The University of Texas at San Antonio
UTSA Academic Innovation

ZOOM
USER GUIDE

# Student Guide to Securing Your Virtual Meetings

## OVERVIEW

Zoom comes pre-stocked with numerous security features designed to control virtual meetings, prevent disruption, and help you secure your virtual meetings. Here are some do's and don'ts for securing your virtual meetings using Zoom.

## Lock your virtual meeting

Did you know you can lock a Zoom session that's already started, so that no one else can join? It's kind of like closing the classroom door after the bell. Give meeting participants a few minutes to file in and then click Participants at the bottom of your Zoom window. In the Participants pop-up, click the button that says Lock Meeting.

How to lock your virtual meeting room

## Control screen sharing

To give meeting organizers more control over what participants are seeing and prevent them from sharing random content, Zoom recently updated the default screen-sharing settings. Sharing privileges are now set to "Host Only," so meeting organizers by default are the only ones who can share content in class.

However, if participants need to share their content with the group, you can allow screen sharing in the host controls. 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 change the default sharing option to All Participants in your Zoom settings.

How to manage screen sharing

## Enable the Waiting Room

The Waiting Room feature is one of the best ways to protect your Zoom virtual meeting and keep out those who aren't supposed to be there.

When enabled, you have two options for who hits the Waiting Room before entering a meeting:

1. All Participants will send everyone to the virtual waiting area, where you can admit them individually or all at once.

2. Guest Participants only allows known participants to skip the Waiting Room and join but sends anyone not signed in/part of your school into the virtual waiting area.

The virtual Waiting Room can be enabled for every meeting (in your settings) or for individual meetings at the scheduling level.

*Update: Starting March 31, the Waiting Room feature will be automatically turned on by default. Visit our support page for more information on adjusting **your Waiting Room settings**.*

## Lock down the chat

Meeting hosts can restrict the in-meeting chat so participants cannot privately message other participants. We'd recommend controlling chat access in your in-meeting toolbar controls (rather than disabling it altogether) so participants can still interact with the meeting hosts as needed.

How to control chat access

## Remove a participant

If someone who's not meant to be there somehow manages to join your virtual meeting, you can easily remove them from the Participants menu. Hover over their name, and the Remove option (among other options) will appear. **Click to remove them from your virtual meeting, and they won't be allowed back in**.

How to remove a participant

As part of our in meeting security features to help you keep your meetings secure, the meeting host can report a user during a meeting. The host is able to select which users they would like to report, include any written details, and add attachments. This report is automatically sent to the Zoom Trust and Safety team to evaluate any misuse of the platform and block a user if necessary.

Enabling the Report feature

Using the Report feature

## Promoting and securing your meeting

The cool thing about Zoom is that you have these and other protection options at your fingertips when scheduling a meeting and before you ever have to change anything in front of your participants. Here are the most important steps to secure your meeting and prevent Zoom bombing:

- **Create your event/meeting in RowdyLink** and select "Students ad Staff Only" for event visibility to provide additional meeting security. Events listed as students and staff only will requiring signing in with your abc123 to view the event details and retrieve the Zoom link. **Do not post**

**meeting specific details on social media (instead direct them to RowdyLink for more information)**.

- Require registration: This shows you every email address of everyone who signed up to join your class and can help you evaluate who's attending.
- Use a random meeting ID: It's best practice to generate a random meeting ID for your event, so **it can't be shared multiple times**. This is the better alternative to using your Personal Meeting ID, which is not advised because it's basically an ongoing meeting that's always running.
- **Do not create a password for your meeting**. Safely distributing a meeting password is difficult and can land in the wrong hands. **A password also eliminates the added security of the Waiting Room**. When a participant is removed, they cannot re-enter the meeting if a password has not been created for the event.
- Allow only authenticated users to join: Checking this box means **only members of your school who are signed into their Zoom account** can access this particular meeting. Students can log in to their own account by visiting utsa.zoom.us and using the myUTSA credentials.
- Disable join before host: Participants cannot join the meeting before the host joins and will see a pop-up that says, "The meeting is waiting for the host to join."
- Designate a meeting co-host or moderator who will monitor the chat and settings of your meeting.
- Manage annotation: Meeting hosts should disable participant annotation in the screen sharing controls to prevent participants from annotating on a shared screen and disrupting the meeting.

*Note: For schools scheduling meetings through an LMS, some of these settings might appear a little differently. Visit support.zoom.us if you need assistance.*

Additionally, meeting hosts have a couple in-meeting options to control your virtual classroom:

- Disable video: Turn off a participant's video to block distracting content or inappropriate gestures while the meeting is in session.
- Mute participants: Mute/unmute individual participants or all of them at once. Mute Upon Entry (in your settings) is also available to keep the clamor at bay when everyone files in.
- Attendee on-hold: An alternative to removing a user, you can momentarily disable their audio/video connections. Click on the attendee's video thumbnail and select Start Attendee On-Hold to activate.

## Getting Zoom security

You can also check out this video on securing your virtual meeting from the Zoom team:
Zoom 101: Securing your Meetings & Virtual Classrooms

For assistance with Zoom contact Academic Innovation:
academicinnovation@utsa.edu or (210) 458-4520