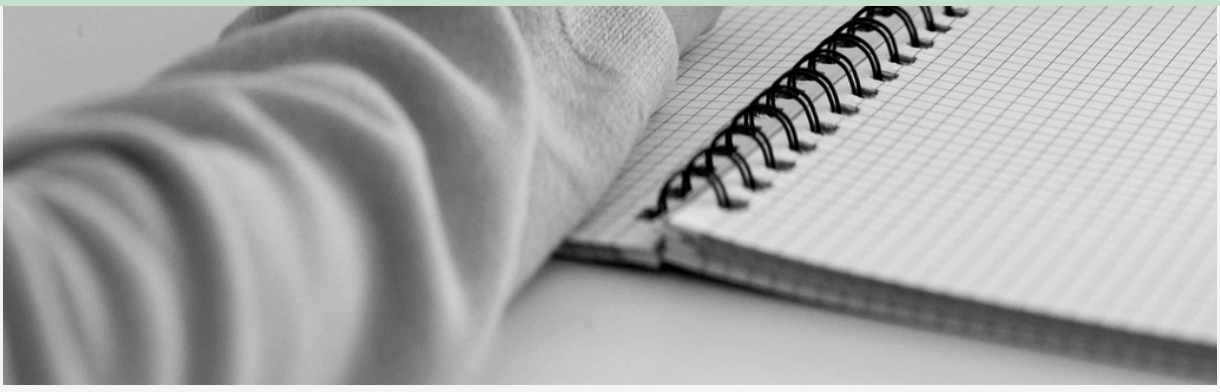
Tips for Securing Your ZOOM Meetings



MIDDLE EAST TECHNICAL UNIVERSITY

Distance Education Application and Research Center
2021

Synchronous Lectures with Zoom

Considering the risks, security measures should be implemented.

With the transition to online education with the COVID-19 Pandemic, live lectures have become one of the most frequently used synchronous teaching tools at METU. Zoom, Webex and BigBlueButton infrastructures are available to our instructors for synchronous lessons. The usage statistics show that Zoom is the most preferred among these options, and that is also supported by the answers of the instructors in the surveys.

Globally, Zoom is the most used video conferencing tool. The extensive usage of the tool also makes it vulnerable to threats and dangers. Although Zoom has taken measures such as end-to-end encryption against the attacks that you may have heard of as "Zoom bombing", there are some precautions that are recommended for meeting hosts to avoid attacks. These precautions will be included in this document.

Scheduling Zoom Meetings in ODTÜClass

You can schedule Zoom meetings for live lectures with the Zoom activity in ODTÜClass. With these activities, you can schedule meetings, start meetings, access reports and recordings, if any. This activity eliminates the need to share the meeting link with your students. Students enrolled in your course can click on the Zoom activity and join the session you have planned.

You can review the ODTÜClass User's Guide (in Turkish) about adding a Zoom event and scheduling a meeting:

https://odtuclass2021f.metu.edu.tr/mod/book/view.php?id=1&chapterid=60

PRE-MEETING SETTINGS

You can increase the security of your meetings with some settings while scheduling Zoom meetings.

01 TURN ON YOUR WAITING ROOM

Enable the waiting room feature when scheduling your meeting. Thus, you can check the participants and admit them to the meeting room. If you warn your students that they should enter the meetings with their real names, otherwise they will not be taken to the class, you can remove the participants from the waiting room or not admit them to the meeting.

02 DON'T USE PERSONAL MEETING ID FOR PUBLIC MEETINGS

Each Zoom user has a static Personal Meeting ID (PMI). Since this number does not change, once it becomes known, uninvited participants can join your meetings.

03 REQUIRE A PASSCODE TO JOIN

Define a Passcode for the meetings you schedule. Passwords can be included in the invitation link, thus the use of passwords will only prevent uninvited people with the meeting number from joining the meeting.

04 ONLY ALLOW DOMAIN VERIFIED (METU) USERS

While scheduling your meeting, you can only allow participants who have created an Zoom account with a "@metu.edu.tr" address to join your meeting. If you are going to use this feature, you should inform your students that they need to create a Zoom account with their METU account and join to the meetings with this account. Otherwise, you will also prevent your students from participating in the meeting along with uninvited people.

IN-MEETING SETTINGS

After starting Zoom meetings, you can prevent unwanted guests from interfering with the meeting by editing the permissions of the participants.

01 LOCK THE MEETING

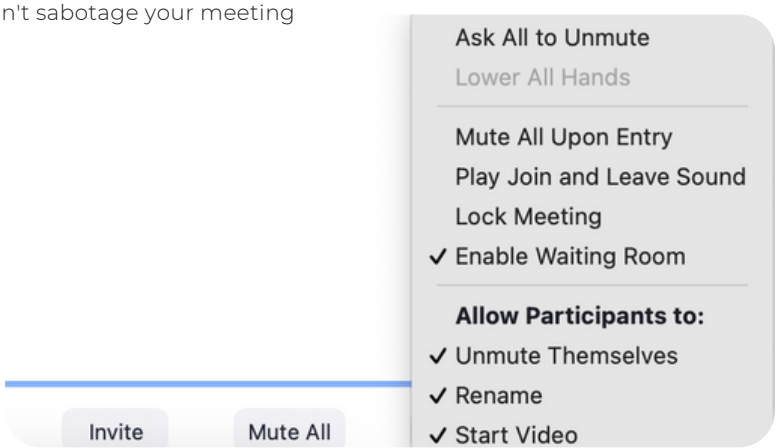
You can lock the meeting room after your students join. As long as your room is locked, no other participant will be able to enter your meeting room.

02 ENABLE WAITING ROOM

You can enable the waiting room even after the meeting has started. After the waiting room becomes active, attendees can only join the meeting with your permission.

03 MANAGE PARTICIPANTS

If there are users you don't know or behaving inappropriately in the participant list, you can remove participants from the meeting. You can also set the permissions of participants to mute/unmute, change names, and turn on their cameras. After removing the unmute themselves permissions and when your students want to communicate they can use the hand raise feature and/or the chat window to request permission. So, uninvited participants can't sabotage your meeting by sharing audio.



04 MUTE PARTICIPANTS

You can mute all users with the "Mute All" option. You can also prevent them from unmuting by clicking the "Unmute Themselves" option. Thus, you can be protected from voice attacks.

05 CONTROL SCREEN SHARING

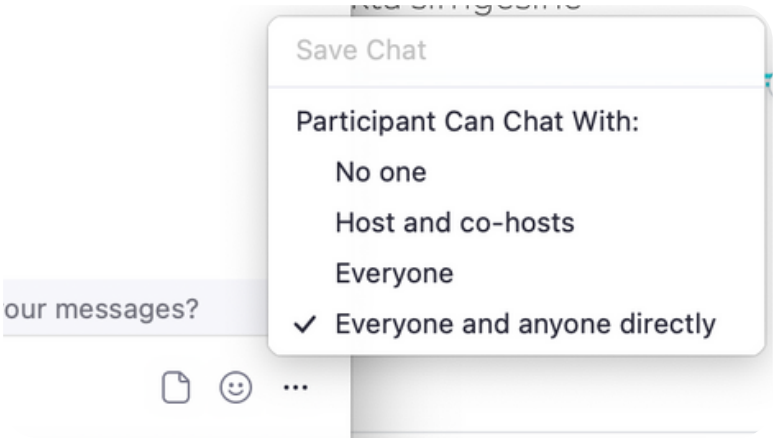
You can only allow the host to share screen in the meeting. Thus, you can prevent unauthorized sharing. For this, you can open the "Advanced Sharing Options" window by clicking the small arrow next to the "Share Screen/Content" option in the Zoom meeting.

06 TURN OFF ANNOTATION

After you start screen sharing, participants can make some annotations on the screen. To prevent these markings, you can click on the "Disable annotation for other" option in the "More" menu on the control bar that becomes visible after you start the screen sharing.

07 DISABLE CHAT WITH EVERYONE

You can control who the participants can chat with in the Chat window. You can prevent unsolicited messages from being written to the chat by editing the permissions of the participants. In some attacks, malicious links can be shared from the chat window. You can also ensure the safety of your participants by controlling chats. To change chat options, you can click on the three-dot icon at the bottom of the chat window.



Not all of our recommendations may be appropriate for each and every course or lecture. However, taking security measures is important for the safety of you and your students, and for the uninterrupted conduct of your live lessons.