Preventing Zoom-Bombing and Zoom Security Best Practices

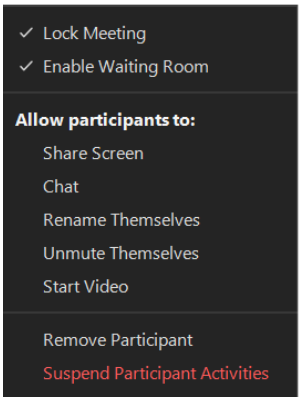
What is Zoom-bombing? Zoom-bombing: uninvited participants join a Zoom Meeting already in progress with the purpose to disrupt proceedings by sharing disturbing pornographic images and/or violent imagery and communicate racial and ethnic slurs. This can happen when a meeting link is shared through public communication sources such as social media or when perpetrators randomly select numbers to join Zoom meetings.

Reminders on Using Zoom When Hosting Public Meetings

Avoid using your Personal Meeting ID to host public events. You should always set a password (passcode) for your meeting. Check here for more information on scheduling meetings.

If you use Meeting registration, consider using **Manually Approve** to control late registrations who could enter your meeting.

In-Meeting Security Controls



The **Security** option provides you, as meeting host, with several important tools that should be configured before participants arrive. Limit **Screen Share** to hosts only. (This option is also available from the separate **Share Screen** option.) If you have multiple presenters in your meeting, you can set them to Co-Hosts by opening the **Participants** window, choosing the **More** option next to their name and changing their status to Co-Host. Disable private chat: uncheck **Chat** in Security or, at the bottom of the Chat window, click **More** (…) then choose an option for **Allow attendees to chat with**. Uncheck **Rename Themselves** to prevent potential zoom-bombers from concealing their identity. Uncheck **Unmute Themselves** to prevent participants from using their microphone. Uncheck **Share Video** to disable the participant's ability to share their video/webcam view. Once all your attendees arrive or once you begin your meeting, consider locking your meeting with **Lock Meeting**. This prevents anyone, even registered users, from entering the meeting. Enable the **Waiting Room** to force participants into a virtual staging area before being allowed into a session. If you are interested in using a Waiting Room by default, enable this option when you set up your Meeting. Finally, use the **Suspend Participant Activities** option if your meeting zoom-bombed. This will remove all sharing abilities from all participants and then allow you to report or kickout any unwanted participants.

Manage Your Participants

Remove unwanted or disruptive participants, disable participant's video, mute participants. From **Participants** window, mouse over a participant's name and several options will appear, including **Remove**. Once a participant is removed from the Meeting, they cannot rejoin with the same user information. **Disable video** - Hosts can turn someone's video off. This will allow hosts to block unwanted, distracting, or inappropriate video. **Mute participants** - Hosts can mute/unmute individual participants or all of them at once. Hosts can block unwanted, distracting, or inappropriate noise from other participants. You can also enable **Mute Upon Entry** in your settings. Turn off annotation: **Disable annotation** for participants to prevent annotating over content being shared during the meeting.

Best Practices

To minimize the risk of zoom-bombing, before the meeting begins disable participants microphones, disable their ability to screen share and annotate, disable their ability to chat with anyone but you (host), do not allow them to rename themselves, enable the waiting room and have all participants muted when they enter. After your meeting begins, lock the meeting. After you have started your meeting and the meeting is locked, scan your list of participants. Be ready to remove any participant whose username is inappropriate or in question. Feel free to privately chat with them to get more information. Once you feel safe about the participants, you may choose to allow them to chat and open their microphone.

Be Prepared

If you are hosting or co-hosting a session and find your session is being overrun by hackers intent on ruining your session, use **Security** to ensure the meeting is locked, the waiting room is enabled, and all participants' ability to share screen, chat, rename themselves, unmute themselves and share video is not checked (disabled). Then, immediately remove offending participants or use the report option. If you have a co-host, before the meeting begins assign corrective actions to each person.

For more information:

- https://blog.zoom.us/best-practices-for-securing-your-virtual-classroom/
- https://zoom.us/docs/doc/Securing%20Your%20Zoom%20Meetings.pdf
- https://support.zoom.us/hc/en-us/articles/360041848151-In-meeting-security-options
- https://support.zoom.us/hc/en-us/articles/201362603-Host-and-Co-Host-Controls-in-a-Meeting
- https://support.zoom.us/hc/en-us/articles/115005759423