Zoombombing – where trolls with ill-intent takeover Zoom meetings with inappropriate audio, video and/or chat - is a problem. These occurrences can be minimized by following the tips below. For large, public zoom events, the School of Social Sciences has determined that while we can minimize our exposure to disruptors through a combination of Zoom settings and hosting techniques, the opportunity for zoombombing can still exist. For these kinds of events, we can purchase Webinar licenses at $40 per month per account to limit chat, video and audio function to host-designated attendees.

When deciding how to host your Zoom event, we recommend following the basic guidelines below:

- Teaching a small class? Use Zoom, with OIT recommended settings (registered users, password)
- Teaching a larger class? Use Zoom, but absolutely use the OIT settings.
- Holding something small with a mix of UCI, non-UCI people? Use Zoom with our very restrictive settings and workflow detailed below.
- Holding anything large and facing the public? Use Zoom Webinar (contact sscs@uci.edu for assistance)

For departments and centers planning lectures, seminars, or other activities that involve members of the public, we suggest you contact sscs@uci.edu for advice. If you do use a Zoom meeting, we strongly suggest you:

1) Appoint one person to serve as the "host" in Zoom who will be responsible for establishing the correct settings and who will admit participants into the meeting in the manner discussed below. We will call that person the Meeting Host.
2) We strongly recommend that the Meeting Host be a staff member who has been trained in the procedures discussed below, not the actual faculty member or center director "hosting" the meeting.
3) Give the Meeting Host the sole authority to shut down the event immediately in the event Zoombombing takes place. This must be made clear to participants when events begin but also to faculty or center directors holding events—they have to understand that in the event of disruption, the Meeting Host will pull the plug and will communicate with attendees about alternative arrangements for the programming to continue or be rescheduled.
4) When you are holding a large event (a colloquium, a guest lecture, a roundtable), begin the event 10 minutes after the advertised start time, to provide the Meeting Host enough time to carry out the procedures described in **C** below.

For faculty teaching classes: If you use Zoom for synchronous instruction and want there to be opportunities for student interaction, breakout rooms, chat or voice discussion, then unfortunately this is one of the least secure ways to use Zoom. You can still mitigate the risk of being Zoombombed by following the instructions on the OIT website here (provide link) and NEVER SHARING THE LINK TO YOUR CLASS ZOOM MEETING PUBLICLY. Only share it via direct email to the students in your class, or from inside of Canvas, which requires students to log in using their UCINetID.

For information on webinar licenses or for other questions, please contact your computing support team at sscs@uci.edu.

How to host a secure Zoom meeting:

- Pick one person to serve as the meeting host.

- Disable Chat (see A below).
- Disable Screen Sharing (see A below).
- Make sure all participants are automatically placed in a waiting room at first (see B below).
- Mute Chat for everyone (see C below).
- Bring participants into the zoom meeting, one at a time (see C below).
- Mute the video of each participant, one at a time (see C below).
- SUGGESTION: Begin your meeting with a discussion about protocol and explain that if a zoombombing attack occurs, the meeting will be immediately shut down and resumed in private with a recording to be released following the event.

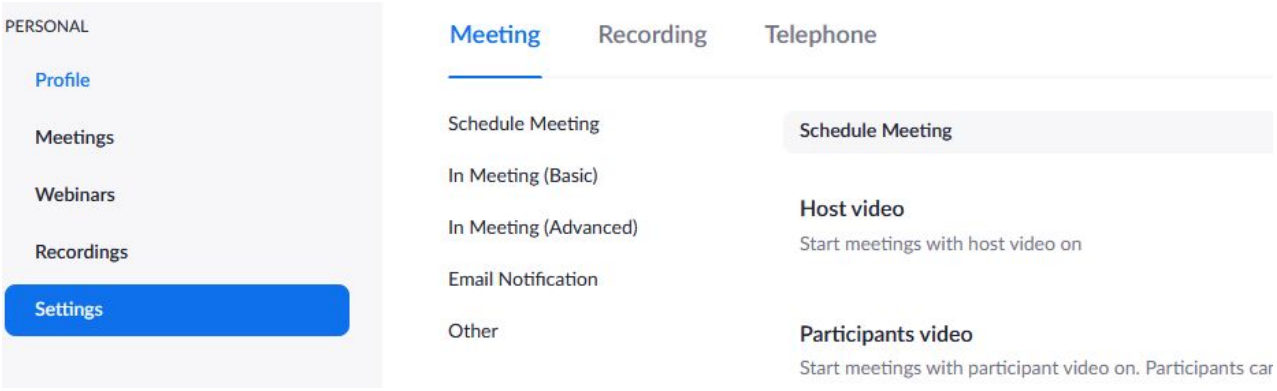
Again, note that if you have intentions to share a Zoom link publicly, there are still workarounds with zoombombing potential. The webinar license is your safest way to keep these attacks to a minimum. The trade off is that the webinar option is designed to limit audience participation; there are no breakout rooms available and audience members cannot easily interact with each other.

A. Before the meeting, we need to adjust our overall meeting settings to disable chat and screen sharing for participants.

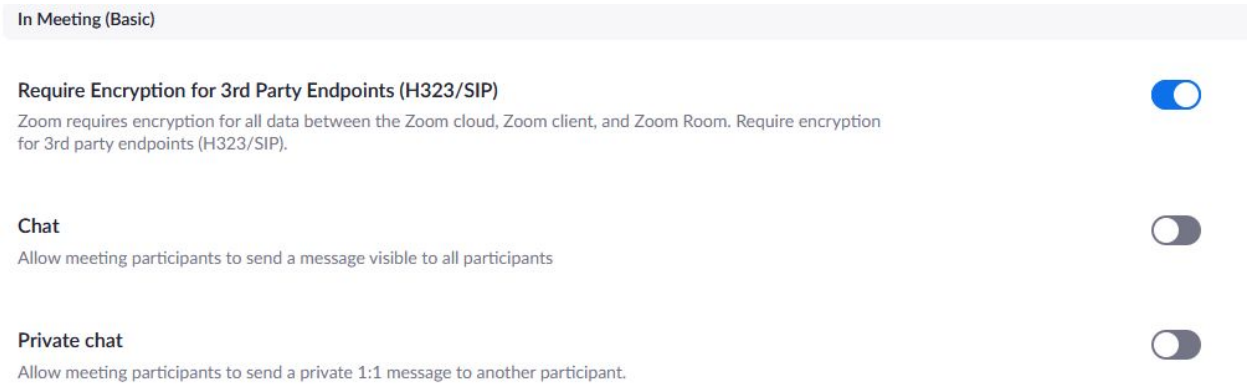
1. Login to your Zoom account via a web browser (not the Zoom app) by going to https://uci.zoom.us and clicking the "Sign In" button.

Note: If you are not asked to login, you may already be logged in. In that case, just click on "MY ACCOUNT" in the upper right-hand corner.

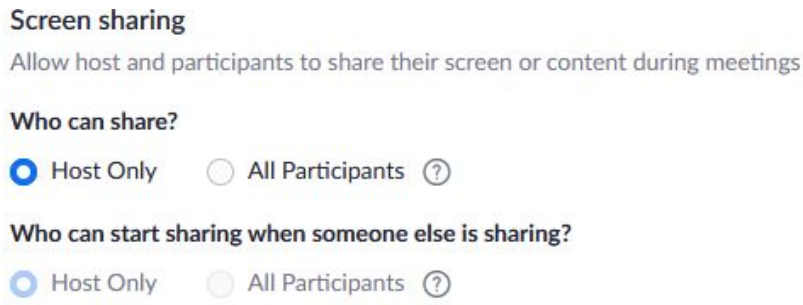
2. That will open your Zoom settings page. From the menu on the left, please click Settings.



3. Next click **In Meeting (Basic)** and make sure that **Chat** and **Private Chat** are both disabled (not blue) - as shown below:



4. Next, we will scroll down to the **Screen sharing** options to make sure that only the host can share their screen (as below).

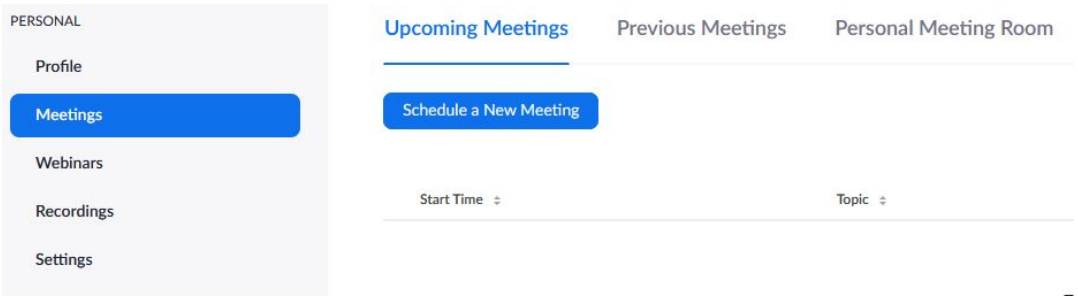


B. We also need to make sure that nobody can join before the host, and that everyone joining is placed into a waiting room until the host brings them into the meeting. This must be done in the settings for each individual meeting (or your personal meeting room settings, if you plan to use that room for your event).

1. Login to your Zoom account via a web browser (not the Zoom app) by going to https://uci.zoom.us and clicking the "Sign In" button.

Note: If you are not asked to login, you may already be logged in. In that case, just click on "MY ACCOUNT" in the upper right-hand corner.

2. That will open your Zoom settings page. From the menu on the left, please click Meetings.

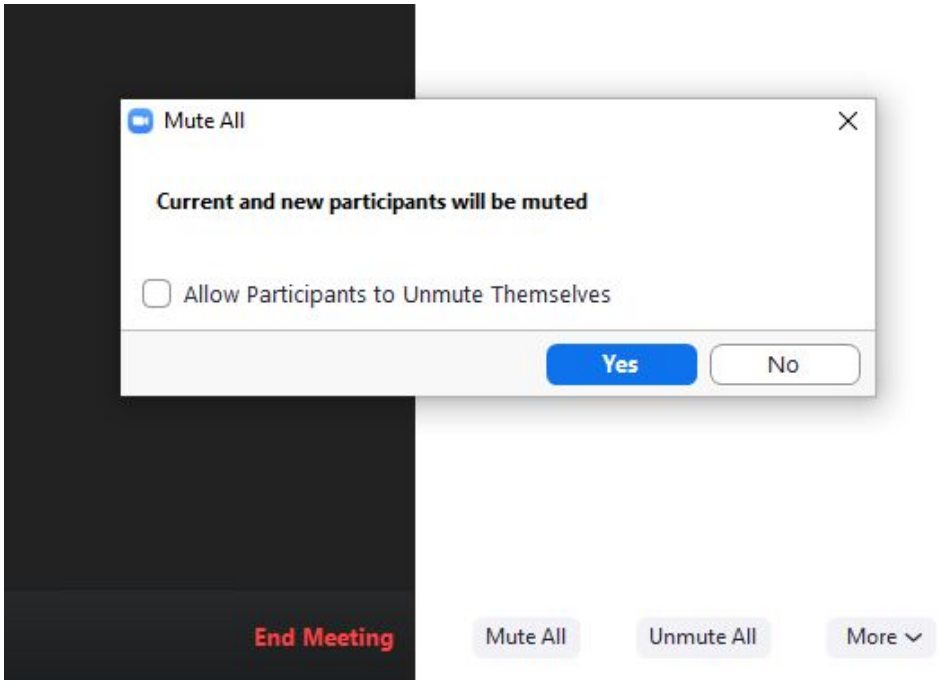


3. From here you can Schedule a new meeting, or click on your Personal Meeting Room. In either place, you will need to adjust your meeting settings to uncheck **Enable join before host** and check **Enable waiting room**.

Note: You may think that the **Mute participants on entry** would be useful, but checking this box does not prevent participants from unmuting themselves – that needs to be taken care of after the host is in the Zoom meeting.

C. After you have started the meeting, mute audio for everyone and don't allow participants to unmute themselves. Then allow participants into the meeting one at a time, muting the video of each participant one-by-one.

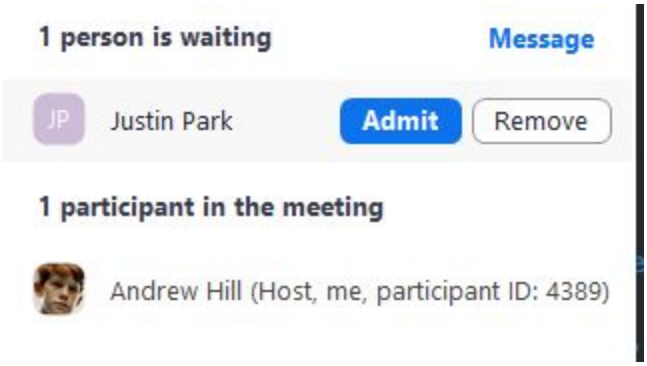
1. When you join the meeting, all other participants will sit in the waiting room. Before admitting anyone, mute the audio of all participants by selecting the **Mute All** button at the bottom of the participants. A dialog box will appear asking if you want to allow participants to unmute themselves. **Uncheck** that box (as below) and click **Yes**.



You want your screen to look like the image above: The box is **unchecked**. Then, click Yes. (As in: Yes, I do NOT want to allow participants to unmute themselves).

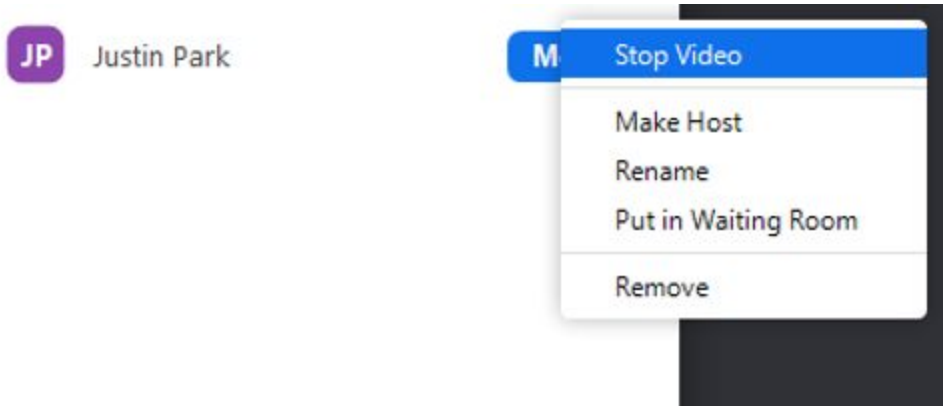
Note: If you don't see the participants list, please click the **Manage Participants** button at the bottom of your Zoom window.

2. Now you can admit participants one at a time. Click Admit to let them into the room as below.



If their video is active, you can mute their video as well (that will mute their video and not allow them to re-enable it). To mute a participant's video, click on the camera icon next to their name in the participants window.

Clicking on the camera icon will bring up a small menu. Select **Stop Video.**



This must be done for each participant.

3. At this point your Zoom meeting is as secure as we can make it. The only issue would be if a participant did not have video active when you allow them in from the meeting room. If their video is not active, you are not able to mute it. They could enable their video for the first time during the meeting and attempt to disrupt the meeting with content from their video camera. The Meeting Host will need to be attentive to the video feed from participants and mute ANY whose feed is active (i.e., showing anything other than a black box/profile picture with a name in it).