HOW TO PREVENT ZOOM-BOMBING

WHAT IS ZOOM-BOMBING?
Zoom-bombing is any time an uninvolved third-party joins your Zoom meeting and causes disruptions. Before it becomes a problem, it can be prevented by the host by adjusting the meeting settings or taking actions at the start of the meeting:

1: USE A UNIQUE MEETING ID
For large or public meetings, it is advisable to have Zoom generate a unique meeting ID instead of posting your Personal Meeting ID (PMI) where it can be accessed by anyone.

TO GENERATE A UNIQUE MEETING ID:
When you schedule a meeting, make sure that the GENERATE AUTOMATICALLY option is checked.

2: REQUIRE A PASSWORD
Zoom also gives the option of requiring meeting attendees to enter a password to gain access; this is also another good method for securing your meeting space.

TO REQUIRE A PASSWORD:
Scrolling down from the Meeting ID setting, there is a password option:
To enable this function, click the checkbox and then enter your desired password; please do not use obvious passwords (e.g., “password”) or the passwords that you use for any of your personal accounts.

3: CREATE A WAITING ROOM
Control who enters a meeting by creating a waiting room; this will prevent anyone from entering the meeting until the host gives them the go-ahead—either collectively, or one at a time.

TO CREATE A WAITING ROOM:
First, navigate to SETTINGS in the left-hand column and then click on IN MEETING (ADVANCED)
Scroll down to WAITING ROOM and click the slider to enable this function.

Select whether you want to individually admit all participants, or only users from outside UCI and users who are not logged in. If you would like to, please also use the pencil icon to customize the waiting room.

Returning to SCHEDULE A MEETING, scroll down to almost the bottom of the page to find the MEETING OPTIONS:
To enable this function, click the checkbox ENABLE WAITING ROOM.

4: HOST-ONLY SCREEN SHARING
Another good method is to disable screen sharing for all participants besides the host.

TO DISABLE SCREEN SHARING:
Navigate to SETTINGS in the left-hand toolbar and click on IN MEETING (BASIC).
5: INVITE-ONLY MEETINGS

Another option is to allow only users with accounts hosted at specific domains to enter the meeting.

TO CREATE AN INVITE-ONLY MEETING:

Scroll down to the MEETING OPTIONS at the bottom of the SCHEDULE A MEETING page.
Check the box beside ONLY AUTHENTICATED USERS CAN JOIN. This will restrict access to only users with Zoom accounts hosted at the domains listed; if you would like to allow users with other domains to enter (e.g., @ucla.edu), you can add them by clicking EDIT and adding them to the list with an asterisk preceding the domain (e.g., *@ucla.edu).

6: LOCK IN-PROGRESS MEETINGS
Once a meeting has started and all expected participants have arrived, you can lock the meeting to prevent anyone else from joining.

TO LOCK A MEETING:
While in the Zoom desktop client, mouse over the bottom of the screen to click on MANAGE PARTICIPANTS.
A pane with all of the current participants will open on the right; click on MORE at the bottom to expand options.

Select LOCK MEETING to prevent any other users from joining.

HOW TO ADDRESS ZOOM-BOMBING IN THE MOMENT
   However, there are also methods to address zoom-bombing in the moment:

1: KICK SOMEONE OUT
   If someone slips through despite your efforts, you can always eject them from the meeting.
TO EJECT A PARTICIPANT:
In the Zoom desktop client, mouse over the bottom of the screen to click on MANAGE PARTICIPANTS.

A pane with all of the current participants will open on the right; hover over the name of the participant you would like to eject and select REMOVE.

2: DISABLE SOMEONE’S CAMERA
If someone is behaving badly on camera, the host can cut their visual feed.

TO DISABLE SOMEONE’S CAMERA:
In the desktop client, click on MANAGE PARTICIPANTS.
Select the camera icon beside the name of the participant whose video you would like to cut; to cut their mic, select the microphone icon just beside it.

FOR MORE INFORMATION:
Please consult the article this tutorial was based on, which includes broader explanations and additional reading at the bottom:
“How to Prevent Zoom-Bombing” by Jill Duffy at PCMag