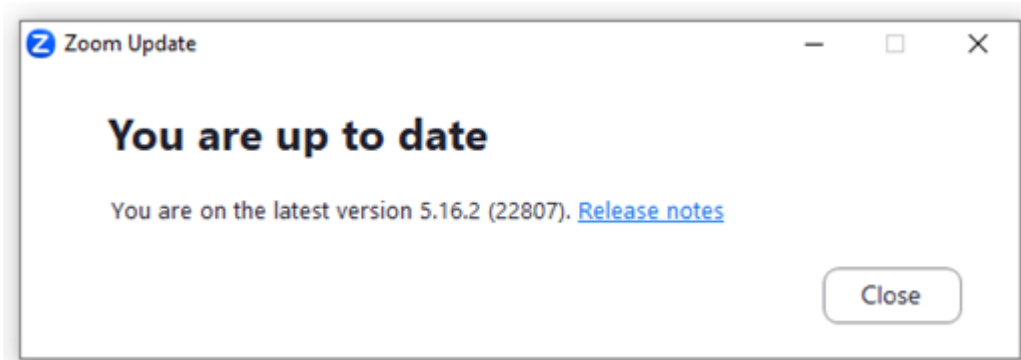
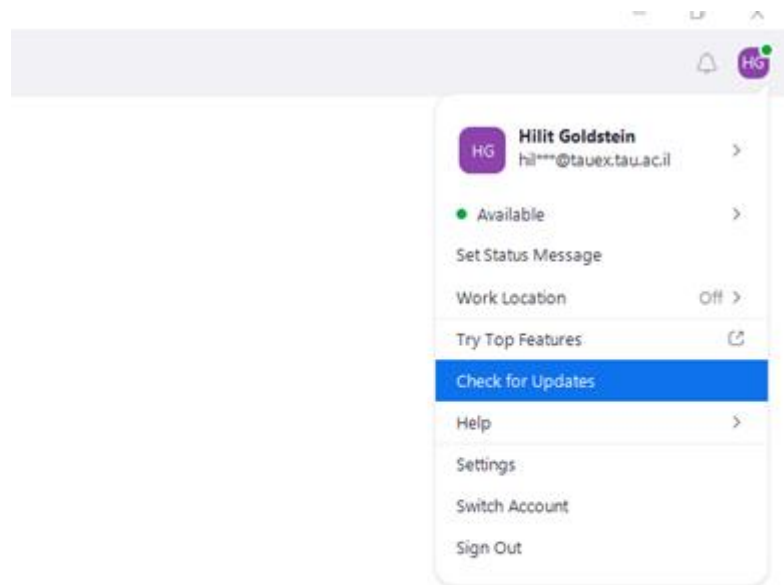
לכן ראשית מומלץ לא לבצע פגישות אישיות רגישות ב-ZOOM.

במידה והשיחה איננה מוגדרת כך יש לבצע את הפעולות הבאות:

1. יש לוודא כי הגרסה שלכם מעודכנת, וזאת על ידי לחיצה על תמונת הפרופיל שלכם, הנמצאת ליד שורת החיפוש:



לאחר מכן יש לבחור באופציה "check for updates", ולוודא כי ההודעה " You are up to date" מופיעה. אם לא, יש לבצע את העדכון.



2. אין לפרסם באינטרנט את הקישור הישיר לשיחת הזום המתוכננת (למשל, כך: <https://zoom.us/j/838142224>). במקום לציין את הקישור באינטרנט, בעמוד האירוע/המפגש – עדיף לשלוח את הקישור ישירות למשתתפים (במייל, ווטאספ וכו'), או, במידת האפשר – להפעיל טופס הרשמה. כך תוכלו, לאחר ההרשמה, לשלוח למשתתף את הקישור ו/או הסיסמה למפגש.

(אין ספק שזה מוסיף עוד חסם בפני משתתפים, אך כך אתם מפחיתים את הסיכונים).

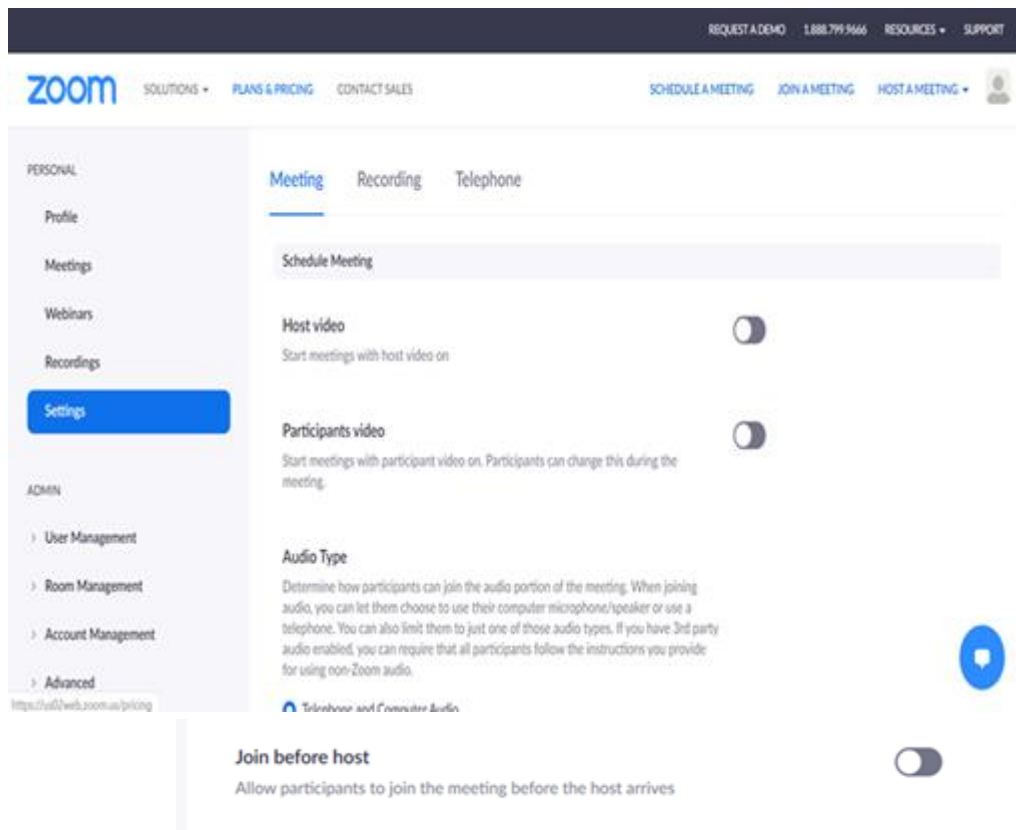
3. יש לבצע הגדרה אוטומטית של **סיסמה**, על מנת להצטרף למפגש (מופיע במערכת הזום כ-**"Require meeting password"**).

4. הגדרה אוטומטית של **"לובי"** לפני כניסה למפגש (מופיע במערכת הזום כ-**"Enable waiting room"**). הקפידו לא לבטל את מנגנון ה"לובי". בכל מקרה רצוי מאד להשתמש במנגנון זו, המאפשר לכם סינון של כניסת משתתפים למפגש. מנגנון זה קריטי במיוחד במידה והחלטתם בכל זאת לפרסם באינטרנט את הקישור הישיר. במקרה זה, משתתף ימתין "בלובי", ותקבלו על כך הודעה. בשלב זה תוכלו לאשר או לבטל את כניסתו, במידה והוא לא אמור להיות בפגישה. (כך גם תוכלו לסנן משתמשים חשודים).

5. נסו לצמצם למינימום פגישות ציבוריות בתקופה זו, כיוון שאפליקציית זום ככל והאוניברסיטאות בפרט הם יעדי תקיפה מועדפים.

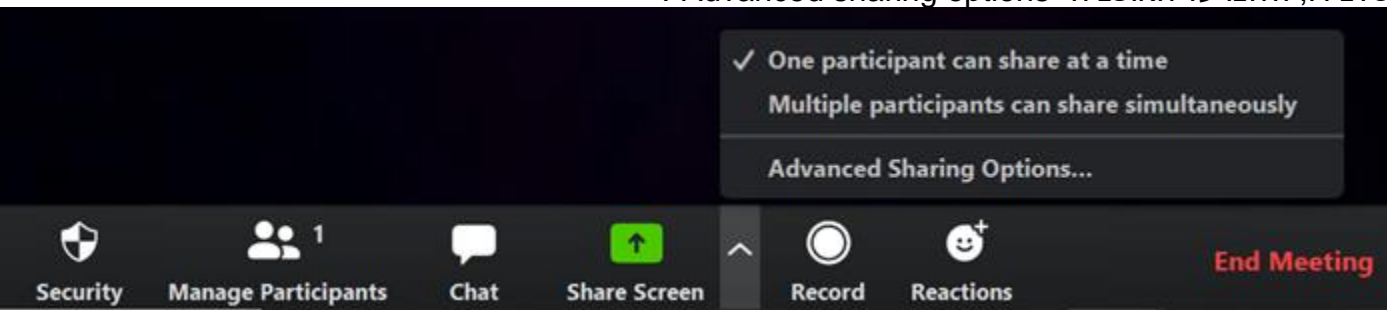
6. ודאו כי האופציה **"Enable join before host"** כבויה (אם הגירסה שלכם מעודכנת, זוהי ברירת המחדל):

* התחברו לחשבון ה-zoom שלכם באתר <https://us02web.zoom.us/profile> ולחצו על **"Settings"**, גללו מעט למטה וודאו שהאופציה להצטרף לפני המארח כבויה, במידה ולא כבו אותה.



The screenshot displays the Zoom web interface for managing meeting settings. The top navigation bar includes links for 'REQUEST A DEMO', '1.888.799.5666', 'RESOURCES', and 'SUPPORT'. Below this, the main navigation menu features 'SOLUTIONS', 'PLANS & PRICING', 'CONTACT SALES', 'SCHEDULE A MEETING', 'JOIN A MEETING', and 'HOST A MEETING'. The left sidebar lists 'PERSONAL' options (Profile, Meetings, Webinars, Recordings, Settings) and 'ADMIN' options (User Management, Room Management, Account Management, Advanced). The main content area is titled 'Meeting' and includes sections for 'Schedule Meeting', 'Host video' (turned on), 'Participants video' (turned on), and 'Audio Type'. At the bottom, the 'Join before host' option is shown as turned off, with the description 'Allow participants to join the meeting before the host arrives'.

7. הגבילו את שיתוף המסך ל"מארח בלבד" (Host only):
* בתוך חלון הפגישה, בסרגל התחתון ליד הכפתור הירוק "screen share" לחצו על החץ שלצידו, ולחצו על האופציה "Advanced sharing options".



*לאחר מכן, בחלון שנפתח, תחת הכותרת "Who can share?", יש לבחור באופציה "Host Only":



8. יש להימנע מלפתוח לינקים שפורסמו לא ע"י המארח.

Dear all

In recent days, due to the significant need for remote virtual meetings, there has been an increase attempts to disrupt meetings in general and the Zoom application in particular. This phenomenon is known as "Zoom Bombing."

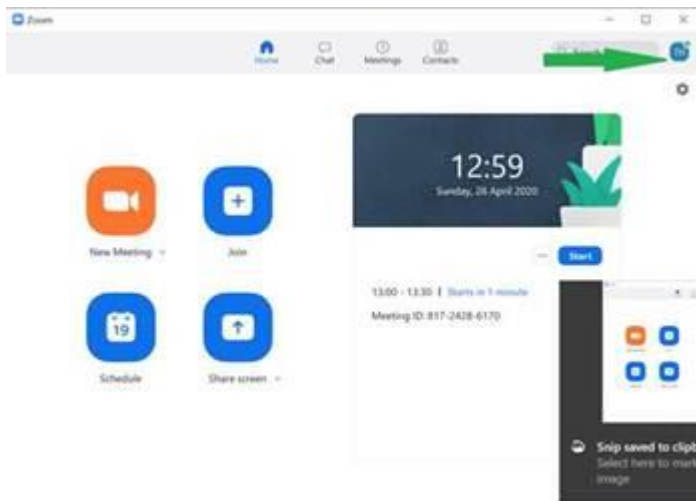
Zoom Bombing - Due to the widespread popularity of video conferencing services these days, many hackers have started to exploit this and intrude into meetings and conferences. Attackers take advantage of the relative ease of "guessing meeting IDs" and use automated programs to find active Zoom meetings and infiltrate them.

These hackers can, in the best case scenario, disrupt the meeting and cause it to crash, and in the worst case, steal information and take control of the computer.

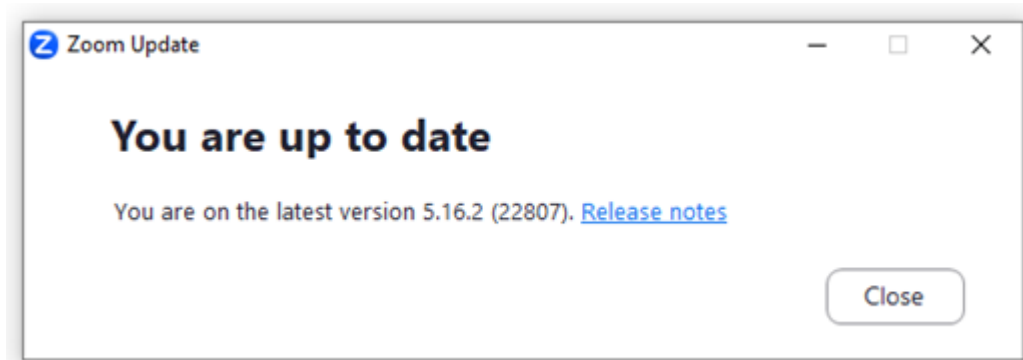
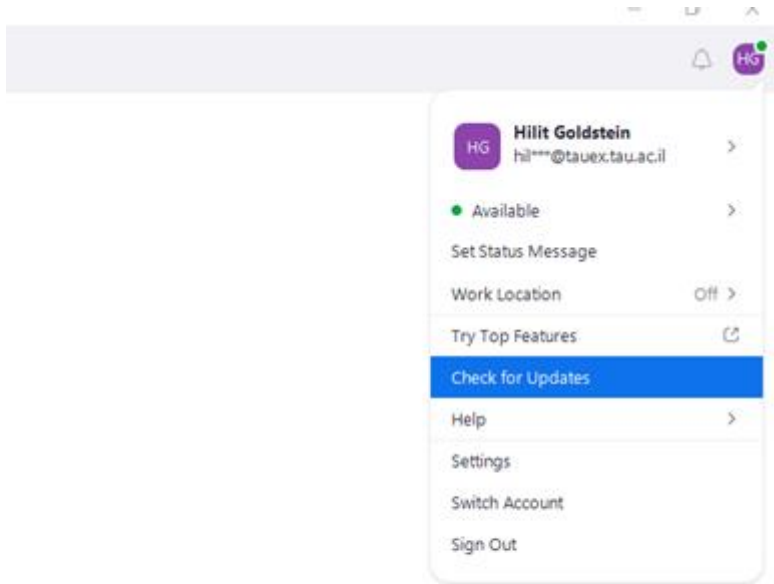
Therefore, it is recommended not to conduct sensitive personal meetings on Zoom.

In case your conversation is not classified as sensitive, you should take the following actions:

1. Ensure that your Zoom version is up to date by clicking on your profile picture next to the search bar:



Afterward, select the "Check for updates" option and make sure that the message "You are up to date" appears. If it doesn't, you should proceed to update your Zoom application.



2. Don't publish the direct link to your Zoom meeting on the internet. Instead, for your event or meeting page, it's better to send the link directly to participants via email, WhatsApp, or other private messaging platforms. If possible, you can also implement a registration form. This way, after registration, you can send participants the link and/or password to the meeting.

This approach does add an extra layer of security by limiting access to those who have registered, reducing the risks associated with sharing public links widely.

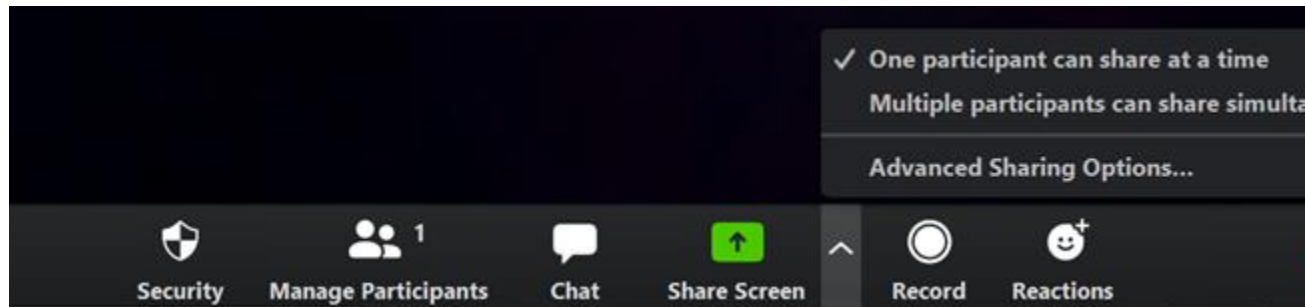
3. Requiring a meeting password is a good security practice to ensure that only authorized participants can join.

4. Setting up a waiting room (known as "Enable waiting room" in Zoom) is a crucial security measure to control who can enter your meeting. It allows you to admit or deny participants before they join the meeting.
5. Try to minimize public meetings during this time, as applications like Zoom are preferred targets, especially for universities.
6. Make sure the "Enable join before host" option is turned off (if your version is up to date, this is the default setting):
 - Log in to your Zoom account on the Zoom website at <https://us02web.zoom.us/profile>.
 - Click on "Settings."
 - Scroll down a bit and verify that the "Join before host" option is turned off. If it's enabled, disable it.

The screenshot shows the Zoom website's settings page. The top navigation bar includes links for 'REQUEST A DEMO', '1.888.799.9466', 'RESOURCES', and 'SUPPORT'. Below this, the Zoom logo is followed by 'SOLUTIONS', 'PLANS & PRICING', and 'CONTACT SALES'. On the right, there are links for 'SCHEDULE A MEETING', 'JOIN A MEETING', and 'HOST A MEETING' next to a user profile icon. The left sidebar is divided into 'PERSONAL' and 'ADMIN' sections. Under 'PERSONAL', 'Settings' is highlighted in blue. Under 'ADMIN', there are links for 'User Management', 'Room Management', 'Account Management', and 'Advanced'. The main content area has tabs for 'Meeting', 'Recording', and 'Telephone', with 'Meeting' selected. Below the tabs, there is a 'Schedule Meeting' button. The 'Host video' setting is turned off, with the description 'Start meetings with host video on'. The 'Participants video' setting is also turned off, with the description 'Start meetings with participant video on. Participants can change this during the meeting.' The 'Audio Type' section provides instructions on how participants can join the audio portion of the meeting. At the bottom, the 'Join before host' setting is turned off, with the description 'Allow participants to join the meeting before the host arrives'. A blue speech bubble icon is visible on the right side of the page.

7. Limit screen sharing to "Host only":

- Within the meeting window, at the bottom toolbar, next to the green "Screen Share" button, click on the arrow.
- Select the "Advanced sharing options" from the menu.



- After opening the window, under the title "Who can share?", select the "Host Only" option:



8. avoid opening links that have been shared by someone who is not the host.