

Ways to avoid Zoombombing

What is Zoombombing?

Zoombombing refers to the act of uninvited parties entering a Zoom meeting room ID and joining into the open meeting. They will often do this with the specific purpose of “trolling” the meeting participants by broadcasting unsavoury messages to the group or posting sexually explicit content to the meeting.

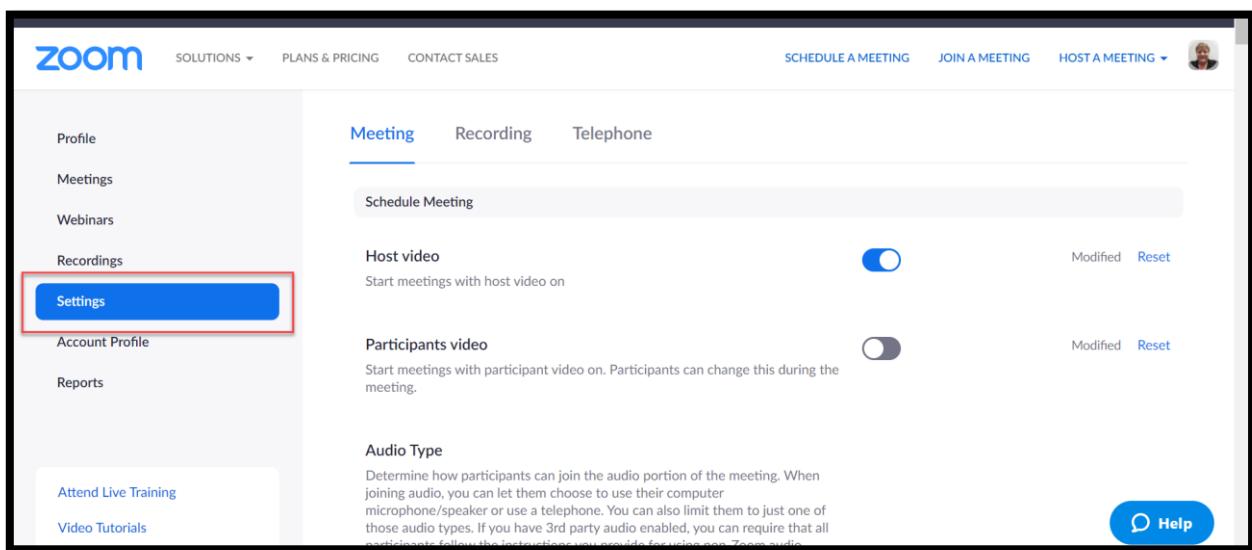
These individuals may be hackers, or, if the Zoom meeting room ID is posted publicly, it can be easily found through a Google search or via the VU class list.

Fortunately, the Zoom platform has inbuilt functionality to assist you in preventing this from occurring.

How can I prevent Zoombombing?

To activate the preventative measures described below, you must first log in and go to your Zoom settings. (victoriauniversity.zoom.us)

Zoom Guides for Virtual Classrooms are also accessible via VU Collaborate for additional reference: <https://vucollaboratehelp.vu.edu.au/help-guides/communication/virtual-classrooms/692-stop-zoom-bombing-with-these-strategies>



1. You can set up a meeting password. Once turned on you can send the password directly to the participants so that only they can join.

Require a password when scheduling new meetings 

A password will be generated when scheduling a meeting and participants require the password to join the meeting. The Personal Meeting ID (PMI) meetings are not included.

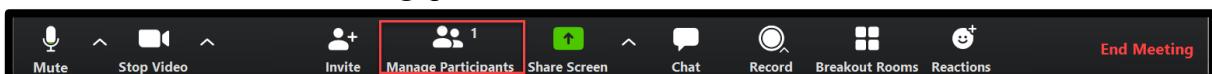
2. Enable the “Waiting room” feature. This lets you allow or block participants from entering and you can block any unwanted strangers from entering during the session

Waiting room 

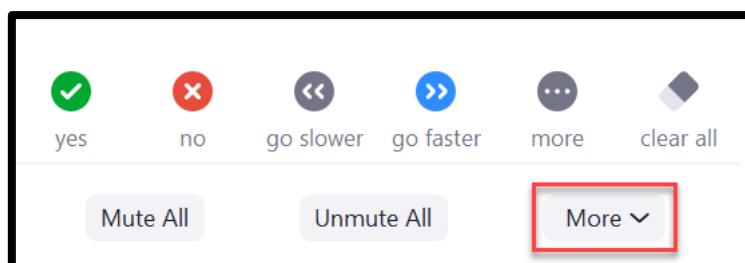
Attendees cannot join a meeting until a host admits them individually from the waiting room. If Waiting room is enabled, the option for attendees to join the meeting before the host arrives is automatically disabled. [\[V\]](#)

3. You can Lock the meeting to prevent anyone new from joining.

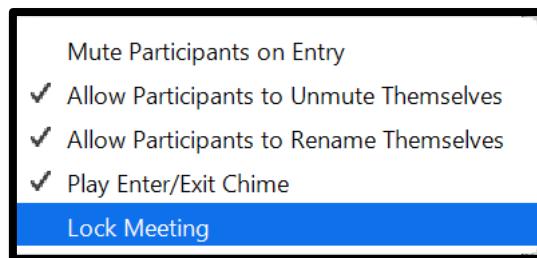
Once in the Zoom meeting go to the toolbar



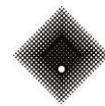
Select More



Lock Meeting



4. Don’t use your Personal Meeting Room. Make sure the below settings are off. If your personal room ID is stored or shared online, unwanted parties could try to enter your future meetings.



Use Personal Meeting ID (PMI) when scheduling a meeting



You can visit [Personal Meeting Room](#) to change your Personal Meeting settings.

Use Personal Meeting ID (PMI) when starting an instant meeting



5. Mute participants upon entry, this also allows you control on who is muted or unmuted during the meeting.

Mute participants upon entry



Automatically mute all participants when they join the meeting. The host controls whether participants can unmute themselves. [\[V\]](#)

6. Staff can choose an authentication method that participants will be required to complete prior to joining the meeting

Only authenticated users can join meetings



The participants need to authenticate prior to joining the meetings, hosts can choose one of the authentication methods when scheduling a meeting.

7. Decide whether your participants will need to share their screen, if not you can ensure only you have screen sharing control

Screen sharing



Allow host and participants to share their screen or content during meetings

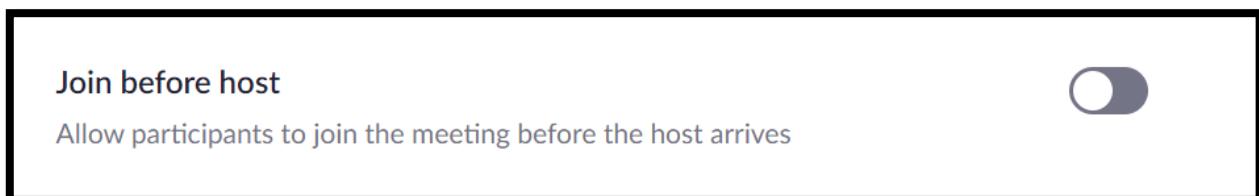
Who can share?

Host Only All Participants [\[?\]](#)

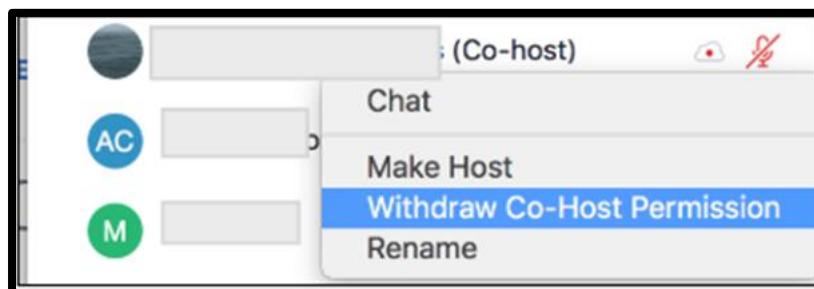
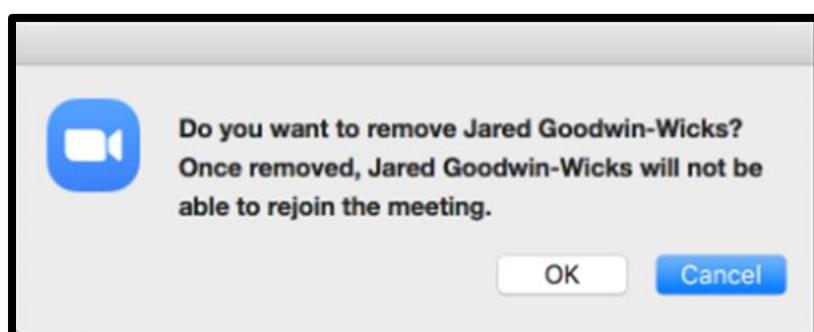
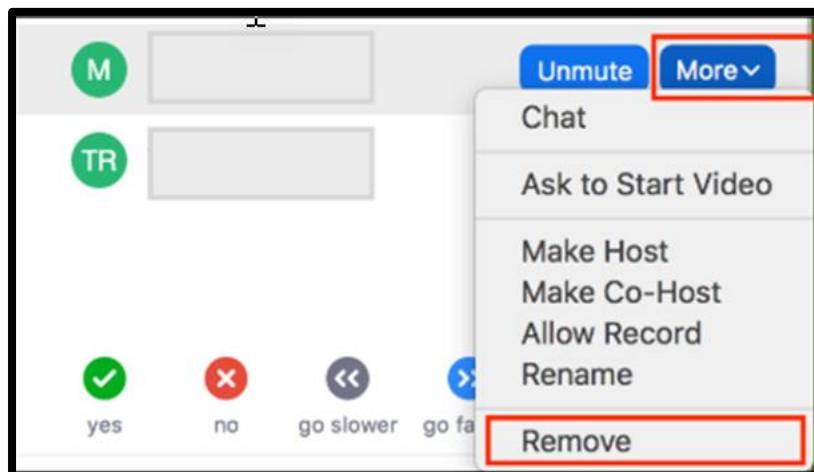
Who can start sharing when someone else is sharing?

Host Only All Participants [\[?\]](#)

8. You can turn off “Join before host” so that no one can be in the meeting before you start it. This way you can control who enters.



9. If someone enters the room that should not be there you may also remove them



REFERENCES:

<https://news.aarnet.edu.au/zombombing-and-how-to-prevent-it/>

<https://www.youtube.com/watch?v=XhZW3iyXV9U&feature=youtu.be>