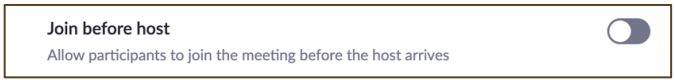
HOW TO PREVENT AND MANAGE "ZOOMBOMBING"

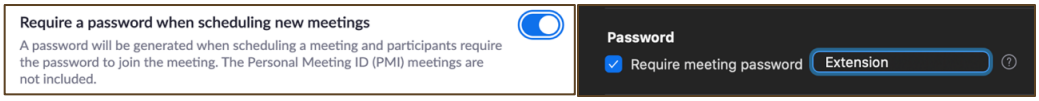
"Zoombombing" is generally defined as an instance in which virtual meetings are disrupted by graphic or threatening messages or actions, inappropriate content, or internet trollers. To ensure the safety of our meetings with both youth and adults, follow this guide in an effort to prevent "Zoombombing" from happening during your meeting.

When Scheduling a Meeting:

Disable "Join Before Host" to keep users out of the meeting before the host arrives. This is the default setting, but make sure it is set prior to your meeting. (web-based settings only)



Create a Password to allow specific users to join the meeting. (web settings and desktop app)

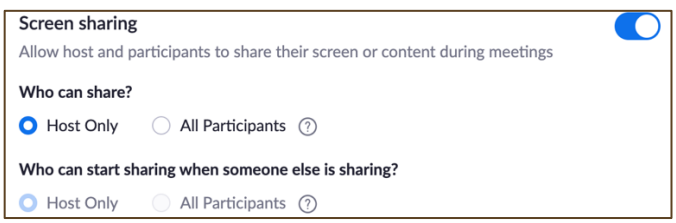


Disable "Join After Removed" to ensure that the participants you have removed from the meeting are unable to rejoin. (web settings only)

To create an even more secure environment, DISABLE the following options. However, make sure to consider that disabling these features will create user limitations within the meetings. With some of these features, you can adjust the settings during the meeting to allow only the host to have access.

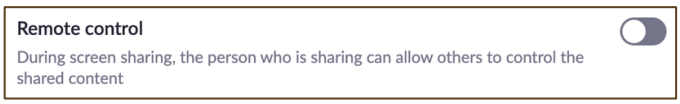
Disable "File Transfer" to ensure that inappropriate files can't be sent through the in-meeting chat. This also means that no one can send any files, not even the host. This is a default setting for the majority of users with UWyo credentials and can't be changed.

Disable "Screen Sharing" or Enable "Host Only" Sharing to prevent participants from sharing their screen. *This setting can be changed during a meeting if you need to allow a specific user the ability to screen share* (web settings and in-meeting).

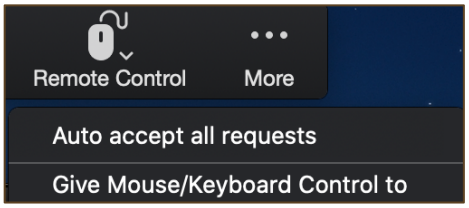


HOW TO PREVENT AND MANAGE "ZOOMBOMBING"

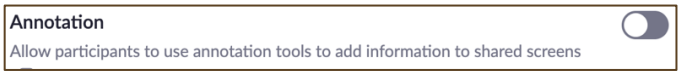
Disable "Remote Control" to prevent all participants, including the host, from controlling screen-shared content of others. This CAN NOT be changed in-meeting (web settings only).



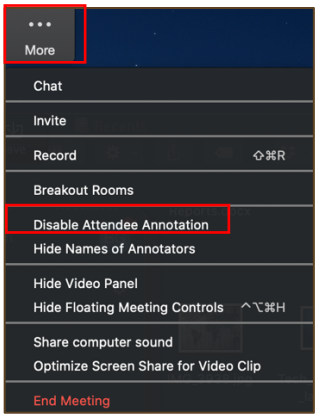
*If "Remote Control" is **enabled**, during the meeting participants can ask permission to control other screens. The requested user can choose to accept or deny the request.*



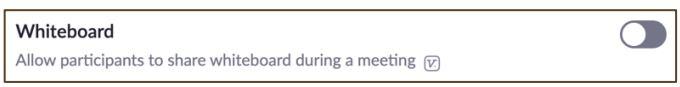
Disable "Annotations" to prevent all users, including the host, from writing and adding information to shared screens. This CAN NOT be changed in-meeting (web settings only).



*If "Annotations" is **enabled**, during the meeting participants can annotate a shared screen. If you would like for the host to only have access to annotating a screen, you must "Disable Attendee Annotation" from the toolbar. It is advised you make this change immediately after sharing your screen.*



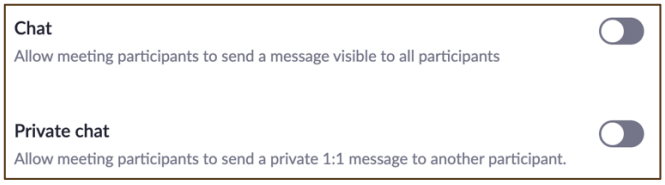
Disable "Whiteboard" to prevent all users, including the host, from sharing their whiteboard during a meeting. This CAN NOT be changed in-meeting (web settings and in-meeting).



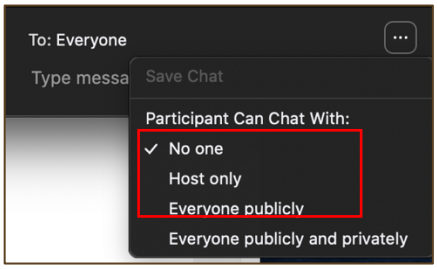
HOW TO PREVENT AND MANAGE "ZOOMBOMBING"

*If "Whiteboard" is **enabled**, during the meeting participants can draw (annotate) on a shared whiteboard. If you would like for the host to only have access to writing on the whiteboard, you must "Disable Attendee Annotation" from the toolbar. It is advised that you make this change immediately after sharing your whiteboard. (The process is the same for Annotations.)*

Disable "Chat" to prevent participants from writing messages to each other. You can disable all chat features or just private (one-to-one) messages (web settings and in-meeting).



*If "Chat" is **enabled**, during the meeting the host can adjust the chat settings to how they see fit.*

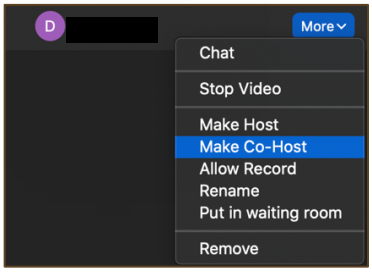


Enable "Waiting Room" to allow you to manually choose which users will be allowed into the meeting. You can also customize your Waiting Room settings by creating a personalized message so those in the Waiting Room can know that they are in the right spot. This is also a great way to post your policies or guidelines for the meeting (web settings only).

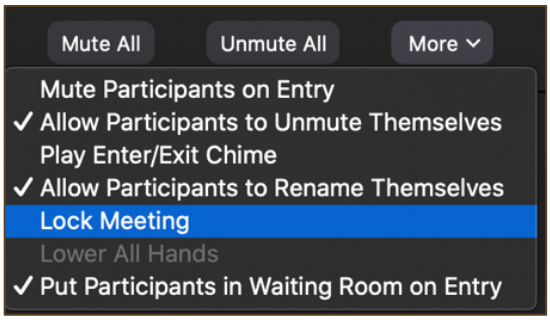
Send Zoom meeting invitations privately so that people who were not intended to join the meeting, don't have access to the link. Email the link directly to participants or post the link on private Facebook pages or groups. Limit posting the meeting link to public platforms.

While in a Meeting:

Assign multiple Co-Hosts to give host responsibilities to other participants which will allow for greater supervision and whose specific role can be to monitor and manage participants.

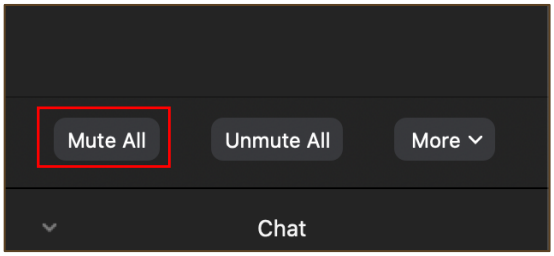


Lock Meeting when all participants have joined. This creates a closed meeting where no one else can join. Click on the "Manage Participants" button in the toolbar. Then, click on the "More" button beneath the list of participants.

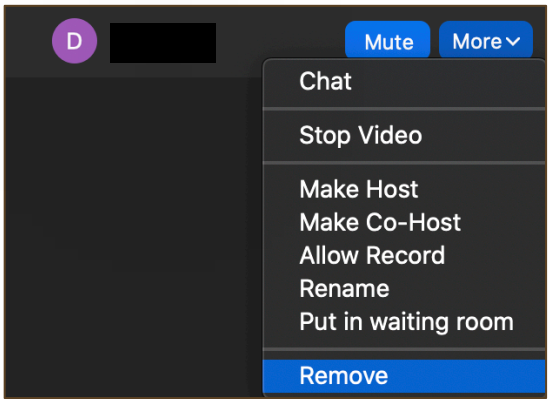


If Meeting is Bombed:

Mute All attendees to silence any audio chaos.



Remove the users from the meeting. They will not be allowed to rejoin the meeting if you disabled "Join After Removed" in your settings prior to the meeting.



Lock Meeting to prevent additional participants from joining.