Protecting Your Video Conference

Zoombombing is a 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

Please follow CUNY's Zoom Security Protocol when using Zoom. In summary, always set a meeting password, do not share your personal Zoom Meeting for your class, and use the waiting room option. Here is a summary of the recommended security settings:

Protocol	Required	Recommended
Don't publicize Zoom classroom meetings on social media or public forums	✓	
Set a password for all meetings	✓	
Turn off file transfer	✓	
Keep the Zoom application updated to the most recent version	✓	
Don't use a Personal Meeting ID (PMI) to host a classroom or large event meeting	✓	
Disable private chat	✓	
Allow chat with host only		✓
Set "Screen Sharing" to "Host Only"		✓
"Lock Meeting" after all participants have joined		✓
Turn off annotation when not needed		✓
Use "Waiting Room"		✓

Additional Resources:

- 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 then 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.