

Settings for Preventing Zoom-Bombing

What is Zoom-bombing?

Zoom-bombing is the term for when individuals "gate-crash" Zoom meetings. These uninvited guests share their screens to bombard real attendees with disturbing pornographic and/or violent imagery. Most of these are perpetrated via publicly available Zoom links; however, not all depending on your settings. Here are ways to protect you and your guests from falling victim.

Reminders on using Zoom to host public events

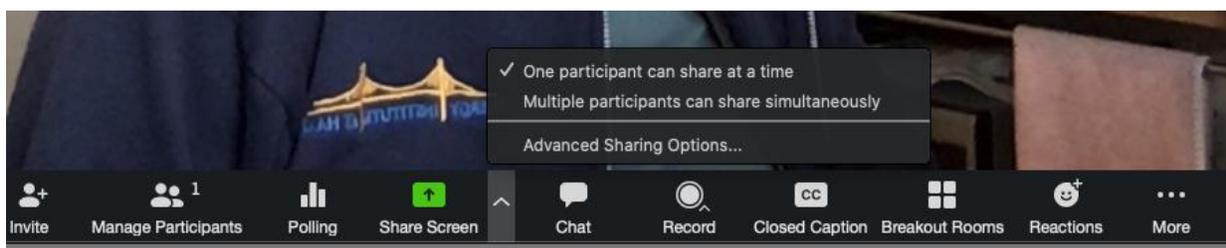
If you share your meeting link on social media or another public location (like a public bCal invite) anyone with the link can join your meeting. Here are some tips you can use to help when needing a public meeting space:

- **Avoid using your Personal Meeting ID (PMI) to host public events.** Your PMI is essentially one continuous meeting and people can pop in and out all the time. Learn about meeting IDs and how to generate a random meeting ID (at the 0:27 mark) in this [video tutorial](#).
- **Familiarize yourself with Zoom's settings and features.** Understand how to protect your virtual space. e.g., use a [Waiting Room](#) (additional details on that below). The waiting room is a helpful feature for controlling attendees.

Read on for a list of Zoom features that can help you safely share your Zoom without unwanted interruptions.

I. Manage screen sharing

Don't give up control of your screen, especially if you are hosting a public event. You can control this either before or during the meeting in the host control bar settings. To prevent participants from screen sharing during a call, using the host controls at the bottom, click 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.

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

Who can share?

Host Only All Participants ?

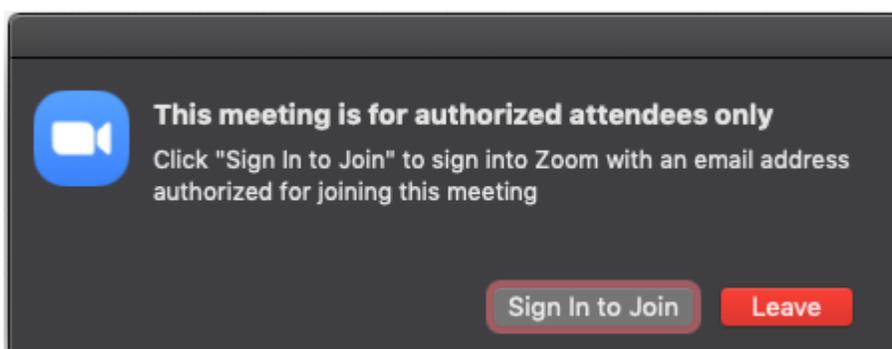
Who can start sharing when someone else is sharing?

Host Only All Participants ?

II. Manage your participants

Some other features to help secure your Zoom event and host with confidence:

- **Allow only signed-in users to join:** If someone tries to join your event and isn't logged into Zoom with the email they were invited through, they will receive this message:



This is useful if you want to control your guest list by invite only to your meeting.

- **Lock the meeting:** When you lock a Zoom Meeting after it has started, no new participants can join, even if they have the meeting ID and password (if you have required one). In the meeting, click Participants at the bottom of your Zoom window. In the Participants pop-up, click the button that says Lock Meeting.
- **Set up your own two-factor authentication:** You don't have to share the actual meeting link. Generate a random Meeting ID when scheduling your event and require a password to join. Then you can share that Meeting ID through a public setting/social media and only send the password to join by email or direct message.
- **Remove unwanted or disruptive participants:** From that Participants menu, you can hover over a participant's name, and several options will appear, including Remove.

- **Allow removed participants to rejoin:** When you do remove someone, they can't rejoin the meeting. But you can toggle your settings to allow removed participants to rejoin, in case you remove the wrong person.
- **Put them on hold:** You can put each participant on a temporary hold, including the attendees' video and audio connections. Click on someone's video thumbnail and select Start Attendee On Hold to activate this feature. Click Take Off Hold in the Participants list if/when you're ready to have them back.
- **Disable video:** Hosts can turn someone's video off. This will allow hosts to block unwanted, distracting, or inappropriate gestures on 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 to keep the noise down in large meetings.
- **Turn off file transfer:** In-meeting file transfer allows people to share files through the in-meeting chat. Turn this off to keep the chat from getting unwanted content.
- **Turn off annotation:** You and your attendees can doodle and mark up content together using annotations during screen share. You can disable the annotation feature in your Zoom settings to prevent people from using it.
- **Disable private chat:** Zoom has in-meeting chat for everyone or participants can message each other privately. Restrict participants' ability to chat with each another during your meeting. This prevents anyone from getting messages during the meeting.

III. Use a Waiting Room

One of the best ways to use Zoom for public events is to enable the [Waiting Room](#) feature. The Waiting Room is a virtual staging area that stops your guests from joining until you're ready for them, like a bouncer carefully monitoring who gets let in. Meeting hosts can customize Waiting Room settings for additional control, and you can even [personalize the message](#) people see when they hit the Waiting Room so they know they're in the right spot.

The Waiting Room is really a great way to screen who's trying to enter your event and keep unwanted guests out.

Tips courtesy of Zoom and UC Berkeley