

UCOP Guidance Against Zoom-Bombing

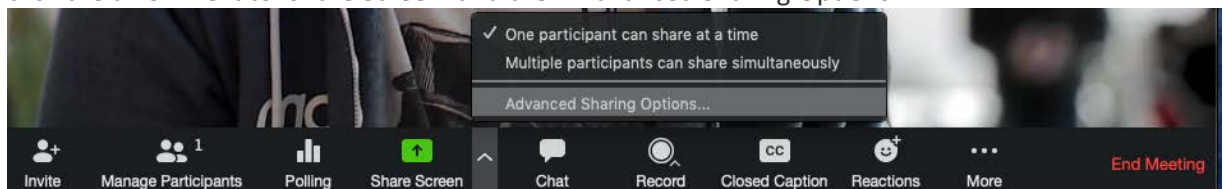
What is Zoom-bombing?

Zoom-bombing is the term for when individuals "gate-crash" Zoom meetings. These uninvited guests may remain silent and if undetected listen to and view your meeting content. Zoom-bombers can also be disruptive or share their screens to bombard Zoom meeting participants with disturbing and inappropriate imagery. Here are some ways to protect you and your Zoom meeting participants from falling victim.

Our top 3 recommendations to update in your Zoom settings immediately:

1. **Avoid "Join Before Host"**. The Zoom Meeting ['Join Before Host'](#) option allows meeting participants, unwanted or not, to join your meeting before you, as host start the meeting. It is always best for you to join as the host before allowing others to join so that you can see who is joining. If you must use the 'Join Before Host' option be sure, at a minimum, to also password protect the meeting.
2. **Protect your Screen Sharing**: To prevent others in your Zoom meeting from taking control of the screen and sharing unwanted content with the group, restrict access to sharing— 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 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

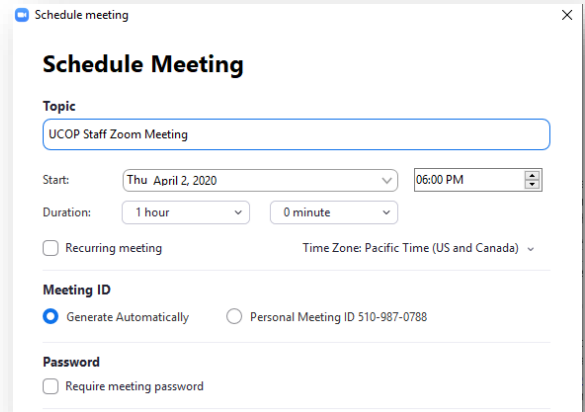
3. **Password Protect your Zoom Meetings**. You can require not just the Meeting ID but also a password to join your Zoom Meeting. You can [require a password](#) for new meetings, instant meetings, PMI meetings or even phone participants. You can also choose not to include the password in the meeting link.

Read on for the full list of Zoom features and instructions to help keep your Zoom meetings safe.

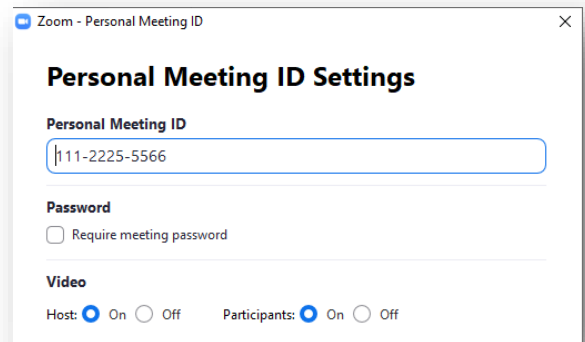
Security Tips on Sharing Zoom Meeting Links and Zoom Settings:

Protect your Meeting ID

1. **Only provide your Zoom Meeting ID** or link to those you want in attendance and that you trust not to inappropriately share it.
2. For additional peace-of-mind, consider **using a random Zoom Meeting ID** (instead of your desk phone number) to make your ID difficult to guess. You can do this by scheduling the meeting and selecting 'Generate Automatically' under 'Meeting ID.'
3. Do not share your Meeting ID or link on **social media or another public location** – especially if your meeting settings do not require a password. Anyone could save the information and Zoom-bomb at a later date.
4. **Avoid using your Personal Meeting ID (PMI) to host public meetings.** Your PMI is essentially one continuous meeting and people can join at their leisure without invitation. [Learn about meeting IDs](#) and how to generate a random meeting ID ([at the 0:27 mark](#)) in this [video tutorial](#).



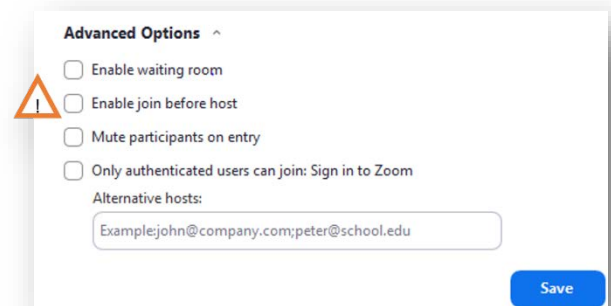
The screenshot shows the 'Schedule Meeting' dialog box in Zoom. The 'Topic' field contains 'UCOP Staff Zoom Meeting'. The 'Start' date is set to 'Thu April 2, 2020' at '06:00 PM'. The 'Duration' is set to '1 hour' and '0 minute'. There are options for 'Recurring meeting' (unchecked) and 'Time Zone: Pacific Time (US and Canada)'. Under 'Meeting ID', the 'Generate Automatically' radio button is selected, while 'Personal Meeting ID 510-987-0788' is unselected. Under 'Password', the 'Require meeting password' checkbox is unchecked.



The screenshot shows the 'Personal Meeting ID Settings' dialog box in Zoom. The 'Personal Meeting ID' field contains '11-2225-5566'. Under 'Password', the 'Require meeting password' checkbox is unchecked. Under 'Video', the 'Host' is set to 'On' and 'Participants' is set to 'On'.

Use Zoom meeting settings to secure your meeting:

1. **Familiarize yourself with Zoom's settings and features.** Understand how to protect your virtual space when you need to. For example, the [Waiting Room](#) (details below) is a helpful feature for hosts to control who comes and goes. Zoom provides extensive [training resources](#) including help articles, videos and regular free training webinars on their website.
2. **Avoid 'Join Before Host.'** The Zoom Meeting [Join Before Host](#) option allows meeting participants, unwanted or not, to join your meeting before you, as host start the meeting. It is always best for you to join as the host before allowing others to join so that you can see who is joining. If you must use the 'Join Before Host' option, you should assign a password to protect the meeting.



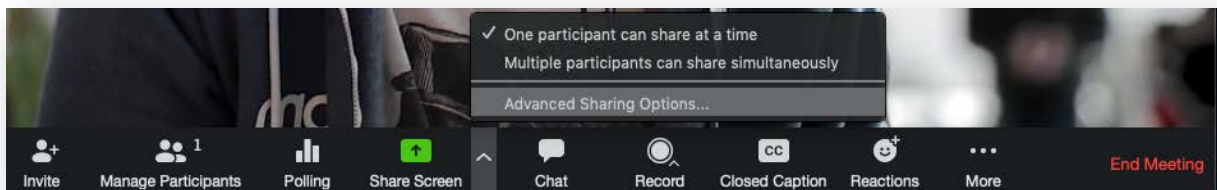
The screenshot shows the 'Advanced Options' dialog box in Zoom. There are four checkboxes: 'Enable waiting room' (unchecked), 'Enable join before host' (unchecked), 'Mute participants on entry' (unchecked), and 'Only authenticated users can join: Sign in to Zoom' (unchecked). Below these is the 'Alternative hosts:' field with the text 'Example:john@company.com;peter@school.edu'. A blue 'Save' button is at the bottom right.

3. **Password protect your Zoom meetings.** You can require not only the Meeting ID, but also a password to join your Zoom meeting. You can [require a password](#) for all meeting types: new meetings, instant meetings, PMI meetings, or even phone participants. You can also choose not to include the password in the meeting link.
4. **Use email notifications.** Keep your Zoom email notification enabled for [when attendees join the meeting before host](#) so that you know when someone joins your Zoom meeting if you aren't expecting it.
5. **Question unknown participants.** If you see an unfamiliar participant or phone number in your participant list or Zoom meeting thumbnails, ask them to identify themselves. As host you can then [rename](#) their thumbnail so that everyone will know who they are. You may also kick out attendees you don't recognize by navigating to the participant list > select 'More' next to their name/number > click 'Remove'

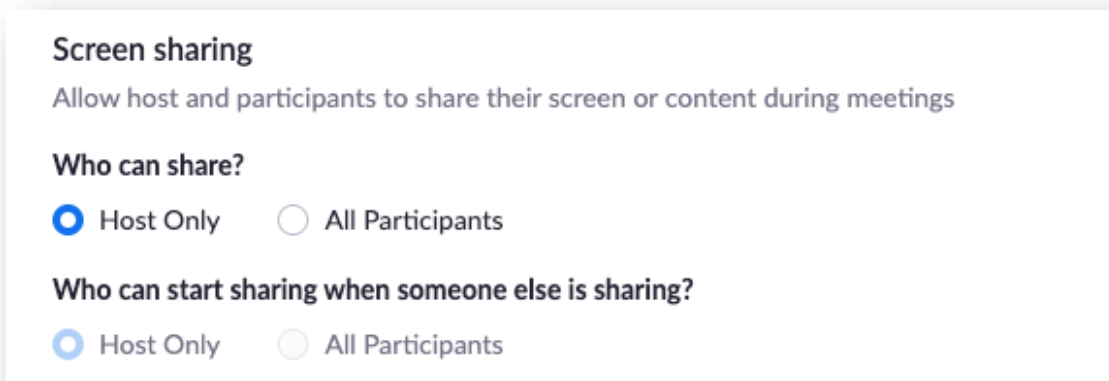
Safe Zoom screen sharing

The first rule of Zoom: Don't give up control of your screen. To prevent others in your Zoom meeting from taking control of the screen and sharing unwanted content with the group, restrict access to sharing so that you're the only one who can screen-share. You can update these settings before the meeting and during the meeting in the host control bar.

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' then close the window. You can also lock the screen share by default for all your meetings in your web settings.

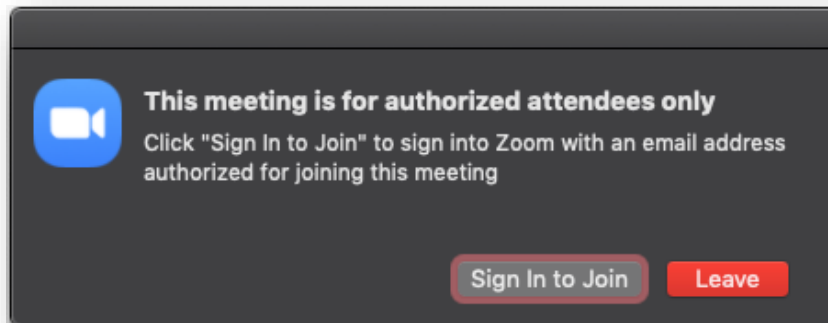


Zoom meeting safety features

Below are a few other features to help secure your Zoom meeting and host with confidence:

Further secure the meeting:

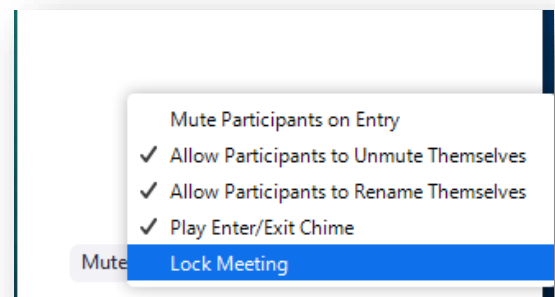
1. **[Allow only signed-in users to join:](#)** If someone tries to join your meeting and isn't logged into their Zoom account, they will receive this message:



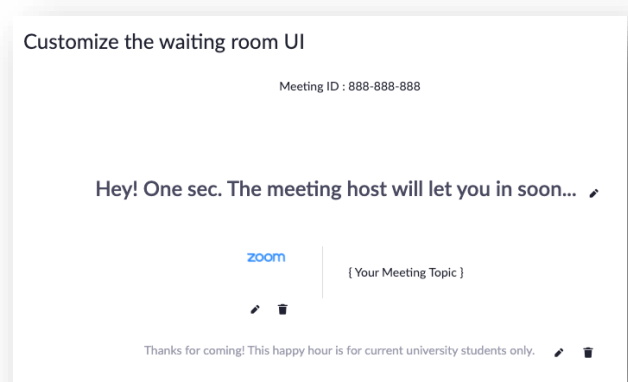
This is useful if you want to control your guest list and ensure that only those invited can attend. The potential challenge is if your participants often join via mobile audio only and have not downloaded the Zoom app.

2. **[Lock the meeting:](#)** When you lock a Zoom meeting in session, no new participants can join, even if they have the meeting ID and password (if you have required one).

From the host panel > click 'Participants' at the bottom of the window > click 'More' in the participants pop-up > select 'Lock Meeting.'



3. **[Use the waiting room feature:](#)** Use the Zoom [waiting room](#) feature to have participants wait until the host arrives and lets participants into the meeting. Meeting hosts can customize waiting room settings for additional control including the ability to [personalize the wait room message](#) people see when they login. This is useful for participants so they know they're in the right meeting. You can also use this feature to post rules or guidelines for your meeting.



The [waiting room](#) feature is a great way to ensure that everyone joining the meeting should be allowed and a great security measure to keep unwanted guests out.

Manage participants

1. **[Remove unwanted participants:](#)** From the Participants menu, mouse over a participant's name, and click 'Remove.'
2. **[Allow removed participants to rejoin:](#)** When you do remove someone, they can't rejoin the meeting. However, you can change your settings to allow removed participants to rejoin. Enable this option in case you remove the wrong person in error.
3. **[Put participants 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 for them to join the call again.
4. **[Disable participants' video:](#)** Hosts can turn someone's video off. This will allow hosts to block unwanted, distracting, or inappropriate gestures on video.
5. **[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.

Managing content and chat

1. **[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.
2. **[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.
3. **[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 meeting is going on and cut back on distractions. This is really to prevent anyone from getting unwanted messages during the meeting.