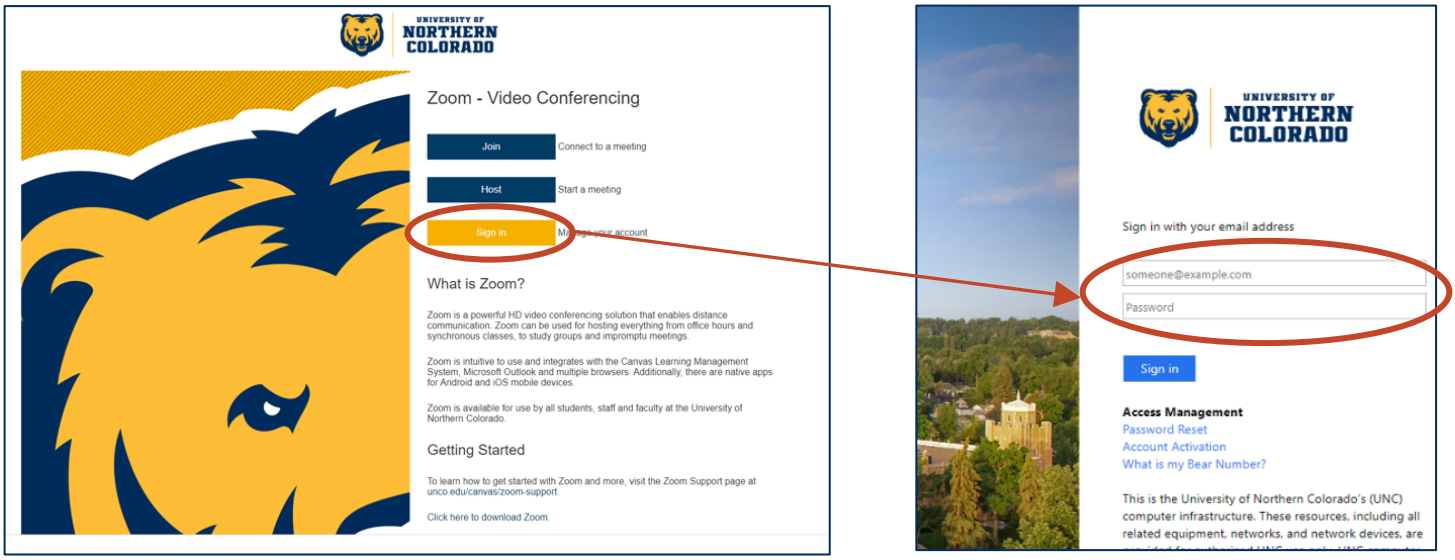
ZOOM SECURITY - BEST PRACTICES

IN RESPONSE TO ZOOM BOMBING 2020

UNC Instructional Design & Development

In response to recent Zoom-Bombing attacks, **we must revisit how we set up and run our Zoom meetings**. At its core, Zoom is a great teaching and learning tool, especially during COVID-19, because it is easy to use and nicely integrated into Canvas. The ease and openness of Zoom also makes it vulnerable to attack, but Zoom has recently done significant security upgrades, and this guide walks you through the Zoom settings you may want to maintain to make your meeting rooms secure. The settings we recommend will make your rooms as secure as possible.

FIRST, ESTABLISH YOUR UNCO ZOOM ACCOUNT



If you have not done so, establish your Zoom account at https://www.unco.edu/canvas/zoom-support/. If you have established your account, log in at https://unco.zoom.us/. **BEST PRACTICE**: Because of UNC's Canvas-Zoom integration, set and monitor your Zoom account settings through the portal pictured above. Once your settings are complete (or updated), then access, schedule, and run your Zoom meetings from within your Canvas course(s). Working in Canvas gives you an extra level of security. You do not need to manage your account outside of Canvas unless you want to make more comprehensive changes to your Zoom settings.

Student access: Students do not need to have a Zoom account to access and attend your Zoom class meetings. Once you have scheduled your meeting, students can open that meeting from their To Do Lists, Calendars, or from the Zoom page in their courses. While the link is redundant in the course, the name, date, and time of the meeting will be clear.

Using Zoom to produce asynchronous content: The most secure way to deliver content in a fully online course is to produce and deliver asynchronous content. You can use Zoom to record your lecture(s), and then you can post the link or embed the video in Canvas. You can record yourself live or without others in your meeting. Our guide, How to Record Yourself in Zoom - Quick Start, provides useful information and guidance for creating course video using Zoom.

OUR RESPONSE TO ZOOM-BOMBING — IMPLEMENT THE MOST SECURE SETTINGS

The best way to secure your online classroom is to work as much as possible inside Canvas, avoid having Zoom send your invitations, and limit your students' abilities to take control of the tools in your Zoom classroom. For an additional level of security, **add a Co-Host** (a colleague or a GTA) to monitor your meeting, especially your Waiting Room, during class.

RE: ZOOM-BOMBING

ZOOM SECURITY - BEST PRACTICES

If a setting is not included here, we don't have a recommendation, or the setting has been locked. If you find that the settings are too restrictive, you can change them. Begin with the most secure settings so you know how they work.

SETTINGS – SCHEDULE MEETING

- Host Video (On) — ON
- Participants Video (Off) — OFF
- Join before host — OFF
- Use personal meeting ID — OFF *(To be safe, always create a new meeting room for every meeting)*
- Mute participants upon entry — ON
- Require a password *(for all meetings)* — ON
- Embed password in meeting link — OFF

SETTINGS – IN MEETING (BASIC)

- Chat — ON
- Private Chat *(Keeps students from attacking other students)* — OFF
- File transfer — OFF
- Co-host — ON
- Screen sharing — ON
- Who can share? **HOST ONLY**
- Disable desktop/screen share for users — ON
- Annotation — OFF
- Whiteboard — OFF
- Remote control — OFF
- Allow removed participants to rejoin *(for anyone removed unintentionally)* — ON

SETTINGS – IN MEETING (ADVANCED)

- Far end camera control — OFF
- Virtual background — OFF
- Auto-answer group in chat — OFF
- Only show default email when sending email invites — OFF
- Use HTML format email for Outlook plugin — OFF
- Waiting Room *(all participants)* — ON

SETTINGS – ZOOM-GENERATED EMAIL NOTIFICATIONS

- When an alternative host is set or removed from a meeting — OFF
- When a meeting is cancelled — ON
- When attendees join before host — OFF
- When someone scheduled a meeting for a host — OFF
- When a cloud recording will be permanently deleted — ON

CREATE A SECURE MEETING

Once you have completed your settings, **WORK INSIDE OF CANVAS**. Also, your meetings will be more secure when you generate a new meeting for every class or individual meeting. For now, it is best to avoid using your Personal Meeting ID (PMI) to host your meetings. Your PMI is basically one continuous meeting and you don't want trolls and hackers crashing your classes.

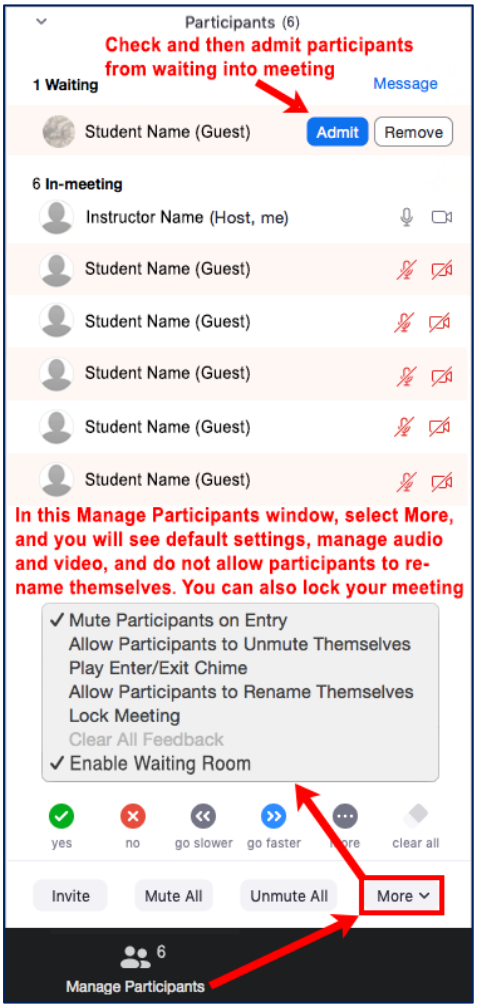
Create a Password for each meeting – When toggled ON, Zoom generates a new password when you schedule a meeting. Participants must enter the password to join the meeting. Don't be tempted to embed a password in the meeting link. It will be most secure if you share the password in a Canvas Announcement just before your class begins.

Invitations – When you use Canvas, Zoom sets up invitations inside of Canvas. Canvas notifies students of their meetings in their To Do List and in their Calendars. Students will be able to go directly to the meeting from either place, and they will also be able to open the Zoom tab in the course navigation, where they will find links to all of their course meetings.

ZOOM SECURITY - BEST PRACTICES
IN RESPONSE TO ZOOM BOMBING 2020

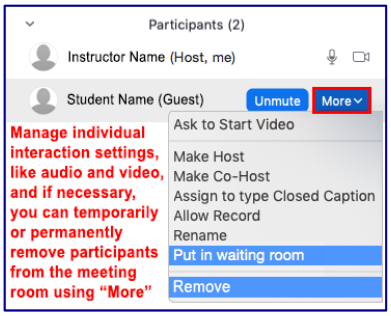
UNC Instructional Design & Development

MANAGE YOUR SECURE SETTINGS DURING YOUR MEETING - HOST CONTROLS



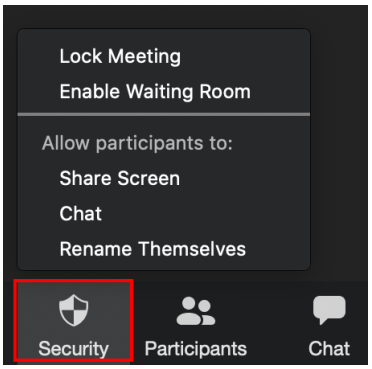
Manage Participants – *During your meeting,* you have several settings to manage. Your meeting functions according to the settings you initially established in your account (see above). Most of these settings can be adjusted, as needed, during your meeting. In addition to managing all participants (see image left), you can also manage individual settings (see image below right).

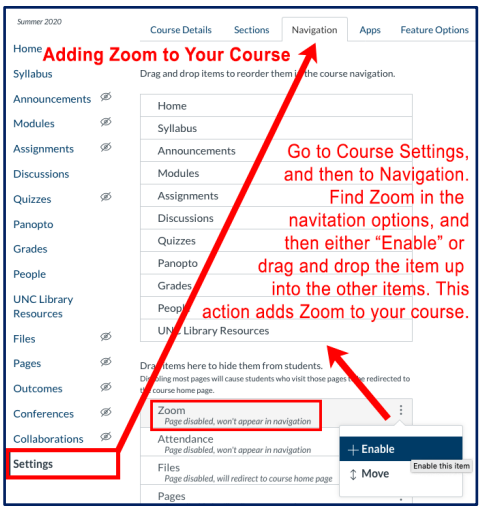
The Waiting Room secures your meeting so that you control who enters. Note that you can remove anyone from your meeting at any time. If needed, you can also put anyone in the waiting room at any time during class.



Add a Co-Host – Managing your waiting room takes time and attention. If you can't lock your meeting at a certain time after class begins, a co-host can monitor your waiting room, your chat, and watch for any other technical issues. The co-host can resolve issues during the meeting.

Secure Sharing – Don't allow students to control parts of your meeting without your knowledge. Using the new in-meeting Security menu (see image right), you can now control when students can share their screen, chat, or rename themselves. If your Waiting Room is not already enabled, you can also easily enable the Waiting Room and/or lock your meeting.





Recordings – You can record any of your class meetings, and share those recordings with your students. In Manage Your Account, you can select Recording settings. If you are recording to the cloud, you will want to think about whether or not to include student thumbnails and student names.

FINAL BEST PRACTICE NOTES

Your meeting is most secure if you work in Canvas. After you establish your account, you can schedule and launch all Zoom meetings in Canvas.

Require that students enter your course using their First and Last name, and don't allow them to change their names within the meeting.

Create a brand new meeting, with a new URL, for every class meeting, and don't share your personal room. Persistent links are vulnerable to attack.