Protecting Your Video Conference

Zoombombing is a new form of trolling where meeting participants use the screensharing feature within a conference to be disruptive. In some cases, it is not our students who are zoombombing, but outside folks who get hold of links to zoom class meetings. It is important to note that Zoombombing is not limited to the Zoom platform. Here are some suggested strategies to mitigating your risk on each platform:

- Zoom
- Blackboard Collaborate Ultra
- Google Meet
- WebEx

Zoom

If you're using Zoom, please follow CUNY's Zoom Security Protocol to secure your meeting. Here is a summary of the recommended settings:

- Avoid using your Zoom personal meeting ID to host your classes.
- Set screen sharing to "host-only" from your account settings ("Settings" > "Who Can Share" > "Host Only")
- Enable the Waiting Room for meetings, which allows you to control when a participant joins the meeting.
- Consider locking your meeting when all your students are in attendance.
- Remove participants if necessary.

If you are new to Zoom and not familiar with the various settings. Here are some detailed articles:

- Preventing Zoombombing by USC
- How to Keep the Party Crashers from Crashing Your Zoom Event by Zoom
- Zoom Settings to Prevent Zoombombing by UC Berkeley.

Blackboard Collaborate Ultra

If you're using Blackboard Collaborate we recommend you do not send the direct link to your Blackboard sessions to your students. Anyone with the “guest link” that Blackboard generates can access your session. Instead, we recommend you create a dedicated content area for your Blackboard Collaborate sessions where students can find all your Collaborate class sessions. For instructions on how to do this see Adding Blackboard Collaborate Ultra as a Permanent Space for Students.

Google Meet

If you're using Google Meet, we highly-recommend inviting your students directly via email using a calendar invite by scheduling a meeting as opposed to sharing a public link to your room. As students join the meeting you will be prompted to admit each student as they enter. Be mindful of who you admit, since there is currently no option to disable attendee screen sharing in Google Meet.

Take the following actions if you experience Zoombombing in a Google Meet session:

1. Immediately mute and remove the user.
2. Instruct your students to leave the current meeting and that you will send them a new meeting invite via email.
3. Delete the Google Calendar event associated with the meeting.
4. Schedule a new meeting and invite your students again via email.

If you fall victim to Zoombombing again, consider switching to an alternative video conferencing option such as Zoom or Blackboard Collaborate Ultra that has additional settings to limit guest screen sharing.

WebEx
If you're using WebEx we recommend the following settings to secure your meeting:

- Avoid using your WebEx “Personal Room” link to host your classes.
- Disable the “Anyone can share” setting from your meeting:
  - Open the “Participant” menu on the menu bar
  - Uncheck the “Anyone Can Share” option
- Use a meeting password when scheduling your meeting. **Note:** All WebEx meetings require a meeting password by default – do not disable this option.
- Invite your students directly via email instead of sharing the meeting link. Your students will receive an email with a calendar invite for your meeting. Try to limit directly sharing your meeting links.