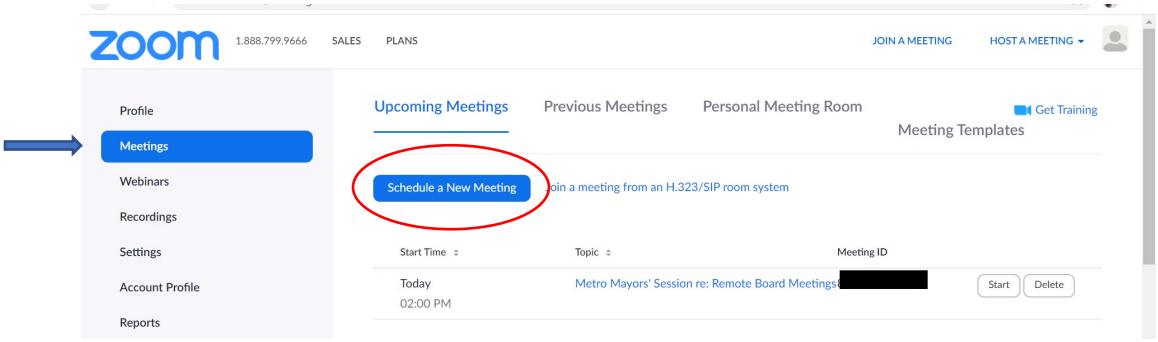
Tips and Tricks to Help You Avoid Zoom Bombing

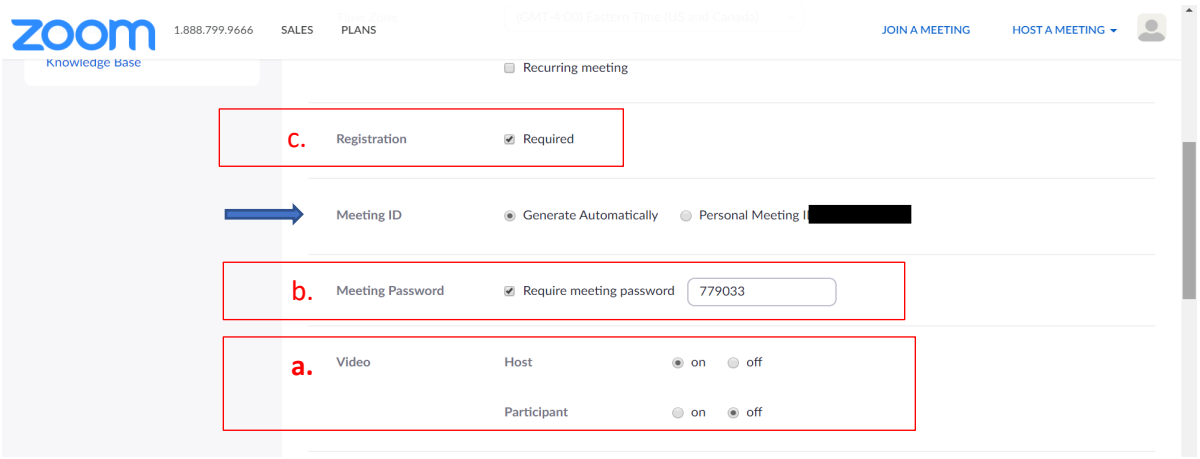
There are several ways to manage your Zoom account profiles to prevent Zoom Bombing from happening. This step by step guide highlights the settings you will want to change on your Zoom account to create greater security while using this application. First, this guide demonstrates how to adjust the room settings within the Meetings tab when you are scheduling a new meeting. Then it shows how to adjust your Settings for persistent control over specific areas which is applied to all meetings until you change those settings.

Meeting Controls:

1. Log into the Host Zoom account being used for the meeting and navigate to Meetings.

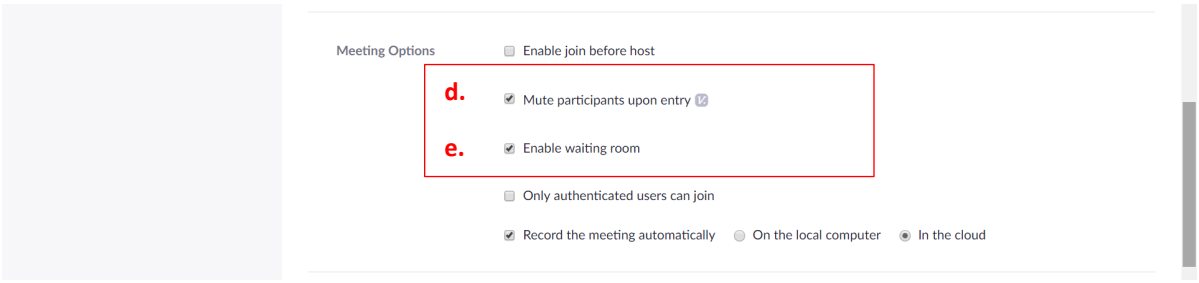


2. When scheduling an upcoming meeting, always generate the Meeting ID randomly and do not use your Personal Meeting ID. This is done under the Meetings section when you click on Schedule a New Meeting.



3. I personally advise that you enable the following items as well, as labeled above.
    a. Registration: Required
    b. Meeting Password: Require Meeting Password.
    c. Video: Host On, Participant Off

Shannon H. Tufts, PhD
Associate Professor and Director of the Center for Public Technology
tufts@sog.unc.edu; 919.962.5438

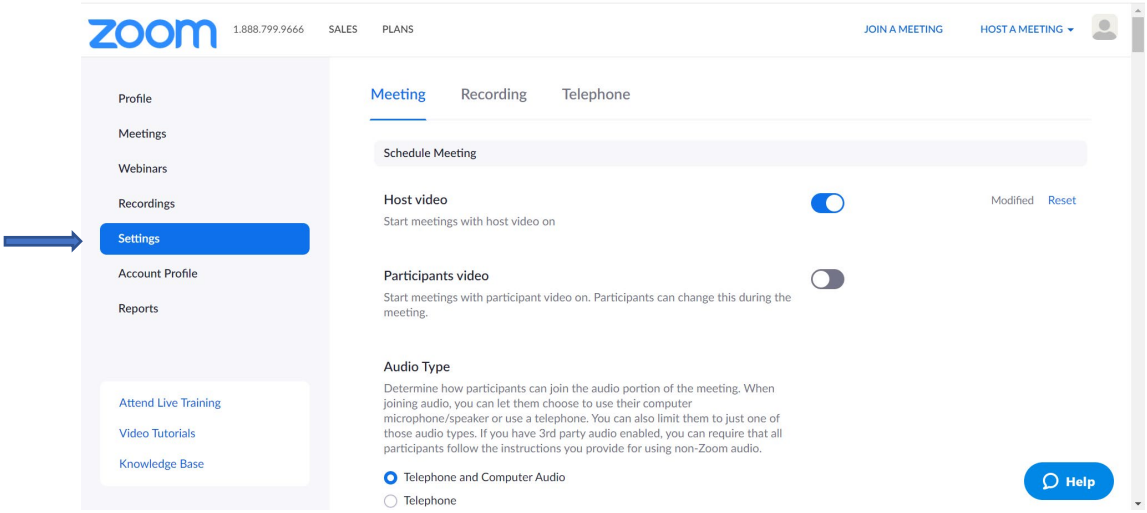


Additionally, you want to Mute Participants Upon Entry (item d) and Enable Waiting Room (item e) as noted above.
**You will notice I don't have Only Authenticated Users Can Join because when I tested the software with my parents (in their mid 70s), it created too many obstacles for them to use the software.

4. The Waiting Room is a great tool. It allows you to admit people into the virtual meeting after the Host is ready for them. This feature allows a level of control, even if you have 100s of people attending the meeting because you can use it to send a participant back to the Waiting Room if they are exhibiting bad behavior (basically a virtual timeout). You can also customize the Waiting Room area with your logo and the meeting room title, so your participants know they are in the right place.

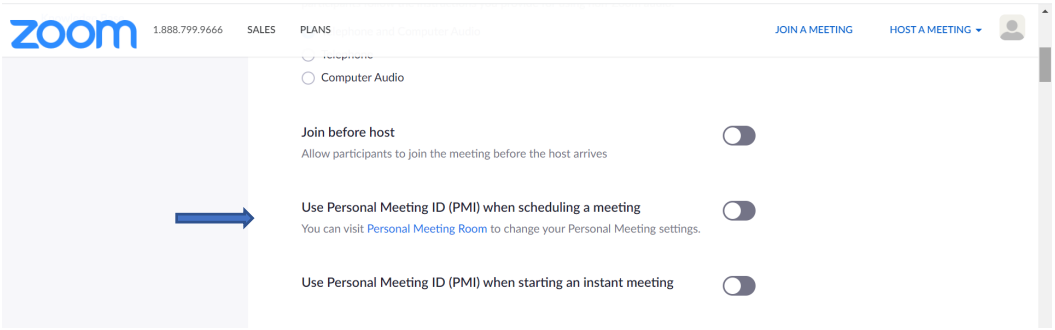
Setting Controls: In order to change Settings that apply to all meetings under the Host account, follow these steps.

5. Log into the Host Zoom account being used for the meeting and navigate to Settings.



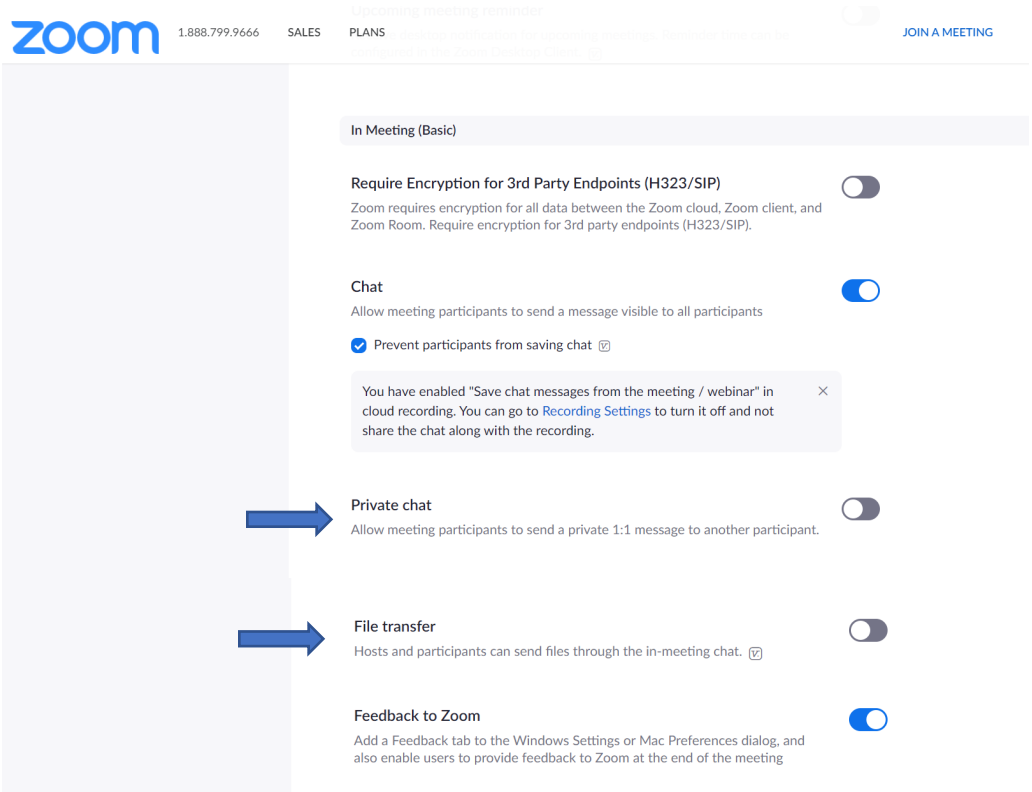
Shannon H. Tufts, PhD
Associate Professor and Director of the Center for Public Technology
tufts@sog.unc.edu; 919.962.5438

6. As noted before in the Meetings settings, don't use your Personal Meeting ID (PMI) for public Zoom meetings, as this is a persistent ID attached to your account. This setting should be toggled Off in order to prevent any scheduled meetings from using your PMI.



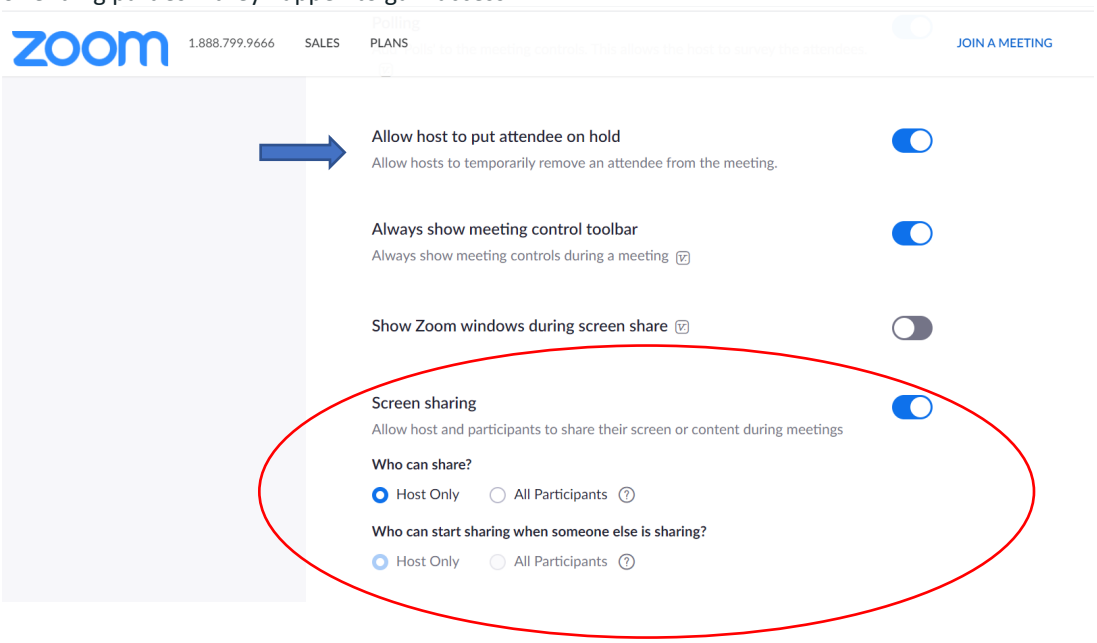
7. Under the first section of Settings, which is "Schedule Meeting", you can make persistent changes for all meetings similar to what was done for the specific meeting being scheduled above, like "Host Video On, Participant Video Off", "Require Password", "Mute Participants Upon Entry", etc.

8. Scrolling down to "In Meeting (Basic)", you can either allow or disallow public chat features. You should "Disable Private Chat" to prevent inappropriate materials, personal threats, etc. from being sent during the meeting. Also disable the "File transfer" option for the same reason.



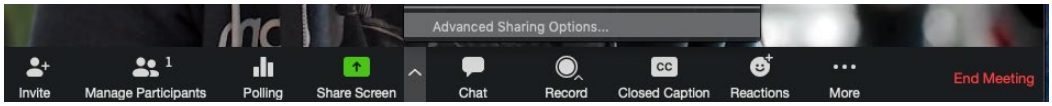
Shannon H. Tufts, PhD
Associate Professor and Director of the Center for Public Technology
tufts@sog.unc.edu; 919.962.5438

9. Enable “Allow host to put attendees on hold” (aka virtual time out) in your Settings, which allows you to remove offending parties if they happen to gain access.

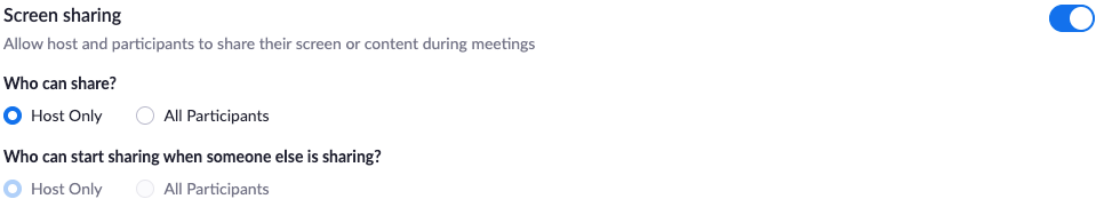


   a. Once you are in the meeting, if a participant is causing issues, go to the “Participants” menu, mouse over the participant’s name, and several options will appear, including Remove.

10. One of the most important features to prevent Zoom Bombing is noted in red above. Always have your settings to “Who can share? Host only” under the Screen Share setting to prevent participants from screen sharing.
   a. You can also do this during the Zoom meeting using meeting host controls by clicking the arrow next to Share Screen and then Advanced Sharing Options.

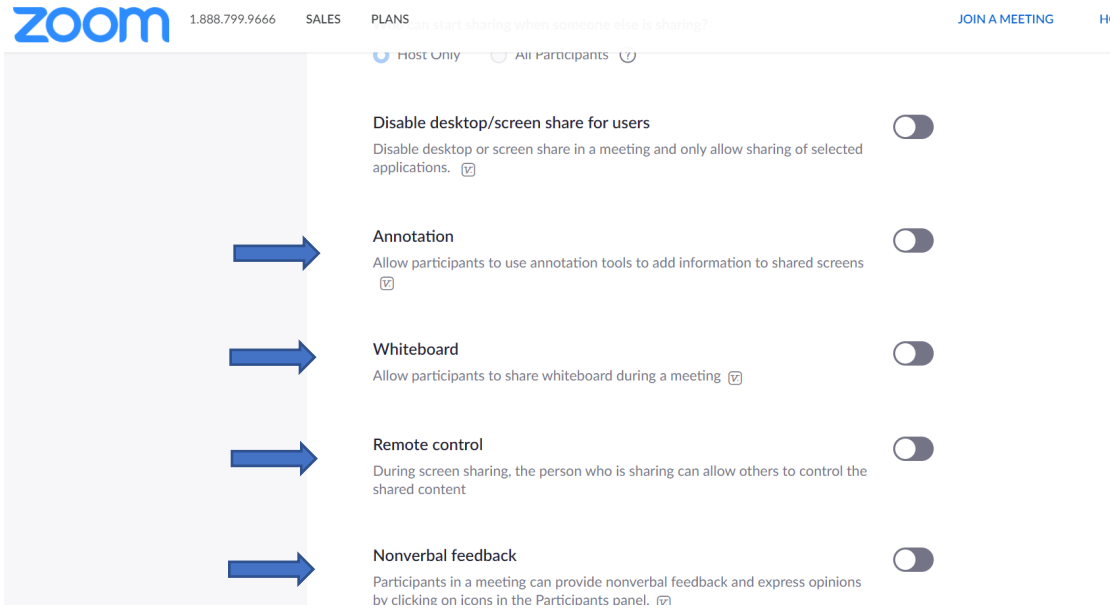


Under “Who can share?” choose “Only Host” and close the window. You can also lock the Screen Share by default for all your meetings in your web settings.



Shannon H. Tufts, PhD
Associate Professor and Director of the Center for Public Technology
tufts@sog.unc.edu; 919.962.5438

11. Other settings to help maintain control of your screen and event include Disabling Annotation, Whiteboard, Remote Control, and NonVerbal Features, as noted below.



12. Finally, once your meeting starts, it is a good idea to **Lock the Meeting** once it begins. When you lock a Zoom Meeting that's already started, no new participants can join, even if they have the meeting ID and password.
    a. To lock the meeting, click Participants at the bottom of your Zoom window. In the Participants pop-up, click the button that says Lock Meeting.

Shannon H. Tufts, PhD
Associate Professor and Director of the Center for Public Technology
tufts@sog.unc.edu; 919.962.5438