ASSINIBOINE COMMUNITY COLLEGE

Taking Zoom to the Next Level - Preventing Zoombombing

What is Zoombombing?

Zoombombing 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, but this is not always the case. Here are ways to protect you and your guests from falling victim.

Protect All Public Meetings:

If you share your meeting link in a public location, anyone with the link can join your meeting. If you need to have a public meeting, avoid using your Personal Meeting ID to host public events.

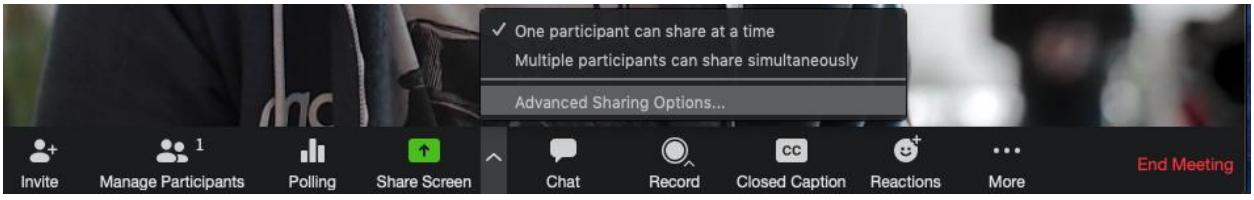
Your Personal Meeting ID is essentially one continuous meeting and people can pop in and out all the time. Learn about meeting IDs and how to generate a random meeting ID (at the 0:27 mark) in this video tutorial.

Manage Screen Sharing:

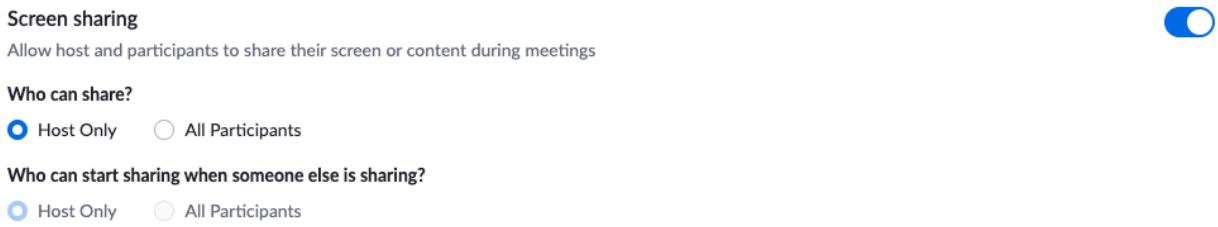
The first rule of Zoom: Don't give up control of your screen.

You *do not* want random people in your public event taking control of the screen and sharing unwanted content with the group. You can restrict this — before the meeting and during the meeting in the host control bar — so that you're the only one who can screen-share.

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**.



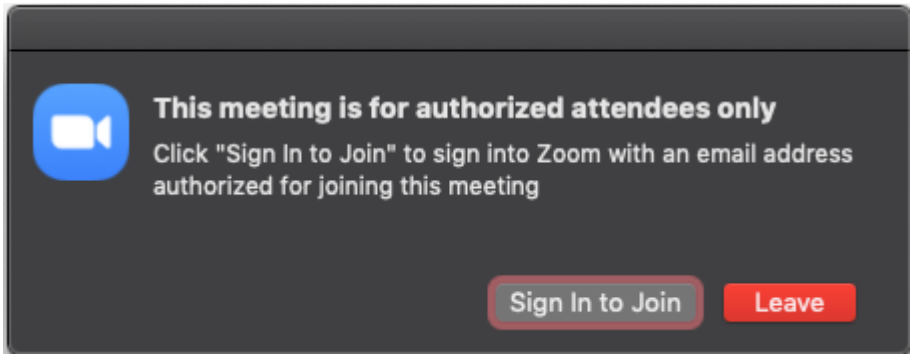
Under **"Who can share?"** choose **"Only Host"** and close the window. You can also lock the **Share Screen** by default for all your meetings in your web settings.



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 and invite only those you want at your event — other students at your school or colleagues, for example.

- **Lock the meeting:** When you lock a Zoom Meeting that's already 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, but only send the password to join via DM.

- **Remove unwanted or disruptive participants:** From the **Participants** menu, you can mouse over a participant's name, and several options will appear, including **Remove**. Click that to kick someone out of the meeting.

- **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 boot 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 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. Toggle this off to keep the chat from getting bombarded with unsolicited pics, GIFs, memes, and other 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 amongst one another while your event is going on and cut back on distractions. This is really to prevent anyone from getting unwanted messages during the meeting.

Use a Waiting Room

One of the best ways to use Zoom for public events is to enable the Waiting Room feature. Just like it sounds, 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. This message is the perfect place to post rules or guidelines for your meeting.

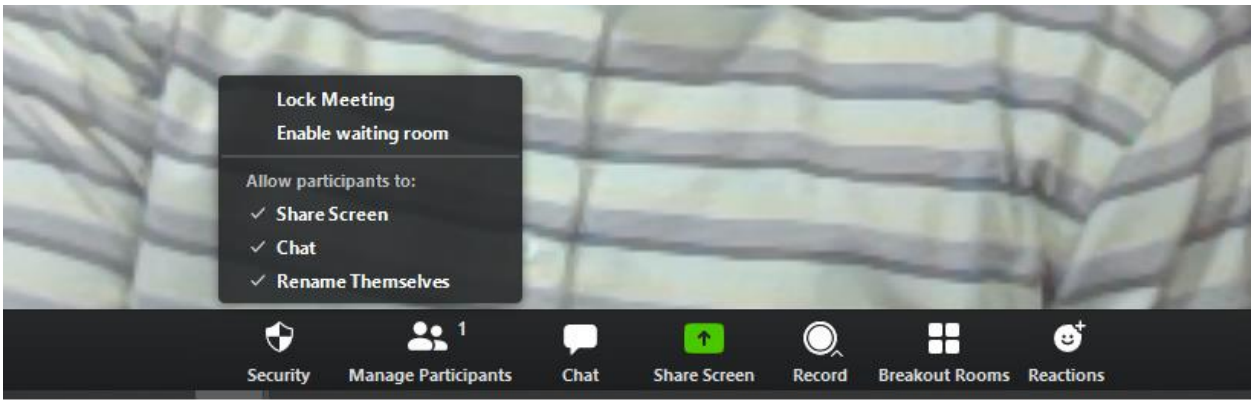
The Waiting Room is really a great way to screen who's trying to enter your event and keep unwanted guests out.

You can also choose secure settings before starting a private class or meeting. Go into your settings page and switch on **"Require a password when scheduling new meetings."** (You can also require a numeric code for people calling on the phone.) That's one way to keep out any unwanted guests.

Update – Security Button

Since publishing this guide, Zoom has added a **Security** button that enables users to manage several of the settings that can prevent zoombombing. The picture below provides a good example of these options than can be either enabled or disabled directly from the meeting screen.

As a reminder, enabling the waiting room function allows the host/presenter to admit or deny access to anyone trying to join the meeting, preventing unauthorized meeting access. In addition, de-selecting **allow participants to share screen** prevents a student or guest from sharing their desktop inadvertently or maliciously.



Adapted from "Settings for Preventing Zoom-Bombing" by Berkeley Information Security Office: https://security.berkeley.edu/resources/cybersecurity-and-covid-19/settings-preventing-zoom-bombing
And "OK, Zoomer! How to Become a Videoconferencing Power User" by Boone Ashworth: https://www.wired.com/story/tips-for-using-zoom/?fbclid=IwAR0D_OrA9ZL2IiF0kasDStdn9GuLzGrbQi5Ci3vkEIKwy2byJIYS3DuE2KI